WRITTEN TESTIMONY OF ALEC YASINSAC, PH.D.
DEPARTMENT OF COMPUTER SCIENCE
FLORIDA STATE UNIVERSITY
BEFORE THE
U. S. ELECTION ASSISTANCE COMMISSION
INTERDISCIPLINARY ROUNDTABLE
MAY 5, 2008

Thank you for the opportunity to participate in this roundtable today. My name is Alec Yasinsac. I am an associate professor of computer science, having joined the faculty at Florida State University in 1999 after serving twenty years in the United States Marine Corps. I am co-director and co-founder of the Security and Assurance in Information Technology (SAIT) Laboratory where I led several voting system security reviews for the state of Florida. I was recently appointed to become Professor and Dean of the School of Computer and Information Sciences at the University of South Alabama, a position that I will assume on June 1st, 2008.

My comments today relate primarily to the 2007 Voluntary Voting Systems Guide (VVSG) components associated with system and software security issues. Before I address the posted questions, there are three critical points relative to this roundtable that I believe must be addressed before VVSG adoption.

- Accuracy in the first count is pivotal to fair elections. Many involved in voting integrity issues advocate focusing predominantly upon strong audit mechanisms in the voting process, even at the expense of first count accuracy. Citizens deserve to have their votes counted accurately and reliably the first time. We must reject any paradigm that sacrifices first count accuracy for timeliness, auditability, efficiency, or any other real or perceived expediency.
- With all of their positive properties, audits add complexity to the voting process and present diverse opportunities for fraud in elections that are not well understood. It is critical that we carefully examine and mitigate the election threats during audits and recounts for every voting system.
- If voting system software development practices do not embrace high assurance techniques, it is a matter of when, not if, election faults will occur due to errant or malicious software faults.

1. **What specifically can be done with the proposed VVSG standards and with the certification testing procedures and infrastructure, to reduce the cost of the voting systems, without compromising core functions of the voting system?**

The single most important contribution that the VVSG can make to electronic voting systems is to require that voting system vendors employ mature system and software development processes. Open Ended Vulnerability Testing (OEVT) is only necessary because present voting systems are not currently engineered with sufficient rigor to reduce or mitigate the present and emerging threats. Requiring vendors to pass through nationally recognized process qualifications can maximize quality expectations while stabilizing, or minimizing, requisite development costs. Some CMMI[1]-qualified developers see CMMI practices as cost-saving in addition to its having a positive impact on product quality and consistency.

A second important characteristic of process maturity requirement is that it may reduce the risk of untimely vendor dissolution. While process maturity is not a guarantee of market share, like all types of maturity, process maturity takes time and commitment to develop. While not definitive, those two characteristics (time in business and commitment to quality) tend to be good success indicators.

2. **What specifically can be done with the proposed VVSG standards and certification testing procedures and infrastructure to reduce time-in-process of candidate systems?**

Incentivize quality development processes. While it is possible for poorly engineered systems to meet functional and security requirements, analyzing well-engineered systems is always easier and more efficient than doing so for their poorly engineered counterparts. Additionally, well-engineered systems will reduce both the necessity and the effort required for re-submission due to unacceptable faults or failure.

While these represent significant detailed improvements, possibly the greatest value is that requiring development process certification shifts much of the voting system quality assurance burden from the government onto the private sector where process maturity certification occurs.

Specifically, the VVSG should:

- Provide streamlined certification procedures for systems that were developed using development processes that are certified as being mature.

[1] Capability Maturity Model Integrated, see http://www.sei.cmu.edu/cmmi/

- Make the certification process for non-mature process development systems onerous and expensive. It should be clear to a developer that it is not in their best interest to submit a system for certification that has a low chance of success.
- Make re-examination expensive. If there is no, or low, developer resubmission cost, vendors will utilize the certification process as a beta test, thus driving up certification costs, extending the length of the certification pipeline, and essentially circumventing the total quality standard that the certification process aims to provide.
- Track vendor performance in the certification process and use previous performance to gauge rigor and cost for present-future certification requests.

Focusing on the product is the least effective and least efficient certification approach. Mature development processes produce effective systems. Certainly, it takes time to shift from a product approach to a process approach, but the VVSG can and should dictate the pace of that transition by considering the recommendations above and other associated approaches.

3. What specifically can be done to increase the efficiency and economy of efforts within the testing process at the federal, state, and local levels?

At the federal level, we recommended requiring that every vendor that submits voting systems for certification meet process maturity requirements. As we described earlier, we contend that this approach will reduce federal certification time and costs.

At state and local levels, decisions are now being made without critical information. It is essential that states have access to accurate, current data about voting systems performance history, known failures or faults, and whether remediation occurred. Full disclosure must be the gold standard in supporting elections official decisions in selecting voting system. Elections officials must know about previous failures in considered systems and also to see past vendor reliability and security performance.

Maybe more importantly, elections officials must receive timely “information-push” when faults are detected in operational voting systems. Voting system accuracy, reliability, and security are only accomplished through a strong combination of system features complemented by carefully controlled elections procedures. When systems vary from their expected properties, elections officials are best able to determine the associated risk and whether to abandon the faulty system or to correspondingly adjust Election Day procedures. State officials must have timely reports that allow them to act promptly and decisively to withdraw or suspend certification, execute correcting procedural directives, or circulate appropriate cautionary advisories.

The EAC presently acts as a voting system information clearinghouse, offering significant opportunity to meet the information needs at state and local levels, but the present effort does not go far enough. The voting infrastructure is critical to our nation's health. While we do not foresee the need for an expansive, controlling program, such as the Federal Aviation Administration's Airworthiness Directives[2], we believe the notification and documentation facilities in that program can serve as a model for voting system data.

To facilitate the voting system information flow we describe, we recommend that the VVSG be modified to require vendors to submit complete fault disclosure processes along with system certification requests. This plan should include fault reporting channels to the EAC and historical records of how they have exercised and modified their described process.

4. How important is the timing of the passage and implementation of the next iteration of the VVSG?

From a risk assessment standpoint, time is of the essence. The struggle to secure our elections infrastructure is not a conventional struggle and the enemy is not a conventional enemy. Rather, this enemy blends into the population[3], operates as independent cells, requires no special equipment or supplies, and needs very little funding or other support. Most importantly, they control the time and place of battle. Their prospects for success depend on surprise and unpredictability. They never act randomly, but they go to great lengths to ensure that their preliminary actions are uncorrelated with their intent.

For this reason, we cannot predict when an electronic attack on a major election will occur. However, it is my opinion that the question is when, not if, an attack on an electronic voting system will occur. The signals are clear: the attack surface is wide, the potential impact is great, and there are many capable foes that could benefit from such an attack.

The time to fix this critical infrastructure is now.

a. In an ideal world when would you choose to have the next iteration of the VVSG become effective?

Elections officials are best positioned to identify and exercise precedence operations for elections schedules, so we defer to them relative to operational considerations.

While time is of the essence, we must get this VVSG right. We applaud the EAC's efforts to systematically capture extensive, diverse feedback and to rigorously analyze collected input. The

[2] See http://rgl.faa.gov/Regulatory_and_Guidance_Library/rgAD.nsf/MainFrame?OpenFrameSet

[3] Inside the United States or abroad

only hope that we have of recognizing and planning for unstated outcomes or side-effects of these unprecedented policies is through rigorous debate, as is occurring in the present vetting process.

We also know that the need for rigor can be a tool for delay by groups with competing interests. We are confident that the EAC will recognize unnecessary delaying actions and ensure that the pace of the VVSG approval process will remain appropriately high to meet this critical need.

5. **How necessary is innovation in voting technology?**
    a. **How can the EAC's program and the VVSG address the desired level of innovation?**

Electoral accuracy in the United States is patently insufficient. Technological innovation is our only hope of overcoming the many pitfalls to capturing, tabulating, and reporting valid vote to the necessary accuracy level. In that sense, innovation is critical to the electoral process.

The innovation question is evident in the proposed related concepts of Software Independence (SI) and the Innovation Class. The VVSG mandates relying on software independent systems as the pivotal guide in ensuring election integrity, and there is a strong case that SI can facilitate elections security. Unfortunately, the VVSG only codifies one pathway to SI certification. That pathway is only suitable for systems founded on a physical vote record, known as the Independent Voter Verifiable Record (IVVR) systems.

Some would argue that the proposed Innovation Class is a second VVSG codified pathway to SI certification. However, there are no "requirements" in the VVSG that would allow any non-IVVR system to achieve SI certification through the Innovation Class.

Rather than being a pathway to SI certification, the Innovation Class is, in a sense, a license to develop a new SI certification pathway, with a complex and expensive licensing process. On one hand, this is a reasonable way to allow alternate certification paths without requiring modification to the VVSG for each new approach.

On the other hand, providing only one certification path limits flexibility. If IVVR is the only presently available technology that <u>can</u> provide the necessary voting system security, then the limitation may be justified, but it does not promote, and may stifle, innovation.

    b. **What are the possible sources of capital to reach the desired level of innovation i.e. from the vendor? From Congress? From private enterprise? From academia?**

6. **Every voting systems stakeholder shares risks with other stakeholders and experience risks unique to their constituents.**
    a. **What risks do you view as being shared?**
    b. **What risks do you view as being unique to your sector?**

c. **Has there been an adequate assessment of those risks?**

d. **In the absence of an adequate assessment of those risks, how can those risks be prioritized and mitigated?**

7. **How do you prioritize the features (i.e. security, accessibility, usability, reliability) of a voting system?** .

    a. **What are the best ways to strike a balance between these sometimes competing features?**

.