U.S. Election Assistance Commission Voting Advocates Roundtable Discussion
Thursday, April 24th, 2008

Comments of Barbara Simons
Board member, Verified Voting Foundation

I want to thank the EAC for holding this round table and for inviting me to present the views of the Verified Voting Foundation.

It is critically important to the well being of our democracy that our elections have transparency and accountability, so that Americans trust the outcomes of those elections. The draft VVSG reflects an impressive effort to establish a framework for the design, manufacture, and, ultimately, deployment of voting systems that will have transparency, auditability, and accountability. Essential to these goals are the mandates for Software Independence (SI), Independent Voter-Verifiable Records (IVVR), integratability requirements, auditing support, and usability benchmarks.

While we fully support the goal of software independence through the use of IVVR, Verified Voting recognizes a qualitative distinction between an IVVR that a voter has marked – either physically or through the use of an assistive device – and an IVVR that a voter has been given the opportunity to review. Software independence is best achieved through the use of voter marked paper ballots.

We also applaud the inclusion of Open Ended Vulnerability Testing (OEVT), which has proven valuable in identifying security vulnerabilities in numerous reviews. While testing alone cannot ensure the accuracy and integrity of elections, testing plays a vital role in efforts to improve the administration of elections. We recognize, however, that there is a point of diminishing returns. At some point, the benefits of additional testing requirements should be weighed against the costs, which could include reduced choices of voting equipment available to election officials and voters, as well as longer delays in introducing improved equipment.

The limitations and costs of testing make the mandates for Software Independence and IVVRs even more imperative. Effective independent auditability is precisely what mitigates the inherent inadequacy of the testing and certification process, and we strongly urge the EAC to retain these TGDC recommendations.

Responses to Questions

1. *On October 7, 2005 the National Institute of Standards and Technology (NIST) held a "Risk Assessment Workshop" in order to evaluate threats to voting systems. The results of that workshop can be found at http://vote.nist.gov/threats/. In so doing NIST recognized the importance of evaluating threats when developing a secure voting system, but no formal risk assessment was developed. The EAC is now interested in learning how to best develop a risk*

assessment framework to provide context for evaluating the security implications of using various technologies in voting systems?

Because elections are messy, difficult, and complicated exercises, risk is inherent in the administration of elections. While an expectation of perfection is unrealistic, we expect systems and measures to reduce or limit the level of imperfection as much as possible. Since we are unlikely ever to have perfect, risk-free voting systems, we advocate strongly for reliability and for independent auditability of elections to safeguard against many acknowledged risks.

a. What are the essential elements of a risk assessment?

Any reasonable risk assessment must determine the possible threats and approaches that might be used to eliminate or mitigate those threats. It should start by addressing the following points:

1. What security properties are being assessed (e.g., election theft, vote stealing; detection of inaccuracy vs. correctability of inaccuracy)?
2. Who are the potential attackers and what are their capabilities? For election systems, this set should include insiders with legitimate access to the software and hardware (and designs thereof), in addition to voters, poll workers, election officials, etc.
3. What is a baseline set of possible attacks that must be defended against?
4. What are the defenses?
5. Explicitly, what assumptions are being made about procedures?
6. Can we quantify the various risks, and if so, how?

Systems being analyzed should also include systems with ADA accommodations, to include threats that are enabled through the accessibility interface.

We urge the EAC to engage the technical community in general, along with the TGDC and NIST (both of whom have expertise in this area) to define a more precise framework along the above lines.

b. How can the EAC best create a risk assessment that recognizes all possible risks and assesses the plausibility and nature of such risks?

It is impossible for the EAC to recognize all possible risks, let alone assess the plausibility and nature of the risks. There is no question, however, that some voting equipment will malfunction in every election. The cause of the malfunction – equipment failure, poll worker error, Acts of God, or malicious attack – is secondary to the inevitability that malfunctions will occur. Consequently, it is unacceptable to employ voting systems that cannot recover from such malfunctions. And it is important to require that voting systems produce information that can help diagnose problems and prevent their reoccurrence in the future.

However, once a set of threats has been identified, criteria for comparison can be defined, following the framework outlined above. For example, a system that permits a very small group of individuals to change the outcome of an election should be considered riskier than a system that would require many participants and would have a much greater chance of detection.

c. How do you evaluate what is an allowable level of risk?

The allowable level of risk should be set at what can be feasibly and cost-effectively achieved with the best available equipment and election practices. In our opinion, the risk can be minimized using paper based systems such as precinct-count optical scan with careful and transparent manual auditing of election results, and optimal procedures for maintaining the integrity of the paper ballots between the close of the polls and the last recount.

2. *How can innovative systems be evaluated for purposes of certification?*
   a. *How can we create a certification process for innovative systems that isn't a backdoor around the standard certification process but at the same time isn't so cost prohibitive and restrictive that it presents a barrier and a disincentive to prospective inventors and manufacturers?*

We oppose creating a process that is so restrictive that it becomes a barrier to new inventors and manufacturers. However, there are certain conditions that must be satisfied by any voting system, whether it falls within the innovative class or currently established categories. Such a system must be secure, accurate, reliable, and have good usability and accessibility. It must protect the voter's privacy, and it must be easy to audit.

In order to satisfy the above conditions, any new system must be software independent and be based on an easily auditable independent voter-verifiable record (IVVR), for example a voter-marked paper ballot. It must also satisfy the testing requirements of current voting systems, including the six points listed in the response to question 1. In addition, it is critical to have public disclosure of those aspects of the system that are the basis for the evaluation. The public should know enough to be able to check the work of the expert evaluators.

   b. Can a set of limited standards be created in order to make the path towards certification of innovative systems more clear? If so, how?

We are opposed to creating a limited set of standards for certifying innovative systems. The reason for the standards is to make our voting systems as secure, reliable, etc. as possible. These are points on which there should be no compromise.

3. *What is the value of the open-ended vulnerability testing model?*
   a. Are there any risks associated with this kind of testing?

Open-ended vulnerability testing (OEVT), which is generally referred to as "exploratory" or "red team testing," is necessary to try to detect unanticipated vulnerabilities and hidden malicious code. Exploratory testing is widely recognized as a dominant testing method in most testing regimes.

OEVT testing should counteract some of the limitations of checklist-based testing and give more transparency and assessment of the quality of the vendor's own software process. If OEVT reports are made public, if we see that it takes the vendor several tries to pass OEVT, and if in the first few tries the testers find significant flaws, then we may have reason to suspect that the vendors' internal software design, engineering, and testing processes are deficient. The assumption might then be that what OEVT found is only the tip of the iceberg, and that the equipment reliability score should be downgraded accordingly.

However, OEVT is only as good as the testers. Doing OEVT well takes very highly skilled, expert testers. Testing by less skilled testers should still uncover flaws, and hopefully it will weed out the most egregious flaws. To ensure against inadequate or mediocre testing and in order to have accountability and transparency of testing labs, there should be disclosure of all source code and all other technical materials that the testing labs produce. If the testing labs do an inadequate job, then independent parties will have the access needed to do such an independent analysis of the testing labs themselves. Ideally, such independent analysis will keep the testing labs "on their toes."

EAC officials and all state election officials should have the authority to order an OEVT any time that they have concerns about the security of a voting system. The vendor should be required to fix flaws uncovered by the OEVT.[1]

b. *What are the best ways to limit the cost of this kind of open ended non-scripted testing so that it can be useable within the EAC's testing program?*

Cost should not be traded off for security, usability, reliability, accuracy, or accessibility. Voting is a matter of national security, and it should be treated as such. Nevertheless, there is a point at which the cost of testing will discourage the development of new systems. One of the primary reasons that we strongly advocate for SI, quality IVVR, and independent auditability is the understanding that they can potentially reduce the need to rely on security testing, compared with software-dependent systems.

OEVT should be based on clear criteria along the lines of the six points listed in response to questions 1. The testing should be searching for violations of specified security properties and making sure that there are effective defenses against specified baseline attacks. The findings should be evaluated in terms of well-defined risk metrics, such as the "number of informed participants."[2] In order not to restrict the choices of voting systems further, the OEVT policy should strike a balance between system quality and expense and delay.

c. *If the EAC were to require OEVT how could it best be included into the EAC's Testing and Certification Program?*

OEVT should be treated the same way as other tests. Vendors should be required to repair any flaws found in voting systems via OEVT.

4. *Do methodologies exist to test voting system software so it can be reliably demonstrated to operate correctly?*

There are no testing methodologies that exist that would allow us to know with certainty that a voting system will operate correctly and securely. This unfortunate fact stems from a fundamental mathematical theorem that shows that it is impossible in general to answer even

[1] Some states rescind state certification when unacceptable flaws are uncovered. A non-permanent certification could be considered at the federal level also.

[2] See *The Machinery of Democracy: Protecting Elections in an Electronic World*, a report produced by the Brennan Center for Justice at NY School of Law.

such a simple question as whether or not a software program will eventually halt.[3] One doesn't have to resort to mathematics to observe that software vendors regularly post patches to their software, in some cases years after the software was released, in response to emerging or previously undetected flaws or threats.

a. *If testing to a thorough set of standards is not enough to demonstrate the reliability of the system, what else can be done to improve confidence in electronic voting systems?*

The best way to improve confidence in electronic voting systems is to institute statistically significant random manual post-election audits of voter-verified paper ballots. Timely, accurate post-election auditing in turn requires getting detailed vote tabulation results quickly after polls close in an open standard format for the media and the general public, as well as for those responsible for conducting election audits.

5. *Throughout the creation of its draft VVSG, the EAC's Technical Guidelines Development Committee struggled to balance the need for useable and accessible systems with the desire to create the most secure system possible.*
   a. *How can the EAC best strike a balance between these sometimes competing needs?*

A well-designed system can be usable and accessible, as well as secure. Problems have arisen because a) some voting systems have not been well-designed and b) in several cases security, accessibility, and/or usability have been added on after the system was built. Ideally, all of the important features of voting systems can and should be integrated into the design and development of the systems from the beginning.

However, we also have to acknowledge some limitations of current technology. Quoting from email from Noel Runyan:

> Absolutely complete independence can never be obtained for all voters. For example, currently many voters with severe motor impairments and many blind voters cannot independently sign their own names in the poll books, but this does not mean that they cannot have enough independence to assure privacy of their ballot choices during other parts of their voting experience.
>
> With near-term technology, we should be making sure the voter has independence where it is essential for assuring privacy of the voter's ballot choices. As a goal, we should strive for 100% of voters being able to be 100% independent in their voting, but be willing to settle in the near term for systems that may require that a few voters accept some assistance that does not compromise the privacy of their ballots.

b. What level of usability or accessibility could be sacrificed in order to gain additional security or vice versa?

We do not believe that aspects of usability and accessibility need to be sacrificed for security. As with other aspects of the VVSG, we need to avoid creating requirements that are not currently

[3] This is known as the Halting Problem. The theorem is the work of Alan Turing, a renown mathematician who, among other things, broke the German code in WWII.

feasible for paper ballot based systems. Quoting from Noel Runyan's written testimony before a recent EAC round table:

> As currently worded, the measures required in the draft VVSG for assuring that voters with disabilities can have personal independence and privacy in their verification of paper vote records takes several quantum leaps in technology development. The draft VVSG goes unreasonably far overboard in apparently requiring that paper record verification for voters with disabilities and alternative language needs must carry out advanced OCR, autonomous ballot parsing and format extraction, and translation of languages other than English.
>
> This seemingly desirable super-verification system for voters with disabilities would require software and therefore not be software independent.
>
> Writing a requirement like this into the VVSG is somewhat like requiring a similarly desirable goal of converting all of our energy generation to fusion power plants within four years.
>
> These requirements for complete personal independence in paper ballot record verification are so technologically far into the future and impractical in the near term that the effect of requiring them in the VVSG would be to simply ban the use of paper ballot records systems.

6. *Are there any changes to the VVSG, in either scope or depth, which would significantly reduce the cost (time and/or expense) of compliance without adversely affecting the integrity of the VVSG or the systems that are derived from its implementation?*
    a. *What needs to be added or removed from this document to strengthen it and the systems to be constructed to its specification?*

We have a few specific comments and suggestions.

1) The EAC should consider expanding the definition of "voting system" to include electronic poll books, especially when they interface with voting systems. Ideally, standards, testing (including testing under Election Day type conditions), and certification criteria should also be applied to ePollbooks.

2) Many current VVPAT systems used with DRE's make voter verification and auditing difficult. Although such systems are better than DRE's without any kind of independent voter-verified records (IVVR), the new 2007 VVSG should require individual paper ballot records that are durable, easy for voters to read and verify, and easy to audit. The most cost-effective, fail-safe technology today is still a paper ballot that voters mark directly and which can be scanned immediately to check for over-votes, under-votes, and other marking problems. For voters with special needs, including visual impairment and languages other than English, the best supplementary technology is a ballot-marking device capable of producing paper ballots that can be independently scanned for voter verification and error checking.

3) We recommend that digital scanners, which should be defined in the VVSG and distinguished from optical scanners, be required to use a format with an open standard, to facilitate audits. the VVSG should distinguish between optical scan marksense scanners

and what are commonly referred to as "digital scan". These newer scanner make a digital image of the voter marked ballot and then interpret than image for tabulation. Standards for the accuracy and reliability of the initial image capture should be established and the image should be created in a loseless open format unencumbered by proprietary issues.The digital image, which the voter is not given the opportunity to verify, should not be construed to serve as an IVVR. We will provide specific suggestions for inclusion in the VVSG before the end of the comment period.

4) In order to support interoperability, as well as timely and effective reporting of results and auditing, all voting system components (including both hardware and software) should be required to support input and output of data using a standard open XML format. A currently available option is the XML-based Election Markup Language (EML) developed by OASIS.[4] The use of a standard XML format will make it easier to disseminate election results quickly to the media and the general public, as well as to those responsible for conducting election audits.

5) A problem with testing to benchmarks is that the software may be designed specifically to perform well for those benchmarks, as opposed to performing well in general. Ideally, there should be a sufficiently large and diverse set of benchmarks as to mitigate against benchmark driven code.

6) It would be desirable for optical scanners to provide descriptive messages when reporting an overvote or an undervote, ideally in multiple languages.

7) Poll worker usability of systems should be more precisely specified, e.g. ease of setting up, weight limits, complexity, limited amount of training time needed, etc.

8) Usability testing should simulate environments that closely resemble voting places, e.g. crowded, poorly lit, noisy, overheated, inadequate seating, etc.

9) Similar simulations should be used for accessibility testing, with the additional requirement to include people with a wide variety of disabilities in the group testing the voting system.

10) The notion of failure rate included in the VVSG is not ideal. Simply lumping all “failures” together in computing the failure rate can be misleading. Some failures might be critical, while others could be very minor.

[4] EML has been developed by OASIS over the past seven years, and is now being considered for adoption as an ISO standard. Recommended by the Council of Europe in 2004, EML has been used in different ways in a number of elections around the world, most recently by the California Secretary of State's Office to report statewide and county totals from the February 5, 2008 presidential primary elections.