In the Matter of	**)**	
	)	
TGDC 2007 draft revision	**)**	
of the	**)**	**US Election Assistance Commission**
Voluntary Voting System Guidelines	**)**	**Public Review & Comment Process**
	)	

TESTIMONY
CONCERNING
THE TGDC 2007 DRAFT REVISION
OF THE
VOLUNTARY VOTING SYSTEM GUIDELINES

I would like to thank the US Election Assistance Commission (the Commission) for this opportunity to provide testimony regarding the 2007 draft revision of the Voluntary Voting System Guidelines (draft VVSG 2007).

The views presented are my individual, professional opinion. They do not represent the views of any other person or entity.

Given the importance of the issue before the Commission I will be direct and even blunt with the objective of being clear in this communication. Reality almost always is mixed with countervailing factors. For brevity and clarity I will primarily give a high level assessment with the hope that the primary message will not be lost in the discussion of the many factors and details involved.

I. General Evaluation

The draft VVSG 2007 is poorly suited to its purpose and almost certain to do more harm than good

As drafted the document will do significant harm to the security, reliability and accuracy of US elections. Of perhaps even greater significance is the fact that the document fails to capture the positive opportunity that a general revision of the VVSG offers.

In many ways the draft VVSG 2007 can be compared to the space shuttle challenger in 1986 on the launch pad in Florida on an unusually cold morning. A terrible and avoidable disaster is about to happen. Many fine, well-intended, hard working, intelligent, even brilliant people have worked on it. Many pieces are well designed and fully capable of serving their intended purpose. However, there is this 'O' ring and its failure will lead to a national disaster.

The foundational flaw in the document is the separation of the voting system from the election process. The document does not treat the voting system, meaning voting equipment, as part of the larger election process. The document simultaneously fails to recognize that it is a component in a certification and conformity assessment process. This larger conformity assessment process seeks to assure that the voting system meets its specifications in the field, when used in elections. The VVSG is one component in this process that certifies voting systems and then monitors its performance in elections, responding to deficiencies as identified.

The primary goal is to increase the security, reliability, usability and accuracy of US elections. In treating the voting system in isolation the draft VVSG 2007 not only fails to do this but actually appears to reduce security, reliability, usability and accuracy of US elections. It does so for at least the following reasons:

1. It adds requirements without an analysis of the need for those requirements.
2. It fails to address issues where experience in elections has amply demonstrated that changes are needed.
3. It continues the discredited practice of writing technically vague and ambiguous requirements unsupported by laboratory grade test methods.
4. In some cases it modifies requirements without any evidence that there is a problem with current requirements.
5. It fails to analyze the potential for unintended consequences or the impact of the changes it makes on either the certification and conformity assessment system or US elections.

II. The draft VVSG 2007 was developed without a failure mode effects analysis

After some of its early disasters NASA invested heavily in developing a structured approach to analyzing the effects of failures in systems and using that analysis to develop systems that had redundant safeguards, were fault tolerant and when failures did occur they produced small consequences. Failure Modes Effects Analysis (FMEA) has come into wide use in many fields and is standard engineering practice when high reliability, accuracy and fault tolerance are needed in systems.

The TGDC should have based its work on an FMEA analysis of both the US election system and the certification and conformity assessment system. It was not developed in that manner but rather treated the VVSG and voting equipment in an insular fashion, out of the context of their use. By doing so it simultaneously fails to bring benefit where it is needed, would pull resources from areas that are already resource limited and is negatively disruptive to the overall process of voting system certification.

III. The draft VVSG 2007 fails to improve election security or reliability

Elections bring together people, administrative procedures and equipment. Together the people, process and equipment form a system. The goal should be to find the best combination to achieve secure, reliable and accurate elections.

People counting paper ballots has a long history with well documented problems. People have one of the highest rates of inaccuracy. Especially tired people tend to make a lot of mistakes. Defrauding elections using paper ballots is well understood and documented. Ballots can be destroyed, substituted or added. Almost all of the problems experienced in US elections are the result of compounding human error.

The classic way to reduce human error is to introduce automation. So in the election system voting equipment was introduced to address the historic problems of human error and

potential for election tampering. However, voting systems, like all automation, have their own vulnerabilities. Further, when automated systems fail or are corrupted they can fail in dramatic ways. The challenge therefore is to find the optimum way to use both automation and human's using well designed process so that they provide checks and balances.

Conceptually there are three major factors to be balanced in elections. There are people and procedures, voting systems and automated forensics and auditing. Automated forensics is not as commonly discussed but it is perhaps the area offering the biggest potential benefit to the election system. It is quite possible to introduce equipment and audit procedures that monitor and detect any failures of the voting equipment. Checking of digital signatures, HASH codes, is one example of automated forensics that is being increasingly used to improve election security.

Commendably the draft VVSG 2007 does address improving election audits. However, it falls far short of the potential offered. The document requires that voting equipment support the ability to audit elections but fails to fully articulate what the features of such an audit would be and as a result it does not provide the amount of support or support in the places where it is most needed. While automated forensics and improved election audits offer great promise, like people and voting systems, they have their own problems and potential for failure or corruption. Election audit tools have the potential themselves to be an attack vector. Forensic tools themselves need to be specified and safeguarded to assure they deliver their potential benefit and are safeguarded against misuse.

The TGDC could have started its work by analyzing the current state of US election. By developing an understanding of how people, processes, voting systems, automated forensics and election audits are currently performed areas for improvement would have been identified. Where improvements in the equipment would bring increased total system security, reliability or accuracy it could then have been implemented with good results. Unfortunately the TGDC did not pursue its work in this way.

An example of the consequence of this failure can be seen in the requirement proposed for software independence. Taken in isolation software independence seems a laudable goal. However, the question needs to be asked, "If elections are software independent, what are they dependent on?" The answer quite obviously is elections become much more dependent on people and paper. People and paper have some of the highest error rates and history of fraud. The draft VVSG 2007 could have sought to simultaneously reduce dependence on people and paper AND software. The third element of automated forensics and system audits could have been brought more to bear. In turn the vulnerability of those elements would need to be guarded by providing specification and safeguards for them. Unfortunately such a total system design was not pursued.

IV. The draft VVSG 2007 will dramatically raise the cost of certification

The following table presents the testable requirements in the current draft as compared to the 2002 Voting System Standards and the current version of the VVSG, the 2005 VVSG:1

Testable Requirements		
Document	**Total Testable Requirements**	**Change from Prior Version**
2002 VSS	**805**	
2005 VVSG	**921**	**116**
draft VVSG 2007	**1173**	**252**

The significance of the change introduced by the draft VVSG 2007 is even more dramatic when the amount of commonality with prior versions is analyzed. Of the 1173 requirements in the draft VVSG 2007 627, 53.5% are either entirely new. An additional 69, 5.9% are substantially modified or expanded from previous versions. Only 477, 40.6%, continue substantially unchanged.

1 The number of testable requirements for the 2002 VSS and the 2005 VVSG was developed by identifying each item in the respective standard which would require a test or evaluation. In some cases requirements group several testable items, for example when a list of required features or attributes is given. Because each required feature or attribute requires an evaluation and assessment it is counted as a separate testable item.

For the draft VVSG 2007 the process was somewhat different. Only the identified requirements, marked by arrows in the draft, were counted. If the count of the testable requirements in the draft VVSG 2007 were performed using the same methodology it would increase, perhaps dramatically.

One effect of this level of change is to dramatically increase the cost of certification, both in terms of dollars and schedule. It has been estimated that certification costs to the 1990 VSS standard cost approximately $30,000 to run all the tests once and that the average company paid approximately $100,000 to $250,000 to qualify a system.[2] Costs to qualify a system to the 2002 VSS appear to be in the $1,000,000 to $2,000,000 range. The draft VVSG 2007 appears to increase that cost by 2 to 4 times, to somewhere in the range of $2,000,000 to $6,000,000. At that cost level a number of unintended consequences will arise. It is quite possible that some companies will exit the business in favor of more certain business opportunities. The cost of system certification will create a formidable barrier to entry for new companies. The likelihood of new companies entered this field will be materially reduced. Fewer systems will be certified and certified systems will be updated and recertified less frequently. That will mean that needed changes will be slower in becoming available. It will also mean that those involved in the certification process will become 'rusty' as they have fewer systems to test and gain experience and skill on.

II. The requirements are vague, ambiguous and confusing

The draft VVSG 2007 continues the discredited practice of writing vague and ambiguous requirements connected to even more poorly defined test methods. The result is a technically confusing document that is difficult to implement. The lack of technical precision and specificity in the testing methodology almost guarantees a wide variation among the VSTL's in how requirements are interpreted and testing is conducted.

When reading a large percentage of the requirements from the viewpoint of a test engineer responsible for evaluating a voting system, a VSTL engineer, a number of questions demand answers. The largest and most frequent questions are:

---

2 These estimates were obtained in personal conversations with ITA staff during the time when the 1990 standard was in force.

1. Exactly what am I supposed to do to check the system for compliance to this requirement?
2. At what point does the system go from passing to failing the requirement?
3. How could I fail a system that technically meets the requirement but does so in a very poor quality way that falls far short of the clear intent of the requirement?

Happily, this is an addressable point. A review of the draft by the engineers who will be responsible for using it could identify the questions they will have to answer when making an evaluation. Answering those questions in the final version of the standard would do much to assure that all VSTL's perform substantially the same evaluation and set the pass/fail criteria at the same place.

III. The draft VVSG 2007 makes the NIST NVLAP very difficult.

The vague and ambiguous way in which test requirements are given makes the NIST NVLAP laboratory accreditation process extremely difficult. NIST NVLAP has been charged with assessing and recommending VSTL's for accreditation. To perform its function the NIST NVLAP program assesses laboratories to ISO 17025, the international laboratory accreditation standard. That standard has two major parts, laboratory management requirements and technical requirements. The laboratory management requirements are consistent across many technical domains and assure that a laboratory has the procedures and quality process to produce a consistent work product. Technical requirements are guided by the standards used for the specific technical area the lab is being assessed for. In the case of the VSTL's they are assessed for their technical ability to test a system to the VVSG.

The problem is that the draft VVSG 2007 is vague and only provides the most abstract guidance on how the VSTL's are to perform their function. A consequence is that a NVLAP assessor would have the most difficult time defending a negative finding against a VSTL.

As an example consider the following requirements in the draft VVSG 2007:

4.2.1-A.1 Records and reports for pollbook audit

Vote-capture devices, activation devices, and tabulators SHALL support production and retention of records and reports that support the pollbook audit.

Applies to: Vote-capture device, Tabulator, Activation device

Test Reference: Part 3:5.2 "Functional Testing", 5.3 "Benchmarks"

and

4.2.2-A IVVR, support for hand audit

The voting system SHALL support a hand audit of IVVRs that can detect differences between the IVVR and the electronic CVR.

Applies to: Voting system

Test Reference: Part 3:5.2 "Functional Testing", 5.3 "Benchmarks"

First note that exactly the same test reference is provided for these two very different requirements. Part 3:5.2 "Functional Testing" is the test reference for a number of other requirements, for example:

4.3.1-A All records capable of being exported

The voting system SHALL provide the capability to export its electronic records to files.

Applies to: Voting system

Test Reference: Part 3:5.2 "Functional Testing"

The problem becomes evident when considering the challenge this presents to the test engineer or to the NVLAP assessor evaluating a VSTL. First, exactly what should the engineer check? Exactly what is the line below which the evaluation is deficient? For requirement 4.2.1-A1, how should the engineer evaluate "production and retention of records and reports"? If a VSTL checks that the system produces and retains 2 records and 2 reports on what basis would a NVLAP assessor cite that as deficient? The test engineer is given no guidance on what kinds of records and reports are to be produced and retained. What if the reports are very confusing and

difficult to understand, on what basis would the VSTL fail the system? The system meets the requirement, at least one interpretation of the requirement.

For requirement 4.2.2, "The voting system SHALL support a hand audit of IVVRs that can detect differences between the IVVR and the electronic CVR.", exactly what is the test engineer to check and at exactly what point does a system fail to meet this requirement? Suppose a test engineer inserts one difference in one CVR spends three hours analyzing the IVVR and CVR and is able to detect the difference. Does the system meet the requirement? Is the evaluation acceptable? If comparing a IVVR to a CVR takes three hours per vote on what basis would a system be failed? However, clearly the intent of the requirement would not be served. If a VSTL only checks one record and one difference then it is unknown if differences in other locations would be detected. However, the NVLAP assessor would be hard pressed to sustain a deficiency.

The point being made is that the VVSG is a component in the certification process, as is NVLAP laboratory assessment. These processes need to support each other and assure that the goals of the certification program are achieved and that ultimately elections are improved.

IV. No threat assessment, risk analysis or protection profile is developed to guide security requirements.

Per the Common Criteria and other well recognized approaches to security evaluation and planning start the process with a systematic threat assessment. Following identification of all identifiable threats a risk analysis evaluates the probability of each threat being exploited. From these a protection profile identifies the threats that a system is required to protect against. For an election system a division between protections provided by the voting equipment and those provided by election procedures is needed. In many cases, a defense-in-depth would have protections at both levels. Certainly a protection profile should assure that a protection is provided on at least one level.

The lack of a threat model means that it is not known if the security requirements provide a complete protection of the system. It is also not known if an equivalent level of security is provided for the system. Some requirements may provide much more security at points but there may be little or no security provided at other, equally important points.

V. Differing security and privacy situations in voting systems are not recognized or treated appropriately.

In a voting system there are two fundamentally different situations, the time when the voter and vote can be linked and then the time when the vote is annonomous. The following diagram contains these two situations but fails to recognize them or their implications:

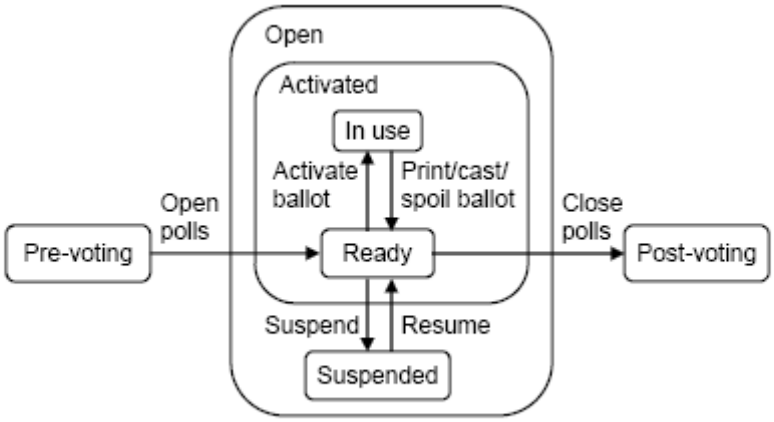


Figure 8-9 Vote-capture device states

The first situation takes place when the voter is in the voting booth casting a ballot. At this point the privacy of the voter must be protected and nothing may be done that will link the identity of the voter to the cast vote record. The security measures that are applied must protect the privacy of the voter. This requirement precludes the use of many effective security and audit process. To secure the voting situation other security mechanisms must be used.

The second situation occurs outside the voting process. This situation exists both before the voter enters the voting booth and after the vote is cast and separated from the voter, e.g. mixed with other ballots in the ballot box. In the second situation many security and audit

measures can be implemented that would be prohibited when the information could link the voter to the cast vote record. These security and audit mechanisms can and should be applied once the vote is separated from the identity of the voter. There should be a clear, traceable link between every vote in every ballot box to the final total and every vote in the final total should come from a known and valid source.

By failing to recognize these two different situations security requirements are not developed to maximize the security of each situation.

VI. Recommendations – The VVSG should be revised using as a guiding principle the improvement of elections by optimizing the combination of election administration and voting equipment

If the primary criticism, that the draft VVSG 2007 does not treat the voting system as part of the larger election process, is accepted, its remedy would be to revise the draft with a goal of finding the optimal combination of equipment specification and election administration best practices. The VVSG in turn should be revised to maximally contribute to the certification process and its contents seek to specify voting systems such that they contribute optimally to elections. The recommendations which follow will provide more details on how these two goals might be achieved.

VII. Recommendations – A rigorous failure modes effects analysis informed by elections experience should guide the revision of the VVSG

A rigorous failure modes effects analysis should guide the revision of the VVSG. This analysis must be heavily informed by experience in actual elections. In this field there are two kinds of problems. There are problems that have been experienced in elections. Some of these are routinely experienced in every election. Others occur rarely but have occurred and are well documented. This experience base can be analyzed as to what the root causes are and when those causes trace back to deficiencies in the voting equipment then improvements can be

considered. The other kind of problem is those which are hypothetically possible. Thankfully US elections have been spared the experience of many problems which hypothetically could have occurred. As a general statement, experienced problems tend to be less dramatic and have smaller consequences which hypothetical problems that are advanced tend to be more dramatic, often postulating disastrous consequences. Both kinds of problems need to be considered. The challenge is to find the right balance between dealing with experienced problems and hypothetical problems.

For many issues that have been experienced the question should be asked, "Is there a current requirement in the VSS 2002 or VVSG 2005 which should have prevented this failure?" To date the author's experience has been that in the overwhelming majority of cases the answer is "YES", there is a requirement in the current standards that should have prevented a flaw from reaching deployment. That raises a second question, "How did the flawed system get through certification?" The answer usually traces to deficiencies in the test methods used to evaluate the current requirements. If this is the case why are we writing new requirements? The current requirements by and large appear to be adequate. There is some room for improvement to be sure. However, the problems seem to be with the test methods and procedures used to evaluate systems against the current requirements.

The preceding discussion gives an example, applied to the VVSG itself of a failure mode effects analysis. Currently in deployment there are only systems certified to the VSS 1990 or 2002 requirements. The majority of field problems trace back to inadequate test methods rather than deficient requirements. The failure mode then is specifications that are implemented before mature test methods are developed. The effect is that flaws are missed and systems slip through and are certified with significant weaknesses. The remedy would seem to be to not advance a new revision without technically detailed and robust test methods to accompany it.

It is of significant note that there are no voting systems certified to the VVSG 2005. Therefore nobody knows for certain what is right or wrong with those specifications. While

every individual has their opinions as to the sufficiency of the VVSG 2005 the fact is that nobody knows what is right or wrong with it.

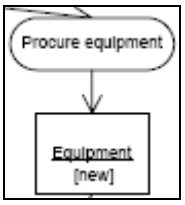
What could be done is to conduct a failure modes effects analysis that is strongly informed by actual elections experience. Where incidents or problems have occurred the analysis could be performed as to how that same system would be evaluated under the draft VVSG 2007. Is there a requirement that should have prevented the flawed system from being certified? If so, as typically seems to be the case, would the test method provided guarantee that the flaw would be detected? In general the test methods of the draft VVSG 2007 are so vague that the typical answer will be that many flaws could pass evaluation undetected. Such findings would then provide very effective guidance to the maturing of the draft to be a very commendable new tool for the system certification process.

VIII. Recommendations – The reference model of Part 1 Chapter 8 should be placed before any requirements and used as the guiding structure for the rest of the document.

If there is an equivalent to the space shuttle Challenger's 'O' ring it is to be found in the reference model of Part 1 Chapter 8. The Challenger had an 'O' ring but it was not sufficient to the demands placed upon it. Similarly the reference model provided could be the mechanism to bring together a election administration and equipment specifications so that they work together to provide fault tolerant, fail safe elections. How election administration and equipment specification interact and support each other could be analyzed and strategies implemented to assure the total system design.

For security producing a threat model and protection profile could transform what is now a grab-bag of isolated recommendations into a unified defense-in-depth security strategy for elections.

An example of how the reference model could be used to design the certification process to support election administration is found in the equipment delivery step depicted on the model.



At this step a local jurisdiction has contracted for some new equipment and the vendor delivers it. The question could be asked, "How does the local jurisdiction know that it is receiving a system identical to that which was certified?" An answer to that question is attempted in Part 1 Sections 5.2, Setup Inspection, and 5.3, Software Installation. However, because these sections are not written from the perspective of supporting election administration they fall short.

The first thing that can be noted is that there is no requirement that the hardware be indefinable at incoming inspection. It would not be too difficult to require a section of the final test report to support incoming inspection of voting systems. The VSTL could have a requirement to record versions and provide sufficient detail of printed wiring boards and other subassemblies to determine that the hardware on a system being delivered is identical to that which was certified.

A second observation is that the requirements of this section are written from a very unusual and insular perspective. An example is:

5.2.1.1-A Voting device software identification

The voting device SHALL be able to identify all software installed on programmed devices of the voting device.

Having the voting device check itself is an interesting approach. Why not just have the voting system check that it is compliant with the VVSG and do away with the VSTL's? As written it is not clear that this requirement or the others in these sections serve much purpose. However, there are two purposes that could be served, incoming inspection and defense-in-depth. From an

incoming inspection viewpoint what is needed is that an election administrator be able to independently verify all software as being unmodified from its certified version. The NIST NSRL provides software to check digital signatures using a self-booting CD. If there requirement were rewritten to first require that all systems allow independent verification of the software digital signatures and second that the VSTL perform an mock incoming inspection, recording in the test report both the procedures used and the values of the digital signatures, then a valuable tool would be provided for incoming inspection. From a defense-in-depth perspective the requirement might be rewritten that various software modules would check each other and alter administrators if a version other than that which was certified is detected. This would not be the only security measure but it could be one component in a larger strategy to provide redundant and overlapping security measures.

A third problem is found in the Test Reference, which states, Part 3:5.2 “Functional Testing”. What is found in Part 3:5.2 is 10 pages of vague, meandering discussion of how test procedures are to be designed. What is needed is a technically precise and specific test method. In this case, at the test reference are specific instructions to the VSTL to perform a mock incoming inspection and record both the tools and methods they used to check the hardware and software and the values they found. The test reference would provide enough specificity to assure that election officials could have the process repeated and assure that they are receiving voting systems identical to those certified. The point is that if the certification process does not document and make available information about the system that was certified then election officials will be hard pressed in performing an adequate incoming inspection.

An additional point is that, as written the test reference almost assures a wide variation among VSTL’s in how they will perform this evaluation. Further, there is almost no way that the NIST NVLAP laboratory assessors could fail a lab on this requirement. The VSTL could do almost anything and the NVLAP assessor would be hard pressed not to accept it given the vague way the test requirements have been written.

IX. Conclusions

The draft VVSG 2007 has been developed by hard working, well-intended, diligent people. There are many valuable elements in it. Unfortunately the failure to structure the work in a way that seeks to improve total election security, reliability and accuracy and more specifically the security, reliability and accuracy of the EAC's certification and conformity assessment system, has produced a fundamentally flawed document.

I thank the Commission for this opportunity to provide this testimony and offer my perspective.

Respectfully submitted,

H. Stephen Berger

H. Stephen Berger
140 River Rd.
Georgetown, TX 78628
(512) 864-3365

March 17, 2008