Research for the EAC: Applicability of VVSG 2007 Requirements for Inclusion in an Amended Version of VVSG 2005

National Institute of Standards and Technology (NIST)

NIST Voting Team

October, 2008

1. Overview and Summary

The Election Assistance Commission (EAC) has asked NIST to investigate whether certain requirements in the 2007 Next Version VVSG (herein referred to as "VVSG 2007") could be integrated with or replace current requirements in the VVSG 2005, resulting in an amended version of the VVSG 2005. Their goal is to improve the overall quality and uniformity of testing for voting systems and to make key improvements in the current VVSG 2005 while the VVSG 2007 is in public review. These requirements would also be accompanied by tests that have been developed by NIST as part of the test suite for VVSG 2007.

Besides the primary issue of improving the quality of testing, the EAC has also asked that other criteria be used to identify candidate requirements from VVSG 2007 for inclusion in an amended VVSG 2005. The candidate requirements criteria would be those that:

1. Improve the overall quality and uniformity of testing voting systems (and are accompanied by test cases),
2. Would not require hardware changes to current voting systems,
3. Would not require complex changes in software to current voting systems,
4. Would not substantially change the structure of the VVSG 2005, and
5. Would not change the intent of the VVSG 2005.

Additionally, the EAC wishes to create this next version within a timeframe of approximately 6 months.

Accordingly, NIST has identified requirements in VVSG 2007 that meet the criteria above. Given the criteria, many aspects of VVSG 2007, such as the complete device and system class structure, performance benchmarks, and software independence, are not candidates for consideration. These

items are too complicated to include in an amended VVSG 2005, especially within a six-month timeframe.

2. Purpose and Structure of this paper

This paper describes material from VVSG 2007 that could be integrated into an amended VVSG 2005, given the EAC's criteria. It begins by outlining some of the general issues involved in selecting and integrating this material.

The paper then presents the selected material, accompanied by specific considerations for integrating the material. While estimates on the ease or difficulty of integrating the material can be approximated, they cannot be precisely known until the actual work commences. Therefore, the material is categorized roughly as "relatively straightforward to do" and "more complicated to do."

3. General issues relevant to inclusion of VVSG 2007 requirements in an amended VVSG 2005

NIST has recommended that the EAC implement VVSG 2007 upon completion of the public review process. The structure and precision of VVSG 2007 offers significant advantages over the VVSG 2005 with respect to clarity, completeness, and testability of requirements. The looseness and lack of consistency in the VVSG 2005 work against achieving a consistent and uniform understanding of its requirements by vendors and testing labs.

Consequently, there are various issues that must be addressed when including material from VVSG 2007 in an amended VVSG 2005. The following issues make some material more problematic to include than other material.

1. **Document structure**: VVSG 2007 was reorganized to correct redundancies, overlaps, and commingled material in the VVSG 2005. VVSG 2007 includes three volumes of requirements, with equipment requirements in the first, documentation requirements in the second, and testing requirements contained only in the third. The VVSG 2005 contains two volumes, but mixes product, documentation, and testing requirements throughout. Additionally, the chapter structure is largely incompatible between the two standards. Thus, sections from VVSG 2007 often do not have one contiguous place to go in the VVSG 2005. It is not a simple exercise to copy a chapter from one standard to the other. For example, documentation requirements in Part 2 of VVSG 2007 would result in editing many different places throughout the VVSG 2005.

2. **Requirement precision and structure**: Incorporating requirements from VVSG 2007 into an amended VVSG 2005 will result in a mixture of precision -- VVSG 2007 requirements are more precise whereas there will still be issues of ambiguity with the VVSG 2005 requirements. This particular problem will not be resolved until a completely rewritten standard such as VVSG 2007 is released.

3. **Scope and conformance**: VVSG 2007 uses the class structure to establish requirement scope and to define conformance. Requirements for devices in VVSG 2007 are built upon the class structure and therefore take into account certain inherited requirements. Without the class structure, device requirements from VVSG 2007 may need to be modified, augmented, or restructured to account for the loss of inheritance. Again, this will result in editing many sections of the VVSG 2005 document. Analysis will be needed to ensure that all relevant sections of VVSG 2005 are modified appropriately and that the VVSG Recommendation requirements are fully captured. Consequently, modifications to the VVSG 2005 conformance section will be needed.

4. **Terminology**: The glossaries of the two standards differ substantially. Conflicts between the old and new terminology are substantial and not easily correctable without a VVSG 2007-style rewriting of all existing material. Having two co-existing terminologies may be confusing, although manageable. It may, however, require mapping of terms and terms being defined based on their origin (i.e., from VVSG 2005 or VVSG 2007).

5. **Limited scope of the VVSG 2005:** In VVSG 2007, there are requirements for electronic pollbooks (epollbooks) and electronic ballot markers (EBMs); these devices are becoming more common and, especially with epollbooks, integral to election operations. There are no specific requirements for these devices in the VVSG 2005. Although the VVSG 2005 includes requirements for DREs, neither of these devices are DREs. While one could conceivably copy all of the relevant epollbook and EBM requirements from VVSG 2007 into an amended VVSG 2005, it is not straightforward. Many of these requirements are derived from requirements inherited as part of the class structure and their inclusion would overlap or be disjoint with existing DRE requirements in the VVSG 2005. This problem will not be resolved until a completely rewritten standard such as VVSG 2007 is released.

6. **Security:** VVSG 2007 was designed with a comprehensive set of security requirements that worked together to improve the security of voting systems. The inclusion of Software Independence allowed for the relaxation of certain other requirements, such as those for software setup validation. Consequently, security requirements that are selectively incorporated into an amended VVSG 2005 will need to be strengthened or re-interpreted in light of the absence of Software Independence or other integral security requirements. In addition, a number of security requirements will result in significant hardware and software changes.

4. VVSG 2007 material for inclusion in an amended VVSG 2005

The following subsections identify VVSG 2007 material that meet the criteria put forth by the EAC. Each subsection is labeled as to whether the integration of the material is "relatively straightforward to do" or "more complicated to do." This is an estimate - the actual ease or difficulty in integrating VVSG 2007

material will not be known until the integration actually begins. At that point, unanticipated problems associated with integrating material from the two very different documents may be realized, e.g., informative text may need to be created in order to integrate the newer material but this may not completely alleviate integration problems or confusion between the two standards.

4.1 Core requirements

The VVSG 2007 addresses core requirements using an integrated approach that includes consistent use of terminology and a structured organization of types of voting systems. In order to meet the EAC criteria, NIST identified several areas in the core requirements chapters of VVSG 2007 that primarily address improved testing and documentation.

1. **Volume Testing - Relatively straightforward to do:** Since volume testing is new material relative to the VVSG 2005, a chapter specifying it could be added at the end of Volume II. The requirements that appear in VVSG 2007 could be expanded with informative material to flesh out the chapter and provide more guidance to test labs.

2. **Hardware and Software Performance Benchmarks and Test Method - More complicated to do:** These requirements make significant changes to the test methods in the VVSG 2005 for reliability and accuracy, and as such may have significant impact on test labs, i.e., test labs will need to create new tests. Manufacturers would be impacted only if their systems are unable to meet the new benchmarks. Including this material requires that the Logic Model of Part 1 Chapter 8 also be included to provide a basis for the assessment of accuracy.

    - Part 1 Section 6.3.1 (Reliability) of VVSG 2007 replaces Volume I Section 4.3.3 of the VVSG 2005. The new material is considerably longer than the section it replaces. To maintain coherency, the reliability requirements in VVSG 2007 that were pulled in from other sections of VVSG 2005 (single point of failure, protect against failure) would not be included; the corresponding requirements in VVSG 2005 would be left as is.

    - The revised reliability benchmarks are divided up by device classes, whose definitions would need to be included in the amended VVSG 2005 in, likely, a separate terminology section.

    - Part 1 Section 6.3.2 (Accuracy) replaces Volume I Section 4.1.1 of the VVSG 2005.

    - Part 1 Section 6.3.3 (Misfeed rate) replaces I.4.1.5.1.e.ii (under Ballot Handling) and I.4.1.5.2.f (under Ballot Reading Accuracy) of the VVSG 2005. Most likely, the VVSG 2005 requirements in question would be entirely replaced with the new section.

    - To update the test methods, Volume II Appendix C of the VVSG 2005 would be completely replaced by Part 3 Section 5.3 of VVSG 2007 and Volume II Sections 4.7.1.1

and 4.7.3 of the VVSG 2005 would be deleted. In addition, Volume II Section 4.5 must be harmonized with Part 3 Section 2.5.3 of VVSG 2007 to close a loophole that can invalidate the test results.

3. **Software Workmanship - More complicated to do:** Software workmanship addresses "coding conventions." While it might appear impossible to change coding conventions without resulting in significant changes to existing software, there are improvements that can be made. The software workmanship requirements in the VVSG 2005 appear in three groups:

    a. Volume I Section 5.2.1 through Section 5.2.7 is where the software workmanship requirements logically belong; most do appear there.

    b. Volume II Sections 5.4.1 and 5.4.2 contain many additional requirements on software workmanship, most of which are eliminated in VVSG 2007.

    c. Additional requirements related to software integrity (e.g., error checking), which are what VVSG 2007 emphasizes, are mixed in with other material scattered throughout Volume I.

    The software workmanship requirements could be partially updated by making changes to the sections identified in #1 and #2 above. Unfortunately, this would still leave some potentially confusing redundancy between the new requirements and the old, which could lead to interpretation conflicts when they do not use exactly the same words. To finish the job would require a list of edits of the form "Strike subrequirements c and d and the first half of subrequirement f" to address the scattered requirements identified in #3, which is possibly a more extensive edit than what the EAC desires.

4. **(Non-EMC) Environmental Hardware - Relatively straightforward to do:** Most of these requirements derive from predecessors in the VVSG 2005. The requirements in VVSG 2007 consist of the requirements in Sections 6.4.3 (General Build Quality), 6.4.4 (Durability), 6.4.5 (Maintainability), 6.4.6 (Temperature and Humidity), and 6.4.7 Testing) and 5.1.5 (Operating Environmental Testing) in Part 3.

    It would be relatively easy to replace the predecessor requirements in the VVSG 2005 with the requirements above. The VVSG 2005 requirements that would be replaced include the Volume I sections 4.1.2.13 (Environmental Control – Operating Environment, 4.1.2.14 (Environmental Control – Transit and Storage), 4.2 (Physical Characteristics), and 4.3 (Design, Constructions, and Maintenance Characteristics). With the inclusion of the VVSG 2007 requirements, introductory and transitional material would need to be created or revised for the amended VVSG 2005.

    With respect to Volume II of VVSG 2005, sections 4.6 (Non-Operating Environmental Tests) and 4.7.1 (Temperature and Power Variation Tests), and 4.7.2 (Maintainability Test) would be removed; most of the text in these sections is devoted to test materials, including detailed test

scenarios, the equivalents of which were not included in VVSG 2007. Test materials are critical, but were deemed outside the scope of VVSG 2007 and would be provided separately. NIST is developing test materials for VVSG 2007 and has devoted thought and planning to retrofitting the VVSG Recommendation test materials to a VVSG 2005 context. Thus, the test materials removed from the VVSG 2005 would be captured in corresponding test materials developed for the amended VVSG 2005.

The EMC requirements in VVSG 2007 are not recommended for inclusion in an amended VVSG 2005. While these requirements would be relatively straightforward to integrate, the complete draft of test materials for the newer EMC requirements will not be completed before early FY 09.

5. **Quality Assurance and Configuration Management - Relatively straightforward to do:** The requirements for Quality Assurance (QA) and Configuration Management (CM) are contained in specific chapters in the VVSG 2005 (Volume I, Sections 8 and 9, and Volume II, Sections 2.6, 2.7, and 7). Similarly, in VVSG 2007, the QA and CM requirements are essentially self-contained in Part 1, Section 6.4.2, Part 2, Chapter 2, and Part 3, Section 4.4. The QA and CM material was totally rewritten for VVSG 2007, however both are based on an acceptance of ISO 9000. This effort would involve replacing the VVSG 2005 chapters with VVSG 2007 chapters.

6. **Test Plan, Test Report, and Public Information Package - Relatively straightforward to do:** If desired, Appendices A and B of Volume II of the VVSG 2005 could be replaced modularly with Chapters 5, 6 and 7 of Part 2 of VVSG 2007. This would have the following effects:

    - The test plan and test report outlines provided in the VVSG 2005 would be removed, replaced by content-based requirements in VVSG 2007.

    - The implied specification of a minimum scope of testing in Appendix A of Volume II of the VVSG 2005 would be removed. If it is needed—that is, if it is not redundant with test materials and manuals published separately—a new section would have to be added to the VVSG 2005 to supply the displaced material. (In VVSG 2007, these testing requirements moved to Part 3.)

    - The VVSG 2005 requirements about reporting benchmarks would need adjustment if the cross-referenced benchmarks and test methods are not included in the amended version.

    The requirements for the Public Information Package in Part 2 Chapter 7 of the VVSG Recommendations is minimal and is new material.

7. **TDP and Voting Equipment User Documentation - More complicated to do:** Much of the core requirements material in Part 2 of VVSG 2007 consists of documentation requirements from the VVSG 2005 that were extracted, reformatted, and organized into a separate volume. Additionally, user documentation requirements were separated from TDP requirements. This

essentially makes clear to vendors and test labs what is expected in terms of documentation. Most of the security-related documentation requirements in Part 2 of the Recommendations is new and, depending upon which security-related material is included in an amended VVSG 2005, the corresponding documentation requirements would be included as well. The human factors-related documentation requirements are included in Part 1, Chapter 3; including Chapter 3 in the amended VVSG 2005 (as is recommended below) will thus include these documentation requirements.

With respect to the core requirements documentation, most of the value added was in the reorganization and cleanup, rather than the rewriting of specific requirements. It may not make sense to incorporate entire sections of the VVSG 2007 requirements unless the VVSG 2005 is restructured similar to VVSG 2007. Instead, just the few new and/or substantially changed requirements should be integrated with the VVSG 2005.

4.2 Human factors

Chapter 3 of VVSG 2007 minus performance benchmarks - Relatively straightforward to do: The general requirements in Part 1 Chapter 3 could essentially replace those in Volume I Chapter 3. However, VVSG 2007 included performance benchmarks that addressed deeper usability issues using a state-of-the-art usability testing approach. This is a significant change in the usability requirements, and, as such, is beyond the scope of the EAC's request. In addition, NIST is still researching the test methods to support the performance benchmarks.

Updating the human factors general requirements will be relatively straightforward. The VSS 2002 contained almost no usability, accessibility, and privacy requirements. As a result, the VVSG 2005 Chapter 3 is mostly new material based on research, best practices, and standards relating to human factors and the design of user interfaces as they apply to voting systems. With the exception of the performance benchmarks, Part 1 Chapter 3 of VVSG 2007 was primarily a maintenance level upgrade to the VVSG 2005 with minor modifications and clarifications. However, there are a few critical additions including performance and poll worker usability requirements.

Updating the general requirements should have little impact on the test labs. Manufacturers may need to make some software changes to their user interfaces and documentation. The new general requirements in Part 1 Chapter 3 are minimal, but high value, including pollworker usability and end-to-end accessibility requirements

4.3 Security

VVSG 2007 laid out a new strategy for securing voting systems based on the concept of Software Independence (SI). SI is beyond the scope of an amended VVSG 2005, since it would result in existing DRE voting systems no longer being conformant. In addition, most of the core security requirements such as access control and auditing could require extensive system modifications. Security also included a new testing approach: Open Ended Vulnerability Testing. While inclusion of this test into VVSG 2005 would not necessarily cause changes in system hardware and software, the test methodology is still being developed and the ramifications of this type of testing are currently unknown. As such, it is also beyond the scope of an amended VVSG 2005.

1. **Communications Security - Relatively straightforward to do:** Both VVSG 2007 and the 2005 VVSG have requirements related to security of communications between voting devices. The communications requirements are found in Part 1 Section 5.6 of VVSG 2007 and in Sections 6.1 Telecommunication Requirements and 7.7 Wireless Communications of the 2005 VVSG. VVSG 2007 limits the scope of communication by prohibiting the use of wireless technology (except for infrared technology) and only allowing communication outside a polling place when an air gap exists between the communicating device (such as an electronic pollbook) and devices that capture cast ballots. The VVSG 2005 does not limit the scope of communication and explicitly allows wireless technology. For an amended VVSG 2005, the EAC could amend the 2005 VVSG to prohibit the use of wireless technology and restrict communications on public communication networks as per VVSG 2007.

2. **VVPAT - Relatively straightforward to do:** VVSG 2007 and the VVSG 2005 both include requirements for Voter Verifiable Paper Audit Trail (VVPAT) systems. The VVPAT requirements in VVSG 2007 (Part 1 Section 4.4.2) were developed as an update and, as a result, could simply replace those requirements and VVSG 2005. The newer requirements improve the auditability and usability of the paper records and ensure that sufficient information is printed on the record so that the systems can be used for early voting and in multi-precinct vote centers.

3. **Electronic Records - More complicated to do:** VVSG 2007 includes extensive requirements for producing and signing electronic reports and records. The VVSG 2005 also addresses reports in Volume I, Section 2.4.3 - Producing Reports. It would be possible to develop requirements to digitally sign the reports already defined in VVSG 2005. These changes would not be the same requirements as VVSG 2007, but would draw upon the general approach to signing records. The amended VVSG 2005 would not include any of the requirements for a hardware cryptographic module, but would include requirements for using a software cryptographic module.

4. **System Security Specifications Documentation - Relatively straightforward to do:** The system security specification documentation requirements of Part 2 Section 3.5.1 are new; including them in an amended VVSG 2005 would help test labs understand how a voting system has been designed to handle security and could easily be included as new requirements. Other security

documentation requirements related to specific security features (e.g., access control, system event logging) also could be included depending on whether the corresponding security feature is included.

5. **External Interface - More complicated to do:** Since VVSG 2007 included SI and other advanced security methods, it did not update the external interface section of the VVSG 2005. This section would have to be clarified.

6. **Initial System Build - Relatively straightforward to do:** The requirements in Part 3 Section 2.4.4 (Initial system build by test lab) of VVSG 2007 are very similar to requirements found in Section 5.6 Trusted Build Procedures found in the EAC's Testing and Certification Program Manual. These could be incorporated into the amended 2005 VVSG or harmonized with the Testing and Certification Program Manual.

7. **Software Distribution - Relatively straightforward to do:** In Part 3 Section 2.6.2 (Software Distribution Requirements for Repositories, Test Labs, and Manufacturers) of VVSG 2007, there are technical requirements to support a process to distribute software in an authenticated fashion. Authentication of the software used by voting system is very important in the absence of software independence since the voting system integrity depends on the software it runs. However, the requirements set up the framework to leverage specific voting system requirements in the area of software installation and system integrity management. VVSG 2007 requirements are more complete in regards to software distribution than the Testing and Certification Program Manual. These could be incorporated into the amended 2005 VVSG or harmonized with the Testing and Certification Program Manual.