Written Testimony of
John Washburn, VoteTrustUSA Voting System Technical Advisor
before the Subcommittee on Information Policy, Census and National Archive
of the Committee on Oversight and Government Reform
U.S. House of Representatives
May 7, 2007

Thank you, Chairman Clay and distinguished members of the committee, for holding this hearing and for giving me this opportunity to present testimony to you on the testing and certification of voting systems.

My name is John Washburn. I have worked in the field of software quality assurance since 1994 and for the 10 years prior to that I was a computer programmer developing commercial software. Since 1998, I have held the certification, Certified Software Quality Engineer, from the American Society for Quality. For the last year I have been a technical advisor to VoteTrustUSA a nonpartisan national organization serving state and local groups working on election integrity.

I am here to present an outside assessment of the testing framework under which voting systems have been tested and certified to Federal standards from the perspective of a software quality assurance professional. I will address both the recently terminated program administered by the National Association of State Election Directors (NASED) and the program recently adopted by the Election Assistance Commission (EAC), established as a result of the Help America Vote Act (HAVA). It is important to consider both past and present testing processes for two reasons – first, all equipment currently in use has been tested under the former NASED/ITA testing process and most of this equipment will be used again in the next federal election. Neither program provides sufficient public oversight or accountability to ensure voter confidence that fielded equipment is in conformance with Federal standards. While the new EAC program has made some steps towards greater transparency and oversight, it retains some of the systemic flaws of the previous program.

I will also suggest a testing framework which can be implemented and administered immediately under the authority of section 241 of the Help America Vote Act. This alternate framework can executed in parallel with and in addition to the EAC framework.

The NASED and EAC testing and certification frameworks suffer from three systemic flaws, which I will explain in greater detail below.

1. Both systems are opaque to most primary stakeholders in the election process. These stakeholders are state election officials, local election officials, candidates for public office, and most importantly the voters.
2. Due to the lack of transparency and accountability, neither system adequately ensures the public that rigorous, thorough, and effective testing has been performed.
3. Neither system permits or encourages the reporting of system defects, nor do they include a responsive corrective action plan.

The System is Opaque

Under the NASED system, the entire testing process was a private sector transaction between the manufacturer and the testing laboratory, shielded from public oversight by vigorously enforced non-disclosure agreements. The reports of test results, as well as documentation of the testing undertaken to confirm a voting system's compliance with standards are considered the property of the manufacturer of the system. In cases where reports have been shared with state or local election officials, the reports have been routinely exempted from open records requests because the whole report is considered a trade secret rather than isolated sentences and paragraphs therein. After considerable effort I have been able to obtain redacted copies of some reports from the Wisconsin State Elections Board, but it is extremely rare for citizens to gain access to even redacted reports.

Trade secret protection is established by the manufacturers in the contracts they negotiate with jurisdictions purchasing their equipment and recognition of the manufacturer's claim to trade secret protection continues in the EAC program as well, as described in the Voting System Testing and Certification Program Manual. A complete copy of this manual can be found in Appendix A of my testimony.

The fact that complete documentation of test plans and results are treated as trade secrets means that necessary evidence to verify that a system is fit for use in administering an election is unavailable for public inspection and oversight.

While some states have the resources to undertake their own state level testing and certification, many states rely entirely upon national certification to ensure that systems that are purchased are in conformance with Federal standards.

Also considered a trade secret and thus closed to public review under both the past and present system is the testing harness itself. What specific tests are done to see if a system meets the requirements of paragraph 5.3 of the 1990 FEC Voting system Guidelines? How is the system identified and where is the physical configuration audit located so a state or local election official can verify the system which was delivered to him is the same system which was certified? Where is the list of types of software inspected? How is the source code inspected? All of these questions of how the testing and certification are done are considered trade secrets and closed to review.

The number and nature of the defects discovered in the testing process, as well as how and if the discovered defects were repaired is also considered a trade secret

For jurisdictions without state-level testing and certification, all that is available is a list of systems which have been granted certification numbers and the assurance that NASED has ruled that the certified system is in conformance with the standards.

Without the test plans and results of the test executions there is no evidence. There is only an appeal to authority. The inadequacy of the test plans, methods, and documentation in independent reviews of testing labs like the one commissioned by the New York Board of Elections, and the non-conformance revealed in penetration attacks and academic reviews has undermined confidence in that authority.

The Testing is not Rigorous

Over the last several years numerous security and design defects have been uncovered by independent researchers and election officials. Each of these discoveries has left unanswered the simple question: How did these non-compliant systems ever get certified?
Here are four examples:

1. Use of a programming technique called "interpreted code" is prohibited by both section 5.3 of the 1990 FEC Voting System Standards and section 4.2.2 of the 2002 Voting System Standards. This prohibition is extremely important because the use of interpreted code makes it easy for someone to change the operation of the voting system on the fly in the field. But, in spite of this prohibition, Diebold systems with interpreted code were qualified by NASED on 11 separate occasions over a span of 3 years. Details of this violation can be found in Appendix B of my testimony.
2. A member of the Technical Subcommittee of NASED's own Voting Systems Board has stated that the vote-tabulation software found on ES&S equipment varies from machine to machine and from election to election because for each election jurisdiction and for each election in each jurisdiction, a new and unique version of the vote-tabulation software is created. This is a violation of sections 8.7.1 Volume I and Appendix B.3 of the 2002 Voting System Standards and sections 9.7.1 Volume I and Appendix B.3 of the 2005 Voluntary Voting System Guidelines. These four sections relate to the identification of the software being certified. If the software changes from election to election how can any version be – "**the**" – certified version? Details of this violation can be found in Appendix C of my testimony.
3. The central election management system from Sequoia, which accumulates the vote totals, includes both source code and the compiler for that source code. This is violation of section 6.4.1.e of the 2002 Voting System Standards and a violation of section 7.4.1.e of the 2005 Voting System Guidelines. The prohibition against the use of source code and compilers in election systems is as important as the prohibition against interpreted code. They make it easy to change the operation of the software on the fly in the field. For details about this violation, see Appendix D of my testimony.

These examples of non-conformance went undetected in multiple rounds of testing conducted over the course of years. Because these violations were found without the benefit of access to test results, I cannot help but wonder how many other violations those results might reveal.

The 2005 Voluntary Voting System Guidelines (VVSG) are stronger than the 2002 Voting System Standards but the 2005 VVSG are still a very weak standard. It has been stated to this committee that the move from the NASED framework to the EAC framework is analogous to moving from college ball and profession ball. This is incorrect. The proper analogy is that the move between the two testing frameworks is the same as the move from sand lot baseball to little league ball. As with little league ball, the 2005 VVSG and the EAC testing framework are the first effort to operate with consistent rules and introduce an umpire to call balls, strikes, and fouls. Since the 2005 VVSG do not require a voting system be as reliable as an incandescent light bulb, the EAC framework has a long way to go before it is in the major leagues.

The profound and real world consequences of this illusion of testing can be found at the one hour and nine minute mark of the documentary, ***Hacking Democracy***. In a realistic simulation of an election, the outcome of the mock election is altered in spite of the election officials following all of the proper election administration procedures. This manipulation of the mock election would not have been possible if the voting system, which NASED declared met the 2002 Voting System Standards, had actually met those standards. A copy of this DVD is included with my testimony.

The System Does Not Promote Self Correction

The NASED testing frame work provided absolutely no mechanism to report problems and no way to receive suggestions for improvement. The EAC has created a new program called the QMP, Quality Monitoring Program, which is defined in chapter 8 of the Voting System Testing and Certification Program Manual; Program manual for short. Excerpts of this manual are included in Appendix A of my testimony.

The EAC's Quality Monitoring Program falls far short of any professional quality monitoring program I have encountered, both in its effectiveness for addressing testing deficits and in its implementation of corrections.

First, the Quality Monitoring Program limits itself to ***fielded*** systems, which are defined broadly in Chapter 1 of the Program manual. This definition is contracted throughout the rest of the Program manual such that only systems which have been certified by the EAC and are used in a federal election are considered ***fielded systems***. Since the EAC has not yet certified any systems, no system currently in use meets this definition. This means that any system in use in 2006 and the vast majority of those that will be in use in 2008 do not qualify for assessment under the EAC's Quality Monitoring Program. Thus, the Quality Monitoring Program fails to meet the mandate laid upon the EAC by section 202 of HAVA to be a clearinghouse of information on ALL voting systems, not just those which meet the limited definition of fielded. Section 202 of HAVA can be found in Appendix F of my testimony.

Second, the Quality Monitoring Program will only record ***anomalies*** as defined by section 8.7.3 of the Program manual. The definition of an anomaly in this section is exceptionally narrow. It permits the dismissal of any report on the basis that the report is an "administrative error" or a "procedural defect".

In contrast, the common practice in the software quality industry is to report and record everything and classify and categorize later. Applying gate keeping definitions such as those found in section 8.7.3 of the Program manual are not only frowned upon in professional software quality assurance, such gate keeping can be regarded as a sign of manipulating the QA process.

Two examples from last year suffice to demonstrate the power the gate keeping aspect used to define an anomaly.

One of the more interesting failures of a voting system last year was in Pottawatomie County, Iowa. The details of this can be found in Appendix G of my testimony. A programming error caused the election system to incorrectly tally the results of 10 races on the June 6, 2006 primary ballot. This error does not meet the EAC's definition of an anomaly because it was ruled the pre-election testing done by Ms. Drake, the County Auditor, was insufficient. Since insufficient testing is a procedural deficiency, the failure of the system to correctly tally votes is not considered an anomaly.

Similarly, the mysterious 18,000 vote under count in Sarasota County would not be considered an anomaly because the official explanation is administrative error. The Sarasota County Supervisor of Elections, Ms. Dent, laid out the ballot pages poorly and it is speculated that this

administrative error led to the 18,000 under votes. Such administrative errors are not considered anomalies and will not be included in the Quality Monitoring Program.

Finally, the EAC has adopted a limited definition of ***credible report*** found in Chapter 9 of the Program manual, which may further hinder the effective recording and response to system deficits. Only ***credible reports*** will be published and distributed to other election officials by the EAC under the Quality Monitoring Program. Information in a credible report must first meet the definition of anomaly. Second, only election officials may file such reports. Third, the events included in the report had to have happened during an election.

If an election official discovers defects in a voting system during pre-election testing or during other testing, this also is not a credible report because it did happen during an election. If an election official were to undertake an independent review and report the security vulnerabilities they uncovered, neither report would be shared with other election officials, because their information does not meet the definition of a credible report. Even though they are election officials, the failures they may find did not occur during an election.

Lastly, the new, untried EAC framework for testing actively resists opportunities for improvement in two ways. The testing plan used to determine if a system meets 2005 VVSG can only be improved based on credible reports. Without such credible reports the NIST has no authority under the provision of Handbook 150-22 to require the labs to improve their testing methods. This provision could inhibit correction or improvement of the testing process. The second way the EAC framework resists improvement is the long lead time needed to make even modest improvements to the standards. For example, in the 2007 standards currently under formulation the modest proposal that voting systems work as described in user and technical manuals was not approved as a guideline. Thus, the soonest this modest requirement can be come part of a standard is 2009 and would not applied to any system prior to 2011.

A Better Way.

While I have been quite critical of the EAC model of testing using slowly changing standards, there is great value in such testing. But, it must be seen as the minimum base and nothing more.

All good software testing follows several general principals:

1. The tests are by design. The design is the tester's design not that of the developer. Testing is not a haphazard or ad-hoc process.
2. The tests are designed to discover defects not success. The operating assumption of effective testing is the system and software under test has defects, and it is the tester's job to discover where.
3. Tests predict expected results. If you are not counting every stroke, it is not golf. If you are not calling your pockets it is not pool. If you are not predicting results, it is not testing. Without prediction there is no testing only documentation.
4. The test results – good, bad, or ugly – are recorded accurately and immediately. Categorization as to cause and relevance is postponed until after the defect is recorded.
5. The test plans and test results form a body of evidence which supports the claims made about the system tested.
6. The system under test can be positively and affirmatively identified.

The NASED framework and the proposed EAC framework fail all six of these simple precepts. Even at this late date there is the possibility the EAC framework can be changed to incorporate these precepts of good software testing. Unfortunately, there is not much time before the primary season for the 2008 presidential election begins. Because of this short time, I propose the EAC use the authority already granted to the Commission under section 241 of the Help America Vote Act to set up a second parallel framework for testing. The details can be found in Appendix H of my testimony. A brief description follows.

The HAVA 241 testing framework purchases a pool of voting equipment. The pool of systems would be identical to those purchased by local election officials. The pool of systems would be made available to academics and others from the public in order to execute tests on the systems. The access to the systems would be granted by auctioning, random lot or some combination of both. The stipulation for testing is that all contact with the equipment is recorded in full video and sound so there is no dispute later as to what was or was not done. These recordings are then available to anyone for a modest reproduction fee.

This HAVA 241 testing framework would be effective and efficient and would preserve the intellectual property of the equipment manufacturers. It would be effective because there is currently a backlog of testing to be performed which only requires access to equipment. It would be efficient (finds the most new information in the least time) because those who bid high are those who have the greatest confidence of their success and paying for access fosters efficient use of time.

In Conclusion

The NASED testing framework

- is opaque to every stake holder in election equipment except the manufacturers
- gives the illusion of rigorous testing without the substance, and
- resists to reports of problems or suggestions for improvement.

The new, untried EAC testing framework has these same, deep flaws.

Before the first system is granted certification the EAC framework needs to be substantially re-structured to remove these systemic flaws.

In the meantime, an alternate testing framework needs to be created. I have suggested one such framework which is more nimble, more effective, and more efficient than either the NASED framework or the EAC framework.

Explanation of Acronyms

DRE	Direct Recording Electronic
EAC	Election Assistance Commission
HAVA	Help America Vote Act
ITA	Independent Test Authority
NASED	National Association of State Election Directors
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Lab Accreditation Program
QMP	Quality Monitoring Program
VSTCP	Voting System Testing and Certification Program
VSS	Voting System Standards
VVSG	Voluntary Voting System Guidelines