Election Officials Roundtable
Friday, April 25th, 2008

Testimony of Russ Ragsdale

First of all, I would like to thank the EAC for the opportunity to participate in this roundtable discussion. I appreciate their efforts in gathering input from a wide spectrum.

Having served Colorado as the local election official representative to the EAC's Standards Board since its inception, I have been introduced to many of the paradoxes and mysteries posed by developing such a set of guidelines as the VVSG. Should systems be made so secure and accessible that their development costs put them beyond most jurisdictions ability to procure? Or should we, in the name of fiscal responsibility, cut corners when it comes to ensuring the integrity of our elections? Are the threats to election systems that some would like to see the VVSG eliminate plausible? Are election officials being intransigent in order to protect investments?

The role of the EAC is not an enviable one. They are routinely pressed into a position of compromise. And compromise may lead to a set of rules that ensure neither integrity nor affordability.

We, as election officials, owe it to the voters of this country to listen, learn, and offer input whenever the opportunity arises. The VVSG is not just setting forth a list of system specifications; it is potentially setting the course for how we conduct elections in this country for many years to come.

1. *The VVSG has more than one audience, including vendors and VSTLs. Do you consider county and state election officials as one of the stakeholders in the VVSG and therefore one of the intended audiences?*
   a. If yes, is the document intelligible to you?
   b. If not, how could it be improved?

Of course. Election officials will play a key role in shaping legislation that will determine how their state utilizes the VVSG. Election officials will be responsible for acquiring voting systems designed to VVSG standards. And election officials will be responsible for justifying the costs of these systems to their constituents and educating them in their use.

a. The VVSG is by its very nature a technical document. Its primary purpose is to convey to manufacturers what is needed from their systems for certification and to VSTLs what is required of the testing regimen; a document written by technically-oriented people, for technically-oriented people. At the same time, its impacts must be understood by election officials for the reasons previously stated.

b. I had the opportunity to testify before the EAC at an August, 2005 public hearing in Denver regarding the 2005 VVSG. I recommended to the Commission that they consider developing a "VVSG for Dummies" specifically for elections administrators. That recommendation still stands.

During the development of this iteration of the VVSG, NASED and both the EAC Standards and Advisory Boards have requested of NIST that it produce a plain language companion document. This document would be used by the "non-technical" community to better understand the nuances of the VVSG. In response to these requests, a draft of this companion document was delivered to members of the Standards Board in December, 2007.

This companion document focuses on material that is new or significantly changed from the 2005 VVSG and therefore requires, to a certain extent, a working knowledge of the 2005 VVSG. Due to a number of reasons, among them being that it was developed quite rapidly and no system has yet been certified to its standards, a minority of election officials possess this type of familiarity with the 2005 VVSG.

As of yet, this companion document is in draft form only and has had a very limited release. I would recommend that the EAC revitalize this effort.

2. *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.*
    a. *What are the essential elements of a risk assessment?*
    b. *How can the EAC best create a risk assessment that recognizes all possible risks and assesses the plausibility and nature of such risks in an election environment?*
    c. *How do you evaluate what is an allowable level of risk?*

    a. I would not assume to be able to identify the elements of a risk assessment better than NIST could do. I would assume that they have been called upon to perform similar efforts or have the networking available to other agencies that have. With that said, one element that may be overlooked is the amount of resources or effort required to mitigate a specific threat. The use of a rating system, possibly as simple as a three-tier HIGH, MEDIUM, or LOW rating would be beneficial to help understand which threats require the most attention.

    b. The EAC must first fully understand and articulate the purpose of such a risk assessment. If the purpose is to assist in developing testing specifications for the VVSG it may look much different than if it is to be used to create a "users manual" for elections officials. Many risk mitigations involve in part, or in whole, procedures rather than built-in system protections. An example of this would be secure storage of equipment. A risk assessment may conclude that continual video surveillance is necessary to secure stored voting equipment but how would that translate to a testable VVSG requirement?

At the December, 2007 Standards Board meeting, a resolution (2007-08) was passed asking the EAC to remove all requirements from the VVSG that mandate procedures rather than system standards.

While a more holistic risk analysis may provide useful information to the entire elections community, caution must be taken before including its findings in the VVSG.

c. After the risk is identified, characteristics of the risk are determined.

- Number of votes at risk. Is the threat likely to be a one-vote effort such as an individual casting a ballot at a vote center and attempting to vote again at another location? Or is it an effort aimed at a large number of votes such as introducing malicious code in the election management software?
- Determine plausibility and likelihood. Will it take collusion among several elections staff or simply the efforts of a single pollworker? Will it require defeating several levels of security (i.e., camera surveillance, userid/password, tamper evident seals) or a simple change of a log record? Will it affect the outcome of an election in a predictable manner or simply cause mischief?
- Amount of resources required to mitigate the risk. This is essentially a cost benefit analysis. If I dedicate an additional staff person for 6 months, I can prevent someone using concentrated ultraviolet rays erasing 1 out every 10,000 optical ballot scan marks….

If the number of votes at risk is few coupled with a very high investment and a very low plausibility, it is probably an acceptable risk.

3. *Could you comment on the value of stability in the standard to your jurisdiction?*
   a. *Which is preferred, a standard with a short-shelf life that accommodates innovation and change or a stable standard that may discourage innovation, but creates longer certification lives of voting systems?*

I would argue that a standard with a short-shelf life does not accommodate or promote innovation. Rapidly changing standards may very well stifle innovation by creating the perception of high risk; what is certifiable today is obsolete tomorrow. Rather, a well-constructed standard that focuses on performance not design will foster innovation more effectively. A "stable standard," focused on performance rather than design should not discourage innovation.

4. *What is the value of the open-ended vulnerability testing (OEVT) model?*
   a. *Would the current OEVT requirement in the standard reduce or decrease voter confidence in your system?*
   b. *If the EAC were to require OEVT how could it best be included into the EAC's Testing and Certification Program?*

As technology solutions develop rapidly, so do technology threats. OEVT allows systems to be tested against "new and improved" threats that may not be contemplated in established VVSG tests. OEVT also allows skilled teams to explore further any indication of hidden flaws discovered during routine testing. But OEVT is subjective and carries with it a potentially hefty price; cost of development which translates to cost of product, and a dampening of innovation.

a. OEVT often involves testing to failure, meaning that testing is not complete until the system fails. Regardless of the logic behind this approach and regardless of how well a system resists failure, the resulting perception will be that the system is vulnerable therefore decreasing voter confidence. On the other hand, if a system survives OEVT without failure, it may create a false sense of security that the system is flawless. This may result in increased voter confidence but wrongly achieved.

b. OEVT should be recommended and encouraged during system development. But to require it within a certification program is probably not appropriate. It may best be used to determine how well a system has matured, but not as a pass/fail test. How do other technology certification programs address OEVT? Voting systems cannot be the first technology to face this issue.

5. *Would component testing (the ability to test and certify components as they are modified or added to an existing system) be beneficial to your jurisdiction?*

Comment [M1]: Good! This is an important question.

Certainly. And conversely, prohibiting component testing, or requiring end-to-end system testing, will adversely affect my jurisdiction.

Testing a complete system end-to-end to the next VVSG standards promises to be a time consuming, costly endeavor. Requiring a complete system test when only limited component modifications are made will discourage manufacturers from making any enhancements to their systems until a complete overhaul is warranted. This will delay or eliminate incremental enhancements.

As an example; in Colorado, many counties are wishing to switch to a paper ballot, central count election method. Their current system manufacturer does not yet offer a high speed ballot scanner. However, the manufacturer did submit such a scanner for EAC testing in early 2007, along with an entire system, but has yet to receive certification. It is doubtful that this device will be ready for service by the November, 2008 election not because of any technical shortcomings but because of the length of the testing and certification process for an entire system.

If a manufacturer decides to proceed with a total system certification in order to add a component, the cost of testing will more than likely be applied to the purchase price of the component possibly putting it beyond reach of many jurisdictions.

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 in order for it to meet what is needed from future voting systems?

b. How could the process of developing and vetting the VVSG be improved to ensure higher volume and higher quality input from election officials?

As was discussed in the response to question 4, if or how OEVT is to be implemented needs to be carefully examined. It has the potential to increase development and testing costs significantly while not guaranteeing a better product.

a. As was mentioned in the response to question 2 b, the Standards Board requested that the EAC remove all requirements from the VVSG that affect election officials' procedures. However, I believe it is well established that the integrity of an election requires far more than any measures an election system alone can provide. Election officials must be included in the equation.

   This leaves me conflicted. The VVSG must be focused on the behavior of the system but at the same time, how the system is to be used must be considered. Requiring a system to be as secure as possible on its own without consideration of physical and procedural measures will result in complex, expensive products affordable by a minority of jurisdictions. This same can be said about accessibility. For example; rather than redesigning a DRE to allow for wheelchair approach, simply placing the DRE on a table without deploying the DRE legs results in the desired level of accessibility. And the table has a multitude of uses. An oversimplification indeed, but illustrative.

   In Colorado, systems that were recently recertified all had accompanying conditions for use. Through testing, a system's potential shortcomings were documented. But rather than discarding and replacing the systems at the cost of millions of taxpayer dollars, procedural solutions were arrived at through conversations with users and industry experts. While this process came under criticism from all angles, much due to its rather ad hoc appearance, it may have revealed a possible approach for the EAC.

   What happened in Colorado was done in retrospect, certifying systems that were already in place. The VVSG looks to future development and deployment. But nonetheless, identifying a system's shortcomings and, if not catastrophic, developing common sense procedural conditions may provide an acceptably secure system while not breaking the local jurisdiction's bank.

b. Election officials are by nature social animals. They are known to gather at annual events, sometimes even more frequently. If the EAC would develop a "road show" VVSG presentation, this could be used as both an educational and an input gathering tool. Most election official conferences would welcome EAC speakers and if EAC resources were thin, if the presentation was modularized, it could be delivered by specific state representatives from the EAC's Standards or Advisory Boards.