Testimony of Michael I. Shamos before the
Election Assistance Commission
on the
DRAFT Procedural Manual for Voting System Testing and Certification Program

October 26, 2006

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 six states, primarily Pennsylvania and Texas, and have personally performed 119 electronic voting examinations.

In testimony before the House of Representatives Committee on Science in June 2004, I offered the 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.” Not only do I still hold that view, but election events over the past two years have convinced me even more that it is the correct one.

As a state examiner, I often feel like a pathologist, my examination table littered with the dead bodies of voting systems that passed federal testing but failed at the state level. The average pass rate for federally qualified voting systems in Pennsylvania is approximately 50%, when it should be well above 90%, and I often ask aloud during examinations how a particular flaw could possibly have gotten past an ITA. But my question is rhetorical, for I cannot find out. Even when I see an ITA Qualification Report, it is obscure. It contains a lengthy list of tests allegedly performed and an indication whether the system passed them or not, but no information on how the tests were conducted, how close the system came to failing or how many times a test had to be performed for the system to pass.

For me, the overriding purpose of federal testing is to relieve the states of the burden of testing to the voting system guidelines. For the states to disband their own testing procedures and place reliance on federal laboratories creates a profound obligation on those laboratories to conduct testing in a way the can be fully trusted upon by the states and the voters. Right now, we cannot rely on the ITA process, and codifying it into a set of federal regulations will not bring the sea change that is necessary.

I find it instructive that in the history of the ITA system, no system ever failed qualification. Instead of a pass/fail system, the only options are “pass” and “hasn’t passed yet.” There is no feedback to the public at all on what, if anything, is flawed about the systems that have been tested. This structure is retained in the current draft Manual, which does not even contain the word “failure.”

My chief criticism of the draft Manual is that it legitimizes by specifying in great detail a system that has proven not to meet the critical needs of either the states or the voters. Section 1.4.4 of the draft Manual states that a purpose of the EAC Certification Program is to "increase voter confidence in the use of voting systems." That will not happen if the EAC simply takes over management of the current ITA mechanism.

The VSTL Process

The responsibilities of the EAC with respect to accrediting testing laboratories are set forth entirely in Section 231 of HAVA. Unfortunately, HAVA is silent on the fundamental purpose of the accreditation program or even of the Voluntary Voting System Guidelines that serve as the basis for laboratory testing.

It is the express intent of HAVA that states will choose to rely on the outcome of federal laboratory testing in deciding whether to certify voting systems in their respective states. It would be irresponsible for a state to repose such trust in a laboratory if it had no independent means to verify or validate what the laboratory is doing.

The fundamental problem with federal testing to the VVSG is a built-in lack of transparency. The laboratories are paid by the manufacturers seeking certification, and they are answerable to the manufacturers. They have no other perceived responsibility other than to retain their accreditation. They have no defined duty to the public or even to the states that rely on their certifications.

The problem is not a lack of qualified laboratories. The problem is the entire architecture of the VSTL system, which must be rebuilt brick by brick, with due attention to the public's interest in a completely open process.

The Manual

The Manual does not address how a VSTL is to be chosen to examine a particular system, how it is to be paid, and to whom it owes responsibility. The choice of VSTL should not be made by the manufacturer, since this encourages gaming the system, but should be made by the EAC, preferably on a random basis. The VSTL should not be paid by the manufacturer, but by the EAC. The EAC can ultimately recover costs from the manufacturer. The immediate consumer of a certification report is the EAC, which is answerable to the public. The secondary consumers are the states and the public, but the public never gets to see what the EAC and state officials are relying upon. The draft Manual states that it "is a comprehensive presentation of the EAC Voting System Testing and Certification Program" and "is intended to establish all of the program requirements." Yet the process by which a laboratory is engaged and paid by a manufacturer is never mentioned, nor is there any provision for auditing that process.

The Manual imposes conflict-of-interest restrictions on EAC employees, but says nothing about conflicts involving manufacturers and laboratories. It contains no code of ethics, nor even an overall statement of ethical guidelines.

The Manual is entirely too solicitous of the supposed trade secrets of the manufacturers. My belief is that any company wanting to enter the voting system business must check his trade secrets at the door. As long as the code in voting systems remains secret, the public will never trust it, nor should it. But regardless whether code should be secret or not, the tests performed by the VSTLs and their results and reports should certainly not be.

In Pennsylvania, every aspect of the examination process is open. The pubic attends the examinations, they are recorded on videotape, and the reports and videotapes are made public. Even that does not stop criticism of the process, but at least it cannot be faulted for secrecy. If a state can make its examinations open, so can a VSTL.

In an effort to be constructive, and not merely to complain, in my written testimony I have provided detailed comments on the draft Manual. However, the problem here is not in the details, but the in overall architecture of the system, for which I urge a significant redesign.

I thank you for the opportunity to address the Commission 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 115 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.

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* 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 has provided testimony on electronic voting to the Pennsylvania legislature and on four occasions to committees of the U.S. House of Representatives.

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

Comments on “DRAFT Testing and Certification Program Manual 2006”

The overall problem with the Manual is not so much in the details, but in the overall structure of the VSTL process. It is not transparent, and VSTLs are not answerable to the correct party. Their fees may ultimately be paid by the manufacturers, but their customer is the states and the voters. The public (and state certifiers who rely on federal certification) are entitled to know exactly what was done to a test a voting system and what the outcome was. To the extent that the process is conducted in secret, then to that extent it will not be trusted. I regard it as an essential goal of the EAC to implement a fully trustworthy testing program.

1.7. This section imposes conflict-of-interest and ethical restrictions on EAC personnel, but does not apply to manufacturers and VSTLs. Right now, there is nothing to prevent a manufacturer, for example, from having a financial interest in a laboratory, though clearly this should be prohibited.

1.12. It is not clear whether documents produced by VSTLs in connection with their examinations constitute “documents submitted under this program,” nor is it clear which documents are “protected from release by law.” It would not serve the goals of the Program to have VSTL reports protected from release by law.

2.3.1.1.6. Disclosure of a controlling interest in a manufacturer is required, but this is not sufficient. Disclosure of all stockholders owning or controlling beneficially one percent or more of an entity should be disclosed.

Further disclosure should be required concerning criminal records of any officer, director or employee of a manufacturer.

2.3.2.2. The permanent affixation of a certification label is unwise. What is to be done if the equipment is subsequently decertified?

2.3.2.7, relating to reports of malfunction, may require modification. After each election there are a huge number of “reports” or claims of malfunction, with no organized way of communicating them to the manufacturer, so some definition will have to be given of when a report to the EAC is required.

2.5. Provision needs to be made for the acquisition, sale or merger of a manufacturer. If B is registered, and A acquires B, is anyone still registered?

4.2 This section leaves the choice of a VSTL to test a system up to the manufacturer. Such a process fosters misconduct and encourages VSTLs to compete with one another by establishing reputations for leniency.

4.6. This section provides for a test report only if testing is successful. There is no mechanism for alerting the public to failures. The very possibility that a failure would be made public will act as a significant force to encourage manufacturers to test their own systems thoroughly before submitting them for certification.

5.8.2. The verification of integrity of voting software cannot depend on any device or software furnished by the manufacturer. It must be possible to connect an independent device to a voting machine or system to obtain a copy of the software and/or firmware present on it by means that cannot be corrupted by the machine or system.

Section 6. While it is theoretically possible for a system to be denied certification, the likelihood of a report being produced to that effect is slim because the manufacturer can always request an opportunity to cure and can appeal. In practice, such reports will not be issued.

Section 7. While decertification is an important tool, it is a weapon so powerful and damaging that it will rarely be used. The reason is that decertification would make it illegal to use a system throughout the United States in states that have adopted the VVSG. Who will pay to replace the decertified machines? One solution is to require manufacturers to grant their customers a continuing warranty of certification, requiring the manufacturer to repair any non-compliant system so it becomes compliant, or pay the cost of a certified replacement.

The process of Section 7 is extremely cumbersome and heavily weighted in favor of manufacturers, when it is the voting public which requires protection. I estimate that under normal circumstances a decertification would take 9 months, but up to two years if contested by the manufacturer. Streamlined procedures should exist for an expeditious determination of certifiability.

In Section 7.4, the powers of investigators should be specified precisely. If they do not have the customary investigative powers, then the penalty to a manufacturer for failure to cooperate with an investigation should be removal from registration as a manufacturer.

Section 10 provides far too much opportunity to submerge vital information about voting systems. Protection of personal and confidential commercial information is reasonable; the manufacturers' claims of trade secret are not.

Section 10.3 skirts a critical issue. It defines certain things that are definitely trade secrets and lists others that are likely not, but gives no guidance on such critical items as voting system source code itself (as opposed to "source code used to develop or manufacture software") and leaves out VSTL reports.