

Election Technology Council Comments on the Current Draft of the Voluntary Voting System Guidelines

The Election Technology Council has released its public comments to the current draft of the Voluntary Voting System Guidelines (VVSG) as proposed by the United States Election Assistance Commission. While the VVSG address shortcomings from earlier versions with the inclusion of clear performance benchmarks, it is important to place the current draft in its proper context and address our concerns as a reflection of our continuing commitment to ensure secure and accurate elections. Below is an overview of the key concerns the Election Technology Council has with the draft document:

Software Independence: *While voting is a unique environment for products, the potential mandate of software independence is unprecedented for any other industry. In fact, no clear consensus exists for what truly constitutes software independence from an academic standpoint. As defined, software independent voting systems would require the use of an optical-scan paper ballot or a voter verifiable paper trail component attached to the individual voting system. While the current membership of the Council currently offers software independent products, as defined within the draft VVSG, this requirement speaks to the overall pursuit of design requirements rather than performance requirements. Design requirements are prescriptive in nature and will limit the opportunity for future products to enter the marketplace which may be truly innovative in accommodating new security thresholds. Since the voting system certification framework is currently voluntary for the states, the VVSG must incorporate the greatest level of flexibility. Software Dependence is currently recognized for its role in “mission-critical” systems used within the Department of Defense and should be recognized as a continuing platform for voting systems.*

Innovation Class: *In an attempt to avoid a trap of requiring specific designs for voting systems, the VVSG includes an “Innovation Class” dedicated to the pursuit of future voting technologies which are software independent, but do not rely on paper. The use of the innovation class acknowledges that software independence is prescriptive based on the current technologies in the marketplace while at the same time attempting to deflect criticisms of the potential design mandates for the voting systems in the United States. It is short-sighted to believe that future innovations in voting systems could not be entirely software driven and incorporate the latest coding conventions and security models to meet the highest security level requirements.*

Open Ended-Vulnerability Testing: *The recommended use of Open-Ended Vulnerability Testing (OEVT) within the VVSG is laudable, but as drafted, it rests too much authority with the subjective viewpoint of a security reviewer rather than providing a testable measurement for voting system providers to use when designing their systems. As structured, the mechanism of OEVT embraces the need for a subjective reviewer and sets the bar so low that a mere description of a plausible security failure by a voting system will result in certification failure. OEVT is based on the tenet that only a complete open-ended security analysis will reveal*

security flaws, but this in itself is a misnomer as the security review will be contingent upon the quality of the reviewer and potentially violate the very principles which should be incorporated in establishing voting system standards.

While the EAC considers the draft VVSG and attempts to incorporate all of the public comments, it is important to note that the current draft of the VVSG is being considered during a time in which the EAC has yet to develop clear test methods for the 2002 Voluntary Voting System Standards or the 2005 Voluntary Voting System Guidelines. As it considers the newest draft and its implementation date, it should be pointed out that the current draft is not addressing all of the shortcomings present within the earlier versions, but represents a dramatic policy shift which will add new stress to the regulatory environment and the voluntary framework for the states that the VVSG is intended to serve.

David Beirne

Executive Director

May 2008

Chapter, Section, Line	Topic	Summary	Comments
2.4, Page 9 Intro	Software Independence	"All voting systems must be software independent in order to conform to the VVSG."	The notion of "software independence" as defined is a misnomer. The requirement for a software independent voting system implies that the election results are only verifiable upon the conclusion of a post-election audit. The logic incorporated into this section requires us to accept that no software can be relied upon for accuracy of election results. In turn, this requirement of software independence assumes that a post-election audit is required and is the only means to verify the accuracy of an election. In fact, it can be argued that the use of voter verifiable paper records attached to a DRE voting unit or optical-scan paper ballots are <u>only</u> software independent if a post election manual audit is incorporated. The intent is laudable, but fails in its logic unless there is an additional pursuit for developing assurance tools to verify the use of software for reporting of election results. Assurance tools can be developed for both software dependent and software independent systems and so the overall recommendation would be for the continuing use of two classifications of voting systems, both software independent and software dependent systems as included within the 2005 VVSG.
2.4, Page 9 Intro	Independent voter-verifiable records (IVVR)	All voting systems must include an IVVR vote-capture device, that is, a vote-capture device that uses independent voter-verifiable records (IVVR)	Although the IVVR does not have to be paper-based, current technology in the market place is all paper-based; therefore, this section is too prescriptive. Maintaining a dual process for software independent and software dependent systems will provide greater flexibility within the marketplace and will permit the users to determine the best platform for their needs. The following phrase, "IVVR relies on voter-verification, that is, the voter must verify that the electronic record is being captured correctly by examining a copy that is maintained independently of the voting system's software." This description is incorrect. There is no way for a voter to verify, through the use of a software independent record, the performance of the electronic record being generated. The IVVR in this instance is serving as its own auditing record, but its existence alone provides no level of assurance on the performance of the software. The performance of the software will continue to rely upon the use of software assurance tools.
2.4, page 11		"Technologies in the innovation class must meet the relevant requirements of the VVSG as well as further the general goals of holding fair, accurate, transparent, secure, accessible, timely, and verifiable elections."	The context of the word "timely" needs to be clarified or stricken. It is impossible for the reader to know if this is reference timely tabulation or processing during the actual voting process.
2.4.2, Page 10-11, Intro	The Innovation Class	The only current method to establish an IVVR system is through the use of paper, the Innovation class is intended to permit further development of IVVR systems not in existence; Provides for a review panel process, separate from the VVSG conformance process, who will review innovation class submissions and make recommendations as to their conformance to the	This review panel process needs to be clearly defined or simply include current EAC model with the use of the TGDC, Standards Board, and Board of Advisors. Since the EAC is not a rule-making agency, no variant procedure should be codified with the inclusion of a separate review panel unless specifically authorized or at such time the EAC becomes a rule-making agency.

		VVSG	
2.5, Page 11, Intro	Open-Ended Vulnerability Testing	Provides for open-ended vulnerability testing (OEVT) to discover architecture, design, and implementation flaws which may otherwise remain undetected; OEVT “relies heavily on the experience and expertise of OEVT members, their knowledge of the system, its component devices and associated vulnerabilities;	The use of OEVT is laudable from the standpoint of attempting to increase security levels, but multiple problems exist for a voting system provider to design a system to meet security thresholds in which the thresholds are undefined and subjective. This section is too ambiguous. Although assurances have been given that the OEVT will not have “fail” authority, this does appear to be the case especially in light of the discussion in Part III, Section 5.
Part I, Equipment Requirements			
1.1.3, Page 2, Ch. 1	Security Requirements	Concept of independent verification defined in 2005 VVSG has been expanded to include software independence;	Independent verification remains a more accurate description for the role and function of the IVVR as it can not, by itself, provide an assessment for software performance.
1.1.4, page 3, Ch. 1	Epollbooks and ballot activation	New requirements affecting epollbooks have been added to protect and integrity and privacy of ballot activation and credential information and to ensure records on epollbooks and voting machines cannot be aggregated to violate secrecy of the ballot; various requirements will also address network security	The inclusion of epollbooks within the VVSG is further evidence of the need to include industry representation within the development of the VVSG as many epollbook providers are not currently subject to voting system certification. While the intent is clear, epollbooks are an evolving field of products which operate differently from one another and may have no direct relationship with a voting system. This approach to epollbooks needs to be closely scrutinized as it may portend a jump for the EAC to begin regulating other products "deemed" to be part of the overall voting system.
2.7, page 20, Ch. 2	Software Independence	Software independence means that “an undetected error or fault in the voting system’s software is not capable of causing an undetectable change in election results	Removes 2005 VVSG classifications for two types of systems, software dependent and those that are software independent. This essentially mandates a VVPAT as an IVVR solution for any state who stipulates a requirement for “2009 VVSG” compliance until such time that products are submitted for certification under the “Innovation Class”. Public comments from EAC Commissioners continue to point to the application of this version of VVSG to new voting systems in the future; however, a state that chooses to comply with this VVSG must incorporate a paper trail. This is too prescriptive and does not recognize the voluntary framework.
2.7, page 20, Ch. 2	Software Independence		The use of an optical scan ballot or Voter Verifiable Paper Record (VVPR) does not make a voting system software independent unless the intent is to require a 100% audit of the paper records after each election or for the election’s initial count. The use of an optical scan ballot or vvpr should be only be used for purposes of providing an independent voter verifiable record, not software independence.
2.7.1-A, page 21, Ch. 2	IVVR, software independence		Strike this section. If the desire is to require software independence, you have required the system performance. Section 2.7.1.-A speaks to the design of voting systems and speaks to it falsely.

2.7.1-B, page 21, Ch. 2	IVVR, requires IVVR vote-capture device	In a voting system of the IVVR class, every vote-capture device must be an IVVR vote-capture device	Under current technologies, every DRE system would have to have a VVPAT unless a future system is submitted under the innovation class. This is too prescriptive of a requirement and speaks to this new draft of the VVSG focusing on the design of voting systems rather than the performance.
2.7.2, page 21, Ch. 2	Innovation class submissions	Typo: "Technologies in the innovation class must sufficiently <u>differ</u> from other technologies..."	Grammatical correction
2.7.2, page 22, Ch. 2	Innovation class submissions	Provides for a process through which a reasonable case must be made that the system does not represent excessive "logistical complexities" or a reasonable case must be made that the new technology does not represent an excessive burden on election administration. Provides for a separate review panel process (undefined) for the consideration of innovation class submissions;	The innovation class review panel process is undefined-the EAC process should be strictly adhered to as provided under federal law; The VSTL should have a clear set of basic criteria for considering submittals under the innovation class submissions; Section 2.7.2 needs to be aggressively reworked as it is too ambiguous; If all references to IVVR compliance in the form of an optical-scan ballot or VVPR are removed, the innovation class subset becomes unnecessary.
3.2.1.1, page 29, Ch. 3	Overall performance metrics	Establishes various benchmarks for the usability of a voting system as a whole including Total Completion Score, Perfect Ballot Index, Voter Inclusion Index, Average Voting Session Time, and Average Voter Confidence	Average Voter Confidence is a purely subjective criterion and should be stricken from the listing of performance metrics; It should be used only for purposes of validating the usability benchmarks. Since it is a subjective measurement, it should be only used for validation and internal purposes or reporting back to the applicant. It should not be used for public consumption as it is uncontrolled and speaks to the need for the EAC to focus on performance, not subjective impressions.
3.2.1.2-A, page 31, Ch. 3	Manufacturer testing- Usability testing	Manufacturer is required to conduct summative usability tests on the voting system using individuals who are representative of the general population and shall report the results;	I would suggest defining "individuals who are representative of the general population."
3.2.2.1-D; page 33, Ch. 3	Functional capabilities- Ballot editing per contest	The VEBD (Voter editable Ballot Device) shall allow the voter to change a vote within a contest before advancing to the next contest	From a usability standpoint, the forward advance of a voting system can reduce ballot errors and speed ballot efficiency; This requirement should be stricken or further reviewed before incorporated.
3.2.8.1-C.2, Page 53, Ch. 3	Usability for poll workers- Usability at the polling place	Documentation provided SHALL be in a format suitable for practical use in the polling place	Are pollworker training manuals also subject to the certification process? Is a VSTL qualified to make a determination on the usability of pollworker training materials? This clause appears to be subjective and should be either stricken or changed to a recommendation rather than a requirement.
3.3.1.-E, Page 57, Ch. 3	Disability Requirements- Accessibility of paper-based vote verification	If a paper record is generated, the system SHALL provide a means to ensure that the verification record is accessible to all voters with disabilities	This section needs to be reconciled with Section 4.4.1.-A "Direct verification by voters" which appears to acknowledge that not all voters with disabilities will be able to verify the contents of the software independent record which is why there must be observational testing performed and also Section 4.2.4 (second paragraph) which states that the same software base can be used to generate the IVVR and read it back.

3.3.2-D, page 60, Ch. 3	Disability requirements- Synchronized audio and video	Voting station SHALL provide a synchronized audio output to convey the same information as that which is displayed on the screen. The system SHALL allow the voter to switch among the three modes (synchronized audio/video, video-only, or audio-only) throughout the voting session	Throughout Section 3, the focus has been on greater voter flexibility/convenience to “toggle” between various settings. Has an analysis been conducted to assess the usability of a voting system when it comes to the voter’s experience and the use of such mechanisms?
4.2	Security and Audit Architecture Requirements		This section exposes the inherent disconnect between software independence and the use of an IVVR. Software independence is only achieved in conjunction with a review of the IVVR compared to the electronic record. Although specific mention is made of the role of a post election recount/audit as not subject to the jurisdiction of the VVSG, the intent is clear and could be construed as intrusive into state election administration requirements. What other purpose is there for this section which ensures “that IVVR” voting systems produce records that are capable of being used in independent audits” if an independent audit isn’t also required?
4.2.1	Pollbook Audit		Pollbook auditing is not a traditional means of verifying the accuracy of voting machine performance, but rather the accuracy of local procedures in the polling place when issuing ballots to voters based on their assigned ballot style. This section should be stricken as it is not relevant to the performance of the voting system itself.
4.2.1-A	Support for pollbook audit		No voting system can support a secure pollbook audit which can detect differences in ballot counts between the pollbooks and the vote-capture devices unless a provider offers such a comprehensive solution. The use of a pollbook audit does not block threats to voting systems such as the insertion of additional votes on voting systems. This may be used as a detection tool to verify the frequency of ballot styles issued from the pollbook versus those recorded on the voting system, but this is not a secure method and is often dependent upon local election administration procedures. This section should be stricken.
4.2.3	Ballot count and vote total audit		The use of the term “election management system” here may be better termed as “vote tabulation software”. Local users often use election management system to reflect a separate platform used to track all aspects of the election process, not necessarily related to the voting system.
4.2.4	Additional behavior to support auditing for accessible IVVR voting systems		In the fourth paragraph, “Election procedures must actually ensure that sufficient numbers of voters use the accessible IVVR voting system in this way to ensure that the audio feedback matches the IVVR records.” The VVSG should not contain any language that potentially prescribes election administration procedures. In addition, the description of observational testing goes beyond the performance requirements of voting systems and is indicative of local election administration procedures.

7.3.1	Logic and accuracy testing		Strike "It is not a defense against fraud." This is a subjective statement and should be stricken and is not relevant to the section.
7.5.7	Procedures required for correct system functioning		This entire section is not relevant to the VVSG and should be stricken and reflects general statements attempting to intrude upon election administration procedures.
Part III, Testing Requirements			
5.4	Open Ended Vulnerability Testing		OEVT is laudable, but difficult to incorporate into voting system design features. It is, by definition, subjective and undefined resulting in a security threshold that is difficult, if not impossible, to design for. Given the fact that the current dynamic for the industry is the financing of the voting system certification, no provider wishes to submit a product through an expensive process to have it fail based on a subjective standard that is not repeatable. This security process should be renamed and should incorporate clear security benchmarks that are broad in scope, but clear in their performance requirement.
5.4.2.-A	OEVT resources and level of effort		No security model should incorporate unfettered access which is granted within the VVSG as written in this section. If the certification process is effective, the security protocols specified within the VVSG will be incorporated. At this point the question should be whether, in a real-world exercise, the system performs as it should. If an absolute standard is unreachable, then the goal should be the highest possible confidence level.
5.4.2.G	OEVT level of effort-commitment of resources		Permitting 12 weeks of unfettered access is not a demonstration of security; it is a demonstration of deconstruction and far exceeds any potential for access in an election environment. This is especially true given the fact that an election environment is typically 8 weeks once the ballot definition process has begun.
5.4.4-A	OEVT fail criteria		Despite assurances from NIST officials that the OEVT would not result in a "failing" mark, this section speaks to a troublesome feature of the new VVSG. The fail criteria speak to the redundant nature of the OEVT as it does not consider the role of the VSTL itself during this process.
5.4.4-C	OEVT fail criteria-critical flaws		This section should be stricken as it is too permissive. The OEVT is essentially saying that the security of a voting system doesn't actually have to be penetrated, only a "plausible description" of how the penetration would occur. The bar for failing a voting system has been set low that the OEVT will remain as the final arbiter for the certification of a voting system based on a subjective review and one that only requires a description of events that may cast doubt on the system's security.