Requirements for Evaluation of Voting System Security

by

Roy G. Saltman
Consultant on Election Policy and Technology

presented to:
Technical Guidelines Development Committee
of the
Election Assistance Commission
at the
National Institute of Standards and Technology
September 20, 2004

1. Personal Information

The panel chair, Dr. Ronald L. Rivest, has asked that each panelist commence with a personal introduction. The following is intended to fulfill that requirement:

Since May,1996, I have consulted individually on election policy and technology for, among others, the International Foundation on Election Systems and the American Civil Liberties Union. For the former, I have consulted in Brazil, Ecuador, Venezuela and Japan. For the latter, I have served as an expert witness on the failings of pre-scored punch card voting in California and Ohio. I was employed at NIST as a computer scientist from 1969 until 1996, when I retired. Previously, I was employed by the Sperry Rand Corporation from 1955 to 1964 and by the IBM Corporation from 1964 to1969. With both organizations, I worked in the field of computer engineering. I have two master's degrees, one from MIT in electrical engineering and the other from American University in public administration. I have two additional degrees in engineering, one each from Rensselaer Polytechnic Institute and Columbia University. My CV shows a significant number of publications and presentations.

While employed at NIST, I authored two reports that are well-known by those concerned with the voting process. The first, entitled *Effective Use of Computing Technology in Vote-Tallying*, was published in 1975 as NBSIR 75-687 and re-published as NBS SP 500-30 in 1978. The second report, entitled *Integrity, Accuracy and Security in Computerized Vote-Tallying*, was published in 1988 as NBS SP 500-158. At NIST, the author's name is printed on the face of the publication and anyone who has seen my reports knows that this situation pertains to my reports.

2. The Bottom Line: Public Confidence in Announced Results

A national awakening occurred after November 7, 2000; the Help America Vote Act (HAVA) was enacted by the Congress and signed by the President in October, 2002. Regardless of what went before, the nation is now counting on NIST and the Technical Guidelines Development Committee (TGDC) to develop recommendations that can be implemented to improve election integrity and security.

The functions of the TGDC are described in Section 221 of HAVA. The Director of NIST is a member and is to serve as its chair. Some specified subjects to be considered by the TGDC that are most relevant to this hearing are:

> (A) the security of computers, computer networks and computer data storage in voting systems, ...
> (B) methods to detect and prevent fraud;
> (C) the protection of voter privacy; ....

The bottom line by which TGDC may be measured is the effect of its recommendations on public confidence. This is not a new idea. In 1975, I wrote:

> "The assurance that steps are being taken ... to prevent unauthorized computer program alteration or other computer-related manipulations remains, nationwide, a continuing problem for the maintenance of public confidence in the election process" [Saltman, R., 1975, p. 4].

The issue of public confidence is older than that. Concern that elections have been stolen goes back to the earliest days of the Republic. The three decades after the Civil War, 1865 to 1895, were perhaps the heyday of election fraud, involving the infamous Tweed Ring's New York frauds of 1868, the stolen Presidential election of 1876 and the unsurpassed bribery and intimidation of the Cleveland/Harrison election of 1888. More recently, the uncertainty and ambiguity surrounding the outcome of the 2000 Presidential election in Florida has continued to resonate with many citizens. Even though the concern now is placed on different subjects, namely the correctness of software and the potential failure of electronic equipment, rather than on hanging chad and inability of many voters to correctly record their intentions, many voters have a recurring nightmare that the turmoil generated in that election's aftermath will happen again.

For example, I was told just last week by a professor at a Maryland university the "real reason" that the Maryland State Board of Elections wants to remove the State Director of Elections. It is not just their difference in party affiliation, he said. It is so that the current state director would not be able to manipulate the software to benefit her party and so that the new director would be able to arbitrarily change the software to benefit the party of the Board of Election's majority. This anecdote demonstrates that the TGDC will never be able to convince <u>all</u> the people of the efficacy of what it will develop, but let us hope that it will be able to convince important molders of public opinion. These include the editorial writers of major newspapers who, after many years of neglect, have suddenly discovered the issue of the voting process. It appears that the issue of public confidence, now, is closely tied to the question of software correctness.

3. <u>Testing All the Software to be Used</u>

The New York Times, on May 30, 2004, published an editorial entitled "Who Tests Voting Machines?" The article, 9 inches long and over 6 inches wide in two columns, fails to mention NIST at all or the TGDC. Nevertheless, the *Times* makes some good points and asks good questions.

The editorial quotes a well-known activist as stating that:

> "The standards do not require examination of any commercial, off-the-shelf software used in voting machines, even though it can contain flaws that put the integrity of the whole system in doubt."

I agree that this is a problem. I wrote in 1975:

> " ... in order to eliminate as many security threats as possible, the least complex operating system that provides the capabilities required by the vote-tallying program should be used to support the vote-tallying process" [Saltman, R., 1975, p. 50].

In my opinion, it is necessary to test the <u>entire</u> software package that exists in a voting machine that is used to record and count votes. When I wrote the 1975 report, central processing of ballots was almost universally carried out. That meant that the computers doing the vote-recording and counting were probably multi-processors and they may have been undertaking non-elections processing at the same time. The report section just quoted is part of Section V.F.2, entitled "Use of Dedicated Operation" [Saltman, R., 1975, pp. 49, 50]. I proposed dedicated operation only.

Now, technology has changed. Much vote-recording and counting has been accomplished on precinct-located computers. Indeed, requirements in HAVA imply that <u>only</u> precinct-located vote-recording may be done in the future to allow the voter the opportunity to correct overvotes. That could not be accomplished with a central-count process. When precinct-counting is being done, the likelihood is very high that the computer is dedicated to vote-recording and counting and is not performing any other task.

Therefore, it makes no sense to use an operating system in such a computer that is intended for multi-tasking operations by a human user. Nevertheless, it appears that at least one election equipment manufacturer has based its offerings on just such an operating system. If software is based on an enormous operating system containing much code that is unused for voting purposes, it cannot be effectively tested. The size, i.e., the number of lines of code, of the vote-tallying software presented by the vendor should be considered as a parameter in the certification process. Either the cost of testing should be increased accordingly to the vendor, or the product may be summarily refused certification for being beyond a testable size or for including extraneous functions. Additionally, the certification process should be undertaken on the software in its final object-code form (as well as in source-code form), to include the effects of compiler software that may have contained malicious code to be implanted in the vote-recording and counting software.

4. <u>Publication of the Accreditation and Testing Requirements</u>

The New York Times editorial just quoted makes recommendations on the testing process. Specifically, it states:

> (1) "Government, not the voting machine companies, must pay for the testing and oversee it."

(2) “Voters should be told how testing is being done and the testers’ qualifications.”
(3) “[Rigorous standards] should spell out in detail how software and hardware are to be tested, and fix deficiencies computer experts have found.”

With regard to (1), the *Times* is incorrect when it states elsewhere in the editorial that “these labs are selected by the voting machine companies, not the government.” However, the labs had been selected by NASED, which is a private association of state election officials. Thus, it has been reasonable for NASED, as well as the labs themselves, to refuse to reveal the accreditation criteria and the testing criteria. While I know of no law that would require government to pay for the testing process of vendors’ products, the remainder of the *Times*’ recommendations are in agreement with HAVA.

Under HAVA Section 231, “the [Election Assistance] Commission shall provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories.” Further language of HAVA gives much responsibility to NIST in this area. Thus, certification and follow-on work is to be done by a public process, and TGDC must follow the law on revealing the results of government deliberations and decisions. TGDC needs to develop laboratory accreditation criteria and software testing methods in detail and should, upon their completion, submit them for public review and then, final publication as public documents.

5. <u>The Practicality of Testing for Software Correctness</u>

It is often stated by opponents of the use of DRE voting machines that it is theoretically impossible to assure the correctness of software. That is true, but on basis of theoretical impossibility, no bridge, dam or other large structure should ever be constructed. It can never be assured that the maximum stress beyond which the structure will fail will never occur. Engineering decisions on the strength and resilience of a structure to be built must be a trade-off between cost and some maximum expected stress. There is a concept called “due diligence,” that is, that the latest professional understanding of processes of construction and predictions of stresses are to be utilized. Nevertheless, if there are several levels of testing of voting software, we need a high-quality procedure that may cost a bit more, but provides a very high level of confidence.

The functions of vote-recording and counting are more like on-line, real-time processes than they are like Internet-connected multi-tasking systems. We need to absolutely prevent external connections to voting equipment that are unnecessary for the specific functions it performs. This is necessary to minimize complexity as well as assure security. We need to apply the type of testing procedures that are used by airplane and automobile manufacturers for their respective vehicle control systems. Planes and cars now contain programmed computer chips. How do Boeing and Ford test them? We need to know. If we really believe that software can never be assured to be correct, we should never fly or drive. One of the leading proponents of the impossibility of software correctness made that statement at NIST last December after flying in from California. All of our human brains are filled with these types of contradictions. Life is not a certainty and we cannot expect absolute certainty in any of the machines we use. We need to do the best we can with the best professional quality that we can find and pay for.

6. **Security, From Completed Testing to Use in Elections**

The transition of precious or dangerous materials from the custody of one organization to another is very often the subject of detailed administrative procedures. Think of hospitals and controlled substances. Think of nuclear materials and gold bars. Once testing has been completed on voting software, administrative procedures must be in place to assure the absence of tampering until the software is actually used in the elections for which it was designed. Cryptographic techniques that can assure that the sequence of bits in a long string have remained the same may be used, as well as "chain of custody" concepts. We must assure that the software that was tested for correctness is the same software that is to be used. The necessary procedures should be developed by the TGDC in cooperation with the states and local governments that will be using the software and will be responsible for its protection.

7. **Other Aspects of Security**

In the voting process, it is difficult to separate security from other aspects of integrity. For example, in 1975, I recommended that records of overvotes and undervotes be retained and reported. I have been informed recently that there are still local jurisdictions in which that procedure is not carried out. As in accounting, where double-entry bookkeeping has been standard for about a century, there needs to be cross-checking that distributes the total responses possible with each ballot to each category that could have been used by each voter. In voting, this cross-checking will produce a spreadsheet where the sum of the horizontal summations will equal the sum of the vertical summations. That is, for each contest, the total number of ballots cast multiplied by the number of legitimate votes cast per ballot should equal the sum of votes assigned to each candidate plus the number of overvotes plus the number of undervotes.

In DRE systems, this process is possible with the use of the "electronic ballot images" (EBIs) that are required to be implemented under the Federal standards that were issued in 1990 and 2002. I first proposed this concept in DRE systems in my 1988 report, pages 112 and 113, referring to EBIs as "voter-choice sets."

There are other facets of assurance of public confidence that I might discuss, but there number is to great for their presentation here. For example, in my 1975 report, Appendix B discussed the number of precincts needed to recounted based on the closeness of the contest. The adaptation of this process to non-ballot systems may require additional considerations. In addition, the viability of different methods of supplying a "voter-verified paper audit trail" needs evaluation. Recently, Richard Smolka's *Election Administration Reports* revealed that, in Nevada, with regard to the printed receipt, "most [voters] ignored this verification feature." If voters are not checking the receipt for correctness, then this receipt fails its purpose as an audit trail. The receipt is generated by the computer program. If voters are not reviewing it and approving it, it is not a document ballot; it is just another computer-based artifact.

Thank you for your attention.