Order Code RL33146

CRS Report for Congress
Received through the CRS Web

Federal *Voluntary Voting System Guidelines:* Summary and Analysis of Issues

November 9, 2005

Eric A. Fischer
Senior Specialist in Science and Technology
Resources, Science, and Industry Division

Federal *Voluntary Voting System Guidelines:* Summary and Analysis of Issues

Summary

The Help America Vote Act of 2002 (HAVA, P.L. 107-252) gave the federal Election Assistance Commission (EAC) the responsibility to develop a set of *Voluntary Voting System Guidelines* (*VVSG*) to replace the current voluntary *Voting Systems Standards* (*VSS*). The *VVSG* are to provide a set of specifications and requirements to be used in the certification of computer-assisted voting systems, both paper-based and fully electronic. That was also the purpose of the *VSS,* which were developed in response to concerns raised about voting systems in the 1970s and 1980s. Most states have adopted the *VSS* in whole or in part, and most are expected to adopt the *VVSG,* which are scheduled to go into effect two years after approval.

The draft *VVSG,* a partial revision of the *VSS,* was released in June 2005 for a 90-day comment period. Volume I provides performance guidelines for voting systems and is intended for a broad audience. It includes descriptions of functional requirements and performance standards, and requirements for vendors. The most extensive revisions are to the section on usability and accessibility and the section on security of voting systems. Standards are also included for the use of voter-verified paper audit trails (VVPAT), a recent security measure developed in response to concerns that electronic voting machines are vulnerable to tampering that might otherwise be difficult to detect. Volume II provides details of the testing process for certification of voting systems and has few revisions.

Some issues associated with the *VVSG* have been controversial. Among them is the question of timing. Some vendors claim that there needs to be more time for technology development before the new guidelines become effective; some activists argue that problems with voting systems, and HAVA provisions, demand more rapid implementation of the *VVSG*. In any event, it is generally considered unlikely that the guidelines will have much direct impact on voting systems used in 2006, when HAVA requirements for voting systems go into effect. One exception may be the VVPAT provisions, since the *VSS,* under which most current voting systems are certified, have no provisions relating to this innovation. The *VVSG* will be voluntary, but some observers believe that a regulatory approach would be more appropriate given the importance of elections to the democratic process. However, since many states require that voting systems be certified, vendors are expected to treat the *VVSG* in the same way they have treated the *VSS* — as effectively mandatory.

Among the other issues being debated about the guidelines are whether they should be expanded to include voter registration systems, whether they impede innovation by focusing on integrated systems rather than components, how to treat commercial off-the-shelf (COTS) products that are incorporated in voting systems, and whether a graded certification would be more effective than the current pass/fail approach. Several bills introduced in the 109th Congress could affect the scope or other aspects of the VVSG by requiring VVPAT or other security provisions, addressing concerns about conflict of interest, and other measures. None have received committee or floor action in either chamber during the first session. This report will be updated in response to major developments.

Contents

Federal *Voluntary Voting System Guidelines:* Summary and Analysis of Issues

The Help America Vote Act of 2002 (HAVA, P.L. 107-252) established the federal Election Assistance Commission (EAC) and gave it the responsibility to develop a set of *Voluntary Voting System Guidelines* (*VVSG*). The guidelines are a set of technical standards for computer-assisted voting systems that will replace the federal voluntary *Voting Systems Standards* (*VSS*) originally developed under the auspices of the Federal Election Commission (FEC). Like those standards, the guidelines are intended to be used in the development and certification of voting systems. The *VVSG* are to provide a set of specifications and requirements to be used in certification testing by independent laboratories.

The EAC released a draft set for public comment in June 2005. That draft is a partial revision of the *VSS*. The most extensive revisions are to the section on usability and accessibility and the section on security of voting systems, which have been largely rewritten. The public comment period on the guidelines closed September 30. The EAC had expected to have the final version of the *VVSG* revised in response to those comments and ready for approval in October, but the large number of comments received at the end of the period has created uncertainty about when the guidelines will be finalized.

Many issues about the *VVSG* have been raised by voting system manufacturers, state and local election officials, academic researchers, professional and trade associations, public interest groups, and members of the public. Among the questions are the following:

- To what extent are the *VVSG* truly voluntary rather than regulatory?
- What is the appropriate role of the *VVSG* and similar standards?
- Is the process by which the *VVSG* are developed the most appropriate for ensuring high-quality, timely standards for voting systems?
- Is the scope of the revisions in this version of the guidelines appropriate?
- What impact will the *VVSG* have on the 2006 federal election?
- Should the scope of the *VVSG* be expanded to include voter registration systems?
- To what extent should the guidelines accommodate interoperable components of voting systems rather than integrated systems?
- How should certification of commercial off-the-shelf (COTS) products be managed in the *VVSG*?

- Should the certification process result in ratings of voting system performance or is the current pass/fail system adequate?
- How should the guidelines treat voter-verified paper audit trails and other verification systems?

This report begins with a discussion of the historical context of the *VVSG*, followed by a summary of the guidelines and a discussion of each of the issues identified above. However, there are many specific issues, such as whether wireless communications should be permitted, that are not covered here. The report also briefly summarizes relevant legislative proposals in the 109th Congress. It contains two appendices — a section-by-section summary of the guidelines and a glossary of abbreviations used in the report.

Historical Context of the Guidelines

The *VSS* were developed in response to concerns raised in the 1970s and 1980s about the then largely unregulated voting technology industry. In 1977, an FEC advisory panel recommended the development of voluntary standards, following an FEC-requested study released in 1975 by the National Bureau of Standards (renamed the National Institute of Standards and Technology, NIST, in 1988). Two years later, Congress enacted legislation directing the FEC to perform a study on the matter in cooperation with the National Bureau of Standards. The study, submitted to Congress in 1984, reaffirmed the advisory panel's recommendation, and the FEC received federal funding over the next several years to develop the *VSS;* however, Congress did not establish the *VSS* specifically by statute (see CRS Report RS21156, *Federal Voting Systems Standards and Guidelines: Congressional Deliberations*, by by Eric A. Fischer for more detail about congressional deliberations).

The *VSS* were first released in 1990. They applied to computer-based voting systems — namely, punchcard, marksense (optical scan), and direct recording electronic (DRE) systems. They were developed for both hardware and software and included functional and documentation requirements, performance characteristics, and testing procedures. No standards were developed for lever-machine or hand-counted paper ballot systems.

The FEC developed a plan to implement the *VSS* through cooperative action by the FEC, NIST, a set of laboratories that would be called the independent test authorities (ITAs), state and local governments, and voting system vendors. Under the plan, states would adopt the standards and the ITAs would test voting systems to determine whether they met the standards. NIST's intended role was to assist in accreditation of the ITAs. However, the plan did not materialize as originally conceived. Instead, the National Association of State Election Directors (NASED), which was established in 1989, appointed a voting systems board[1] to choose ITAs and administer a process for qualifying voting systems under the *VSS*. The testing program began in 1994. NASED chose The Election Center, a professional

[1] The former chair of this board, Thomas Wilkey, became the first executive director of the EAC in June 2005.

organization of election officials, to serve as the secretariat for voting system qualification.

States began adopting the *VSS,* with some requiring that voting systems be qualified under the standards before being used in the state, and others adopting elements of the *VSS* into state requirements. As implementation proceeded and technology continued to evolve, calls increased for revising and updating the *VSS*. The FEC began a project to update the standards in 1997. The second version was approved by the FEC in May 2002. The revision took a broader approach than the original version, focusing on the voting medium — paper-based versus electronic — rather than specific kinds of voting systems. It also included or expanded coverage of functions and requirements not in the original version — such as accessibility and some aspects of usability, telecommunications, and audit trails.

While this update was underway, Congress was considering legislation to respond to the problems that arose in the November 2000 presidential election. The enacted version, HAVA, the Help America Vote Act of 2002 (P.L. 107-252), was signed into law in October 2002. It includes voting system requirements and an administrative structure for promulgating standards and certifying systems. The act established the EAC and assigned it responsibility for developing the *VVSG.* It also created three bodies — a Standards Board, a Board of Advisors, and a Technical Guidelines Development Committee (TGDC) — to provide advice on standards and other matters; and it gave NIST a substantial role. For example, it made the director of NIST the chair of the TGDC. Sec. 222 of HAVA effectively renamed the *VSS* as the *Voluntary Voting System Guidelines* (*VVSG*),[2] to be developed by the EAC pursuant to recommendations by the TGDC and with support from NIST. Thus, HAVA provided a statutory basis for the *VSS*. HAVA does not direct the EAC to include any specific issues in the guidelines. However, in the debate on the House floor before passage of the HAVA conference agreement on October 10, 2002, a colloquy (*Congressional Record,* daily ed., 148: H7842) stipulated an interpretation that the guidelines specifically address the usability, accuracy, security, accessibility, and integrity of voting systems. Also, Sec. 221(e) requires NIST to provide support to the TGDC for development of guidelines relating to security, voter privacy, human factors, remote voting, and fraud detection and prevention.

The current *VSS* will serve as the guidelines until new ones are completed. Work on development of the first version of the *VVSG,* a partial revision of the *VSS,* began in 2004 with the appointment of the TGDC. That committee transmitted its recommendations, in the form of a proposed version 1 of the *VVSG,* to the EAC on May 12, 2005. After reviewing the recommended guidelines and making some

[2] The changes in terminology are a potential source of confusion: The requirements for voting systems established by §301 of HAVA are called Voting Systems Standards. They are not the same as, and should not be confused with, the *VSS*. The EAC was also to develop voluntary guidance (§311) to assist states in implementing the HAVA requirements (§301-5). However, no statutory role is given to the TGDC or NIST with respect to that guidance. Presumably, the EAC could have continued referring to the guidelines as the *VSS* but has chosen instead to use the terminology contained in HAVA, possibly to avoid confusion between the guidelines and the requirements.

revisions, mostly but not entirely of an organizational nature,[3] the EAC released the draft *VVSG* on June 27, 2005, for a 90-day public comment period, with adoption initially anticipated in October 2005.[4] They will go into effect two years after being adopted.[5]

HAVA also requires the EAC to provide for testing and certification of voting systems (§231) by laboratories it has accredited, with support from NIST, thereby transferring that responsibility from NASED. The act stipulates that the current system of NASED certification will continue until the EAC adopts its replacement. HAVA does not specify whether the guidelines it establishes are to be used as the standard against which voting systems are tested and certified, but that is how the *VSS* have been used, and it is how the EAC intends to use the *VVSG*.[6]

NIST began the process of soliciting applications for accreditation in June 2005, under its National Voluntary Laboratory Accreditation Program (NVLAP).[7] It will

[3] For example, Appendix D, on dual independent verification systems, was part of Section 6 in the TGDC draft. Also, recommendations on best practices that were in section text have been moved to Appendix C. Changes were also made in some cases that narrowed or otherwise modified provisions to line up more precisely with HAVA or other legal requirements or for other reasons (see Election Assistance Commission, "U.S. Election Assistance Commission Excerpt from the Public Meeting," Transcript, June 30, 2005, available at [http://www.eac.gov/06-30-05_Meeting.htm]). For example, two of the three principles cited in the subsection on human factors were revised: "1. All eligible and potentially eligible voters shall have access to the voting process without discrimination" was changed to "1. All eligible voters shall..."; and "2. Each cast ballot shall capture the intent of the voter who cast that ballot" was changed to "2. Each cast ballot shall accurately capture the selections made by the voter." Other changes were made for clarification. For example, provision 2.2.6: "If the normal procedure includes VVPAT, the Acc-VS [accessible voting system] should provide features that enable voters who are blind to perform this verification" was augmented with the following: "If a state requires the paper record produced by the VVPAT [voter-verified paper audit trail] to be the official ballot, then the Acc-VS shall provide features that enable visually impaired voters to review the paper record." (EAC draft for public comment: Election Assistance Commission, *Voluntary Voting System Guidelines*, 2 volumes, [hereinafter cited as *VVSG*, vol. 1 or vol. 2] June 27, 2005, available at [http://guidelines.kennesaw.edu/vvsg/guide_toc.asp]; final TGDC draft: Electronic Privacy Information Center (EPIC), *Voluntary Voting System Guidelines Version I, Initial Report*, May 9, 2005, [http://www.epic.org/privacy/voting/eac_foia/], obtained by EPIC via a FOIA request).

[4] Election Assistance Commission. "EAC Releases Voluntary Voting System Guidelines for Public Comment," Press Release, 27 June 2005, available at [http://www.eac.gov/news_062705.asp]. Given the large volume of comments received, the EAC has withdrawn that initial estimate and has not stated when adoption is now expected.

[5] This means that anyone submitting a system for federal certification after that date will need to follow the new guidelines rather than the 2002 version of the *VSS*. The latter went into effect in January of 2004, 20 months after they were adopted.

[6] *VVSG*, vol. 1, p. 1-15.

[7] National Institute of Standards and Technology, "Availability of Applications for the Laboratory Accreditation Program for Voting System Testing Under the National Voluntary

(continued...)

make recommendations through this program on accreditation of individual laboratories. Because of the length of the accreditation process, in August the EAC adopted a resolution to provide temporary accreditation to the laboratories (ITAs) accredited by NASED.[8]

Summary of Guidelines

Most sections of the draft version of the *VVSG* released for public comment are virtually identical to those in the 2002 update of the *VSS*. That was a consequence of a stated intent by the EAC to create a version that could be used in preparation for the 2006 election cycle.[9] Consequently, major revision focused mainly on usability and certain aspects of security. Major changes included

- addition of a conformance clause;
- revised and expanded standards for accessibility and usability;
- revised standards for security, including voter-verified paper ballots used with electronic voting machines (DREs)[10];
- some changes to testing procedures; and
- some new and expanded appendices.

A more extensive revision is reportedly underway.[11] A brief summary of provisions in the current draft is provided below, and a section-by-section summary is included at the end of this report in Appendix 1. These summaries are intended only to aid in understanding the basic scope and contents of the guidelines from a legislative perspective; other writers might choose to emphasize different aspects.

The *VVSG*, like the *VSS*, are divided into two volumes. Volume I provides performance guidelines for voting systems and is intended for a broad audience. It includes descriptions of functional requirements and performance standards, as well as requirements for vendors in quality assurance and in configuration management, a complex discipline that involves ensuring that a system and its components function in the ways they are specified to function under various modifications and throughout their life cycles. It includes an extensive glossary and references, suggested practices for election officials in some areas covered by the guidelines, and discussion of verification concepts for future design of voting systems.

[7] (...continued)
Laboratory Accreditation Program," *Federal Register* 70, no. 116 (June 17, 2005), p. 35225.

[8] NIST expects to make its initial recommendations in early 2007 (Election Assistance Commission, "Staff Recommendation: EAC Voting System Certification & Laboratory Accreditation Programs," adopted August 23, 2005, [http://www.eac.gov/VSCP_082305.htm]).

[9] Although the *VVSG* will not go into effect before 2007, the guidelines are voluntary, and states are therefore free to adopt them sooner if desired.

[10] A DRE is a direct (or digital) recording electronic voting machine, where votes are recorded directly electronic media rather than first being marked on paper by the voter.

[11] See Technical Guidelines Development Committee, "Voluntary Voting System Guidelines, Version 2, Draft," April 13, 2005, [http://vote.nist.gov/VVSG2_20050418.doc].

Volume II provides details of the testing process for certification of voting systems. It is aimed at a narrower audience of vendors, testing laboratories, and election officials. It includes a description of the data that vendors are required to provide when submitting a system for testing, and basic requirements for testing against the standards described in Volume I. It also provides guidance and requirements for testing laboratories in planning tests and reporting certification results.

Issues Raised by Guidelines

Many of the issues described below, as well as a number of more specific ones, have been captured in the various public comments made on the draft *VVSG*.[12] Commenters include election officials, vendors, academic researchers, representatives of professional associations and interest groups, and members of the public. However, the discussion is not limited to issues raised in the comments.

Technical Guidelines versus Regulatory Requirements

The *VVSG,* like the *VSS* before them, are voluntary technical standards, not regulatory requirements. Such standards are usually developed through a consensus process. They are common in industry, and federal law encourages their use by federal agencies.[13] Some observers believe that making standards voluntary at the federal level cannot ensure sufficient quality of voting systems and that adherence should be mandatory or at least a condition of receiving any federal grants for voting equipment.[14] Others state that mandatory standards would give too large a role to the federal government and reduce the flexibility of state and local governments to respond to their specific needs. They also point out that most states have adopted the *VSS* in whole or in part — many require that any new voting systems purchased adhere to the *VSS* or *VVSG*. The practical effect of such state requirements is that voting system vendors can successfully market systems only if they are certified under the *VSS* or *VVSG*. In this sense, the provisions have acquired some of the force of regulation, in that they are treated by manufacturers as requirements. Comments by vendors often reflect that perception.

HAVA addresses this controversy by establishing some specific requirements for voting systems (Sec. 301), but leaving the method of implementation to the states

[12] See Election Assistance Commission, "Voluntary Voting System Guidelines: View Comments," October 13, 2005, [http://guidelines.kennesaw.edu/vvsg/view_section.asp].

[13] Section 12(d) of the National Technology Transfer Advancement Act of 1995 (15 U.S.C. 272 note) requires federal agencies to use voluntary consensus standards except where they would be "inconsistent with applicable law or otherwise impractical." Office of Management and Budget Circular A-119 provides guidance for implementing this provision of the 1995 act.

[14] Congress has made some standards mandatory for federal agencies. For example, the Federal Information Security Management Act of 2002 (P.L. 107-296) requires that federal agencies adhere to a set of computer-security policies, standards, and practices, but these do not apply to voting systems, which are under the purview of state and local governments.

(Sec. 305). The act is largely silent on the relationship between the *VVSG* and the Sec. 301 requirements.[15] The EAC is required to provide guidance for implementing the requirements (Sec. 311–312), but the guidance is not a technical standard and its use is also voluntary.

What Standards Can and Cannot Do

There are many different kinds of standards. They may be classified according to purpose — e.g., product, process, testing, or interface standards. They can also be classified according to their focus — commonly, a distinction is made between performance standards, which focus on function, and design standards, which specify features, dimensions, or other such characteristics.[16] A third classification is based on how standards are developed and implemented. They may be developed through consensus or some other process. They may be implemented voluntarily, or they may also be imposed, for example by law, and therefore mandatory. Standards may also be open or proprietary, but different observers define "open standard" somewhat differently. Some form of open standards is the approach used typically by major standards organizations such as the American National Standards Institute (ANSI).[17]

The *VVSG* and the *VSS* before them do not fall neatly into any one of the above categories. They combine product, process, and testing requirements. They are intended to be performance-based, but in some cases they provide fairly specific design details. That has been criticized by some observers as not providing sufficient flexibility for innovation, but it has been praised by others as providing more precise requirements. The *VVSG* have also been criticized, on the one hand, for being too precise and detailed, and on the other, for being too vague and ambiguous.[18] Also, they are voluntary at the federal level but mandatory in a number of states. Finally, the process of development of the *VSS* might best be described as having been only partially open. With the involvement of NIST and the various EAC boards and committees, the development of the *VVSG* is arguably more closely akin to a typical consensus process for standards development.

[15] Those requirements are that voting systems must provide for auditability, accessibility, and ballot verification and error correction by voters, that states must set standards for what constitutes a vote on a given system, and that machine error rates of voting systems must conform to the standards set in the *VSS*. This last requirement (Sec. 301(a)(5)) is the only direct connection in the act between the requirements and the *VVSG*. It does arguably provide further impetus for vendors to have systems certified under the *VVSG* and for states to require that they do so. In contrast, Sec. 251(d) specifically exempts states from adherence to the *VVSG* as a condition for receipt of payments to meet HAVA requirements.

[16] This distinction may be somewhat artificial. A focus on performance versus design can also be thought of as end points on a continuum, or even as different dimensions that may be differentially emphasized.

[17] ANSI is a private, nonprofit organization that administers and coordinates the U.S. voluntary private-sector standardization system (American National Standards Institute, "About ANSI," n.d., [http://www.ansi.org/about_ansi/overview/overview.aspx]).

[18] Of course, it is possible for both kinds of criticisms to be valid if, for example, they refer to different parts of the guidelines.

Properly designed standards can provide a clear baseline of expected performance. In conjunction with a well-implemented certification program, they can provide assurances to all parties that voting systems will operate according to specifications. The *VSS* and the NASED certification program are widely credited with having greatly improved the performance of voting systems in several areas, such as reliability and accuracy.

However, standards can address only those issues that were considered by the developers, and the way that the standards are developed and implemented can also affect the way issues are addressed. Those factors can lead to at least two kinds of problems. First, specifications and testing might not reflect real-world conditions. That has been a criticism of the *VSS* and especially certification testing, which was done in a laboratory testing environment rather than realistically simulated election conditions. Thus, consideration of error rates in the 1990 *VSS* was limited to machine error and did not take into account the kind of voter error that became such a central issue in the 2000 presidential election.

Second, standards may not be able to anticipate changed conditions. This is especially true for rapidly evolving information technology. For example, the security weaknesses found over the past few years in some DREs[19] were discovered in systems that had been certified under the *VSS*.[20] Those 1990 standards could not anticipate the rapid evolution of information technology and the kinds of security threats to which it would be subjected.

The Development Process for the *VVSG*

HAVA created a relatively complex process for the development of the *VVSG*. Proposed guidelines are developed by a technical committee chaired by the director of NIST. Those are then considered by two EAC boards — the Standards Board, consisting of state and local election officials from all the states, and the Board of Advisors, consisting of representatives of various groups specified in the act — and finally, by the EAC commissioners, after a public comment period.

Even without that complexity, the development of standards can involve lengthy deliberations. That is especially true for consensus standards,[21] but even the two

[19] For details, see CRS Report RL32139, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*, by Eric A. Fischer.

[20] In the 1990 version of the *VSS*, the security section was under 6 pages in length. In the 2002 version, it was more than double that, and in the *VVSG* draft, it is over 50 pages long.

[21] The IEEE, which is involved in a broad range of standards-development projects, began developing a standard for polling-place voting equipment in 2001 but did not produce a consensus document before the draft *VVSG* was released (see IEEE, "Voting Equipment Standards: Project 1583," January 5, 2005, [http://grouper.ieee.org/groups/scc38/1583/index.htm]). However, the organization is continuing to develop standards for electronic data interchange for voting systems under a project begun in 2002 (see IEEE, "Voting Systems: Electronic Data Interchange: Project 1622," December 3, 2004,

(continued...)

versions of the *VSS* took years to develop. International standards are often updated on a three- to five-year cycle. HAVA does not specify an updating cycle for the *VVSG,* although Sec. 215(a)(2) requires the Standards Board and the Board of Advisors to meet at least once a year "for purposes of voting on the voluntary voting system guidelines referred to it…," and Sec. 301(c) requires that guidance for the implementation of requirements be updated every four years. The first version of the *VVSG,* currently under EAC consideration, is not anticipated to go into effect until two years after adoption.[22] That implies an initial revision cycle of at least two years, although the TGDC has already begun work on the second version.

Some observers believe that a four-year development cycle is desirable, to permit systems to be used for two federal election cycles without requiring recertification. Others have criticized the process for development of the *VVSG* as being too slow and cumbersome, given the rapid development of information technology and associated issues. Others point out that rapid development and frequent revision could create serious financial and logistical difficulties for both vendors and election officials in trying to conform to the guidelines, as well as having a potentially negative impact on the quality of any revisions. This issue has been raised not only with respect to the release and effective date of the current *VVSG* draft, but also subsequent revisions. There appears to be an inherent conflict in responsiveness of the guidelines to, on the one hand, evolving needs and technology and, on the other, time and cost constraints inherent in responding appropriately to such changes. Achieving the right balance between them is likely to be difficult.

The Internet Engineering Task Force (IETF), a professional group involved in the evolution of Internet architecture, has addressed the challenge of rapid development and change by creating a system for developing standards that is performed largely online. Interested parties form a working group that is completely open to anyone interested. There is no active attempt by the IETF to guarantee a balance among different interests. The group identifies the scope of a standard and begins developing it. Drafts are posted online and comments incorporated. Once the group reaches a rough consensus, the draft is sent to the Internet Engineering Steering Group (IESG) for independent review, after which the draft may become a standard through some additional steps.[23] According to some observers, the use of such a fully open, online process, rough consensus, and independent review results in "cleaner" standards and a more rapid process than the more traditional approach. Whether the method could be adapted for the *VVSG* is not clear, especially given the complexities inherent in both the goals of the guidelines and much voting technology. An attempt to use such

[21] (...continued)
[http://grouper.ieee.org/groups/ scc38/1622/index.htm]).

[22] EAC, "EAC Releases Voluntary Voting System Guidelines."

[23] For details, see Internet Engineering Task Force, "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force," RFC 3160, August 2001, [http://www.ietf.org/tao.html].

an approach has been developed for the purpose of creating performance ratings for voting systems but has not yet led to any public results.[24]

Another issue has to do with how other accepted standards are used and incorporated in the *VVSG*. For example, the draft guidelines reference many NIST standards publications that are generally designed for use by federal agencies under the Federal Information Security Management Act (FISMA).[25] Some observers argue that product standards such as the Common Criteria (ISO/IEC 15408), which provides a set of evaluation criteria for the security of information technology,[26] would be more appropriate.

Certification Process

The development of plans for certification testing is also an issue. Volume II of the *VVSG* specifies that testing laboratories are to develop explicit plans for the certification testing. Some observers believe that those plans, like the *VVSG* itself, should be public and that opportunities for public comment should be given before they are finalized. However, since the plans are to be designed for each submitted system and based on the data provided by the vendor, it is not clear that public disclosure would be possible without releasing proprietary information. Similar concerns have been raised with respect to the call from some observers that the results of the certification testing be made publicly available. Some argue that making such information public would be a disincentive to investment and innovation by industry. Others disagree and state further that, given the important role that voting systems play in the democratic process, the public trust is best served by full disclosure.

Some observers have also raised questions about the methods for determining how testing laboratories are chosen. Under the NASED process, there has been little to no competition among different laboratories. Critics have expressed concern that the result has been higher costs for certification testing and barriers to the timely certification of systems from smaller, innovative manufacturers. The NVLAP accreditation process being developed under EAC auspices is expected to address such concerns by increasing the number of laboratories involved. However, this approach has also been criticized: "[W]hen testing authorities compete against each other for business, a vendor can select the authorities most favorable to its products or negotiate for advantageous testing procedures."[27] Those critics argue that government or nonprofit testing centers would be a better approach.

[24] See [http://www.vspr.org].

[25] FISMA is title III of the E-Government Act of 2002, P.L. 107-347.

[26] For more information on this standard, see CRS Report RL32777, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, by Eric A. Fischer.

[27] National Research Council, *Asking the Right Questions about Electronic Voting* (Washington, D.C.: National Academies Press, 2005), p. 6-16, available at [http://www.nap.edu/catalog/11449.html].

The Scope and Features of Revisions in the *VVSG*

The *VSS* were criticized for inadequately addressing usability, security, administrative procedures and practices, performance in actual use, voter registration systems, and other aspects of election administration. Those criticisms have been partially addressed in the *VVSG*. As described in the section above summarizing the guidelines, the TGDC decided to produce only a partial revision of the *VSS* as the first version of the *VVSG*. Except for new sections on human factors (usability and accessibility) and security, and the addition of some new appendices, the *VVSG* is largely unchanged from the 2002 version of the *VSS*.

The two major areas of revision are arguably the most important for immediate action, since usability and accessibility are major focuses of HAVA voting system requirements, and security concerns have been prominent in recent public debate about voting systems, especially DREs. Some observers welcome this restricted focus, believing that limited changes are more likely to be implementable in the short term. Others, however, believe that broader changes to the *VSS* are more urgently needed and that the draft *VVSG* should have been more thoroughly revised with more stringent requirements. Some believe that an "end-to-end" or "life cycle" approach is needed, and that standards or guidelines should be developed for technology, procedures, and personnel across all entities involved in election administration, ranging from developers and manufacturers of voting systems to pollworkers. It is not yet clear to what extent future versions of the *VVSG* may take such an approach. Still other observers have expressed concerns that the first version of the *VVSG* has created more new requirements for certification than is prudent for an interim document, which is intended to be followed by a more complete revision.[28] Those observers propose delaying adoption of the *VVSG* until it can be thoroughly revised.[29]

Yet others believe that the added provisions are inadequate to meet accessibility, alternative language, and security needs and that broader and more stringent requirements are needed. For example, some of the provisions in the sections on human factors and security have been criticized for being recommendations rather than requirements, the concern being that they do not therefore ensure full compliance with HAVA's accessibility requirements.[30] There is also concern among some that the *VVSG* do not adequately cover the full range of disabilities as required by HAVA. Disabilities that are specifically addressed relate to vision, dexterity, mobility, hearing,

[28] See, for example, statements of some vendors at Election Assistance Commission, "U.S. Election Assistance Commission Public Meeting," Transcript, June 30, 2005, available at [http://www.eac.gov/06-30-05_Hearing.htm].

[29] While the TGDC has referred to a Version I and Version II of the *VVSG*, the latter to be the thorough revision, the EAC has preferred not to use that terminology (Ibid.).

[30] Sec. 2.2.7.1.2.2.1 reads, "The vendor should conduct summative usability tests on the Acc-VS using blind subjects and report the test results to the voting system test lab…" (*VVSG*, Vol. 1, p. 2-14). This is intended to be an interim recommendation until the testing laboratories have developed usability testing procedures. However, other provisions containing recommendations do not appear to be interim, such as Sec. 2.2.7.1.3.4, "The Acc-VS should provide a mechanism to enable non-manual input that is functionally equivalent to tactile input."

speech, and cognitive function, although little to no detail is provided for the last two. There are several different ways to categorize disabilities, and the *VVSG* provide neither a source for the list used nor any indication of how exhaustive it is intended to be. The guidelines also state, "As a practical matter, there may be a small number of voters whose disabilities are so severe that they will need personal assistance."[31]

The revised security provisions have also raised questions among some observers. For example, some state-sponsored studies used penetration testing — deliberate attempts to break into voting systems — in attempting to address security issues associated with voting systems.[32] This is a fairly common technique in security testing, and some observers believe that it should be required by the guidelines. Other observers have expressed concern that some of the different requirements may be conflicting — that meeting one will require violating another.

Some have also pointed to concerns about specific elements of the *VSS* that were not examined by the TGDC. One particularly contentious provision is the requirement that failures occur no more often than every 163 hours of use.[33] Some observers argue that this is far too low, permitting 10% of precinct-based electronic systems to fail during an election.[34] Others argue that the more relevant standard is availability — which stipulates that the time it takes to repair a system must be short enough that it is available 99% of the time it is needed. However, availability is tested under laboratory conditions, and in practice may depend on factors such as whether someone is present at the polling place who can effect any needed repairs. Therefore, a system that achieves an availability score greater than 99% in testing might not achieve that level in actual use.

Whether the *VVSG* should include management guidelines for election administrators is also a matter of some dispute. In the current draft, best practice recommendations have been placed in an appendix, whereas they were in the numbered sections in the TGDC recommendation document. Their removal to an appendix eliminates any ambiguity with respect to their role, or lack of it, in the certification process. However, the development of a set of administration or management sections in future versions of the *VVSG* could raise the question of whether certification protocols should be developed for election administration. That possibility may be worthy of consideration, but it could require an additional

[31] *VVSG,* Vol. 1, p. 2-12.

[32] See, for example, Maryland Department of Legislative Services, "Trusted Agent Report: Diebold AccuVote-TS Voting System," prepared by RABA Technologies Innovative Solution Cell, 20 January 2004, [http://mlis.state.md.us/Other/voting_system/trusted_agent_report.pdf].

[33] See summary of Volume I, Section 3 in Appendix 1. The figure is for the mean time between failures (MTBF).

[34] Presumably, this figure is derived by dividing an average time of use of 15 hours on election day for a DRE or precinct-count optical scan voting system by the MTBF, yielding a quotient of 9.2%.

certification mechanism for election jurisdictions as well as vendors, depending on the focus of the management requirements.[35]

The *VVSG* and the 2006 Federal Election

Even with the limitations in scope of initial change to the *VSS*, there is some question what impact the *VVSG* can have on the 2006 election.[36] The EAC has indicated a desire to finalize the guidelines soon after the close of the comment period at the end of September 2005, but it has received more than 4,000 individual comments altogether.[37] In addition, the *VVSG* are not scheduled to go into effect until two years after adoption — that is, no sooner than fall 2007. Until that time, federal certification of voting systems will presumably continue to be based on the 2002 *VSS*, although state or local jurisdictions may choose to require vendors to meet some or all of the *VVSG* requirements sooner, and the EAC plans to issue guidelines to assist states in implementation.[38] That may be especially important for those jurisdictions that require a voter-verifiable paper audit trail for use with DREs, since that option is not covered by the *VSS* but is covered by the *VVSG*.

Some observers have expressed concern that uncertainties about the *VVSG* development and implementation have resulted in delays by states in procuring new voting systems to meet HAVA requirements. Among the reasons are worries about acquiring new systems in time for the January 2006 deadline that might later be deemed not to be in compliance with the requirements, or not obtaining systems of as high a level of quality as would be possible once the *VVSG* go into effect. Similarly, some observers are concerned that systems in use that were certified under the *VSS* but not the *VVSG* could be effectively decertified once certification under the *VVSG* begins. Those concerns are amplified by uncertainties with respect to federal funding for future acquisitions. One proposed solution is for the EAC to advise jurisdictions that systems conforming to the 2002 *VSS* will satisfy HAVA requirements. However, that version of the *VSS* was released before HAVA was enacted, and since the EAC has no regulatory authority, it is not clear what effect such advice would have. Other

[35] For discussion of practice standards and certification in the context of cybersecurity, see CRS Report RL32777, *Creating a National Framework for Cybersecurity: An Analysis of Issues and Options*, by Eric A. Fischer.

[36] See also Government Accountability Office, *Federal Efforts To Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need To Be Completed*, GAO-05-956, September 2005.

[37] The large volume of comments has resulted in delay in finalizing the *VVSG* and no date for adoption has been set.

[38] Sec. 8.1 of the *VVSG* states: "[T]he effective date provisions do not apply to the mandatory provisions of Section 301(a) of the Help America Vote Act (HAVA), which states must comply with on or before January 1, 2006. While the Guidelines set requirements and measures against which voting systems can be examined, they may represent a higher standard than what is required by Section 301(a) of HAVA. To make sure states are able to be in compliance by the January 1, 2006 deadline, EAC will issue guidance to interpret Section 301(a)." Such guidance was not publicly available as of late October 2005. It is not clear whether meaningful guidance would be possible if issued in the remaining two months of the year.

observers believe that delaying the implementation of the *VVSG* means that the 2006 federal election will need to be conducted with voting systems that are not designed to conform to HAVA requirements. Another concern raised by some is that the proposed fall 2007 implementation date may not leave sufficient time for vendors and states to develop and acquire conforming systems before the 2008 federal election.

The *VVSG* and Voter Registration Systems

The focus of the *VSS* has been limited to polling-place and central-office systems involved in the conduct of an election — from ballot preparation to election certification. Neither the *VSS* nor the first version of the *VVSG* address the technology used to create and manage voter registration lists. Sec 221(3)(2)(a) of HAVA requires NIST to provide technical support for development of guidelines relating to the computerized statewide voter registration lists mandated by Section 303(a) of HAVA. That arguably implies congressional intent that the *VVSG* cover that topic, but HAVA does not explicitly require that. The data interchange standards being developed by IEEE include voter registration data.[39] However, there are currently no formal or widely accepted standards for those lists, and that absence has raised concerns about adequate state implementation of the requirement by the January 2006 deadline.

Integrated versus Component Certification

The *VVSG* focus on voting systems rather than on individual components. While they permit the submission of interoperable components for certification, they require that "vendors shall submit for testing the specific system configuration that will be offered to jurisdictions or that comprises the component to be marketed plus the other components with which the vendor recommends that the component be used."[40] This implies, in essence, that a vendor wishing to submit a component that could be used with different voting systems would have to submit those systems along with the component for certification testing. Some observers argue that this restriction stifles innovation by requiring that those vendors who wish to market devices that can be used with existing voting systems negotiate agreements with voting-system vendors before certification of their components. However, such agreements may be difficult to obtain before a component is certified or may entail restriction on the use of the component to only one brand of voting system.[41] One proposal to address this concern is to allow certification of components separately, but require that they subsequently be certified with each voting system with which they would be used.

[39] IEEE, "Project 1622."

[40] *VVSG*, Vol. II, p. 1-7 to 1-8.

[41] See, for example, the statement of Jim Adler of Votehere before the EAC at the June 30, 2005 public meeting (Election Assistance Commission, "U.S. Election Assistance Commission Public Meeting," Transcript, June 30, 2005, available at [http://www.eac.gov/06-30-05_Hearing.htm]). Adler used the example of an Independent Dual Verification (IDV) system to illustrate the problem.

Use of Commercial Off-the-Shelf (COTS) Software

Most if not all voting systems use some form of COTS software that is proprietary — that is, the code is not publicly available. The use of COTS software is somewhat controversial. It is much less expensive in general to use such software when appropriate than to develop code specifically for the voting system. In addition, some commercial software, such as Microsoft Windows, has become standard, with computer hardware developed specifically to work with it. However, vendors have no control over how the COTS software is coded, and the code may be very complex. Code examination is not required under the *VVSG* for unmodified COTS software, and general-purpose software such as operating systems may be exempt from detailed examination. Some observers object to this exemption, arguing that it creates unacceptable security risks. Others believe that the guidelines should prohibit the use of COTS software altogether (although presumably they are referring to its use in a voting or counting machine, not in back-office computers used in such tasks as ballot preparation). Proponents counter that *VVSG* safeguards are adequate and that the use of COTS software permits superior applications at far lower cost than custom software would allow.

Grading versus Pass/Fail Certification

Under the *VVSG* testing scheme, voting systems pass or fail, but no additional information is provided to potential customers or the public about details of performance of certified systems — such as to what extent the tested system exceeded the standards. Some observers believe that a certification regime that provided more finely graded performance reports would be very useful in stimulating innovation and helping election officials decide which systems are best suited to their jurisdictions. However, to the extent such grading was subjective, it could be misleading or potentially subject to abuse. In 2004, a group of computer experts, vendors, election officials, social scientists, and advocates started the Voting System Performance Rating (VSPR) project, which aims at developing performance rating standards for U.S. voting systems,[42] but there has been no public indication from the group about when such standards might be expected.

Verification Systems, Including VVPAT

One thing added to the *VVSG* was a discussion of methods by which votes could be verified. For one such method, the voter-verified paper audit trail, or VVPAT, the *VVSG* provides standards, since such systems have been mandated by several states. However, several other kinds of such systems exist, and some are described in an appendix to the guidelines,[43] with some guidance for how they might be implemented. The systems described all have the characteristic of providing two independently verifiable channels for processing votes and are therefore called Independent Dual

[42] See "Voting System Performance Rating Charter," 15 December 2004, available at [http://www.vspr.org/vspr-charter.pdf], and P. L. Vora and others, "Evaluation of Voting Systems," *Communications of the ACM,* Vol. 47, No. 11 (November 2004): p. 144.

[43] *VVSG,* vol. 1, appendix D.

Verification (IDV) systems in the *VVSG*. The possible need for such systems has become a matter of public interest because of the controversy over the security of DREs. While most public attention has been paid to VVPAT, other methods arguably show more promise in terms of usability, accessibility, and verification power.[44]

Some observers believe that IDV systems — especially, VVPAT — are essential to ensure security of and confidence in electronic voting, whereas others believe that the costs and complexity of at least some IDV systems are disadvantages that outweigh any benefits. The guidelines do not require such a system, although such a requirement was considered by the TGDC.[45] Some observers believe that the *VVSG* should require VVPAT, but others believe that the verification provided by that method is of questionable value in practice and may create unforeseen problems of its own. Some also believe that the accessibility and alternative language provisions relating to VVPAT do not ensure full compliance with HAVA and other federal requirements. Still others believe that the *VVSG* should provide more stringent requirements with respect to what kinds of data should be recorded by voting systems for audit purposes. In any case, the trend at the state level toward requiring the use of VVPAT to address security issues is raising significant questions about whether such requirements can be reconciled with HAVA accessibility requirements under the constraints imposed by current technology.

Legislative Proposals in the 109th Congress

Several bills introduced in the 109th Congress could affect the scope or other aspects of the *VVSG*. They include the following proposals:

- Adding provisions on security of electronic data (H.R. 278);
- Requiring submission to and testing of voting machine software by states before an election (H.R. 470);
- Requiring use of a voter-verified paper audit trail (H.R. 278, H.R. 550; H.R. 704, H.R. 939, S. 330, S. 450);
- Requiring the use of a verification method involving paper, audio, or other means, and relevant standards (H.R. 533, S. 17; H.R. 939 for voters with disabilities);
- Requiring that voting systems used for disability access separate the functions of vote generation, verification, and casting (H.R. 550, H.R. 939, S. 450);
- Requiring the EAC to develop best practices for voter-verification for persons with disabilities and languages other than English (H.R. 550);

[44] For more detailed discussion, see CRS Report RL32139, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*, by Eric A. Fischer.

[45] Resolution 13-05, "Voter-Verifiability II," which was not approved by the TGDC, interpreted Sec. 301(a)(2) of HAVA to require that the paper record produced for manual audit be voter-verifiable (see National Institute of Standards and Technology, "Voluntary Voting Systems Guideline Version 1 (VVSG 1) - Draft Materials & Versions: Proposed TGDC Resolutions," January 2005, [http://vote.nist.gov/resolutions_jan05.doc]).

- Requiring the EAC to develop standards on conflict of interest for testing laboratories, manufacturers, and/or other entities involved with voting machines (H.R. 470, H.R. 533, H.R. 550, H.R. 3094);
- Requiring the EAC to develop standards for the minimum number of voting machines at polling places (H.R. 533, H.R. 939, S. 17, S. 450);
- Requiring the use of open-source software in voting systems (H.R. 3094) and the development of relevant standards by the EAC (H.R. 533, H.R. 550, H.R. 939, S. 450);
- Prohibiting the use of wireless communications by voting systems (H.R. 550, H.R. 939, H.R. 3094, S. 450);
- Requiring public disclosure of information relating to certification of voting systems (H.R. 550);
- Requiring the EAC to establish standards for early voting (H.R. 533, H.R. 939, S. 17, S. 450) and for a federal write-in absentee ballot (H.R. 4141);
- Requiring manufacturers to follow security standards as specified by NIST (H.R. 939, S. 450);
- Requiring the EAC to establish a benchmark for voter error-rates (H.R. 939, S. 450);
- Requiring EAC certification of technological security of state voter registration systems (H.R. 939, S. 450);
- Prohibiting states from not registering certain voters or removing them from registration roles unless accuracy standards established by NIST are met (H.R. 3094).

None of the above bills have received committee or floor action in either chamber.

Appendix 1. Section-by-Section Summary of the *VVSG*

Volume I

Section 1 lays out the overall objectives for the guidelines: to specify what a voting system should do — how it should function and perform — as well as documentation requirements and evaluation criteria for certification. It describes background on the history of the guidelines and describes what a voting system is — not just a voting machine but also software and documentation relating to steps in the election process ranging from ballot definition through system audit.[46] It characterizes voting systems as either paper-based (such as punchcard and optical scan systems) or direct recording electronic (DRE), which are the two kinds of computer-assisted system currently in use, and distinguishes precinct- and central-count systems, but it recognizes that the distinctions may blur with future technology. This section also describes application of the guidelines and test specifications, pointing out that commercial off-the-shelf (COTS) products are exempt from some aspects of certification if they are not modified for use in a voting system. The *VVSG* contains a new subsection, a "conformance clause," which broadly defines what is required of

[46] This definition is similar to that in both the 2002 *VSS* and Sec. 301(b) of HAVA. The *VVSG* defines a voting system as

> The integrated mechanical, electromechanical, or electronic equipment and software required to program, control, and support the equipment that is used to define ballots; to cast and count votes; to report and/or display election results; and to maintain and produce all audit trail information. It additionally includes the associated documentation used to operate the system, maintain the system, identify system components and their versions, test the system during its development and maintenance, maintain records of system errors and defects, and determine specific changes made after system certification. A voting system may also include the transmission of results over telecommunication networks. (Vol. 1, p. A-35)

HAVA defines a voting system as

> (1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used—
> (A) to define ballots;
> (B) to cast and count votes;
> (C) to report or display election results; and
> (D) to maintain and produce any audit trail information; and
> (2) the practices and associated documentation used—
> (A) to identify system components and versions of such components;
> (B) to test the system during its development and maintenance;
> (C) to maintain records of system errors and defects;
> (D) to determine specific system changes to be made to a system after the initial qualification of the system; and
> (E) to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

those implementing the specifications in the guidelines and is a common feature of standards documents.

Section 2 describes the functional capabilities that a voting system is expected to have and is the longest chapter in the *VVSG*. Required capabilities include the following:

- *Security*. This involves both technical and administrative controls and is discussed in detail in Section 6.
- *Accuracy*. This involves both accurate recording and error detection, and specifies that DREs must retain redundant records of all votes cast.
- *Error Recovery*. Systems must be able to recover from malfunctions and resume operating with data intact.
- *Integrity*. Systems must be protected against outside perturbations such as loss of power or attempts at improper data inputs, and must record and maintain specific audit data.
- *System Audit.* Generation of audit records is to be largely automated, including continuous "real-time" data on machine status along with accurate time and date information, and error messages where appropriate. COTS operating systems must have specific protections against vulnerabilities that could affect audit data.
- *Election Management System.* This involves databases that assist officials in performing a wide range of functions, from defining political subdivisions through the processing of election audit reports.
- *Human Factors.* This subsection has been greatly expanded and revised. The standards in it are based on three principles — nondiscriminatory access to voting, accurate capture of ballot selections, and preservation of ballot secrecy. It contains more than 50 specific provisions describing required and recommended features responding to disabilities relating to vision, dexterity, mobility, hearing, speech, and cognition, as well as limited English proficiency and alternative language accessibility. It also contains interim[47] provisions relating to usability for all voters, based on both HAVA requirements and established usability principles.
- *Vote Tabulating Program.* Systems must have software for tabulating votes that is flexible, accurate, and includes monitoring and audit functions.
- *Ballot Counter.* Systems must have accurate, tamper-proof ballot counters that are visible to election officials.
- *Telecommunications.* Systems that use telecommunications must transmit data with no alteration or unauthorized disclosure.
- *Data Retention.* Systems must provide for retention of records in accordance with applicable federal law.
- *Prevoting Functions.* Systems must support preparation, installation, and control of ballots and election programs; testing for readiness;

[47] Only interim provisions are provided because of the limitations of existing research on high-level performance-based requirements (*VVSG*, vol. 1, p. 2-33 – 2-34).

and verification of functions both centrally and at the polling place.

- *Voting Functions.* This involves ensuring that only properly tested, activated, and functioning devices are used in voting, and that systems facilitate accurate and secret casting of ballots and respond appropriately to power or telecommunications interruptions.
- *Postvoting Functions.* Systems must accumulate and report both results of the election and audit trails and prevent additional voting after the polls are closed.
- *Maintenance, Transportation, and Storage.* Systems must be capable of being stored and transported without degradation in capabilities.

Section 3 covers requirements for voting system hardware, from printers to voting devices to paper ballots to back-office computer equipment, regardless of source. These include

- *performance* requirements such as accuracy;[48] operational specifications such as electricity supply, storage, and ability to operate under a range of environmental conditions; vote recording specifications for voting booth, paper ballots, marking devices, ballot boxes, various features of DREs, and so forth; ballot reading and processing specifications for machine readers and DREs; and specifications for printers and removable storage media, and for data management;
- *physical* requirements, especially for transport and storage of equipment;
- *design, construction, and maintenance* requirements, with an emphasis on best commercial practice for design, "the lowest level [of malfunction] consistent with cost constraints,"[49] an average time-to-failure (called MTBF or mean time between failures) in testing of no less than 163 hours[50] with time to repair short enough that the system is available for at least 99% of the time it is needed,[51] the presence of features to assist in the reliability and maintainability of the system, proper product labeling, quality workmanship, and safe design and construction.

[48] This is machine accuracy, not voter accuracy. The standard is one or fewer errors per 10 million events (although the maximum error rate permitted in tests is 1 in 500,000, a rate 20 times higher than the nominal standard but still far smaller than the margin of victory in almost any election; and the maximum false-rejection rate for paper ballots is 2%, although presumably such ballots could be hand-counted if necessary in an actual election).

[49] *VVSG,* vol. 1, p. 3-21.

[50] The *VVSG* (vol. 1, p. 3-22) describe a "typical…scenario" as 45 hours — 30 hours of set-up and testing and 15 hours of operation during the election — so this standard could arguably be interpreted to permit a failure once every 3-4 uses on average. See the section on scope of revisions above for discussion of this issue.

[51] Specifically, availability is defined as the ratio of the average time between failures and that time plus the average time it takes to repair the system.

Section 4 covers requirements for voting system software, including firmware,[52] regardless of programming language or source. These include

- *design and coding*, including the *kinds* of programming language permitted; the importance of stable computer code[53] and modular software;[54] the way program controls are constructed, and the way components are coded, named, and commented;
- *data and document retention,* including accurately maintaining voting and audit data for at least 22 months after the election, and proper security and failure protection for devices;
- *audit record data,* including ballot preparation, system readiness,[55] documentation of operations during diagnostic routines and ballot casting and counting,[56] and detailed vote-tally data including overvotes and undervotes;
- *vote secrecy for DREs,* including erasing from temporary storage and displays the selections of previous voters immediately after a vote is cast or cancelled.

Section 5 covers telecommunications requirements for systems operation and reporting election results, including performance, design, and maintenance characteristics. It covers technologies such as dial-up communications, cable and wireless, and high-speed lines, regardless of provider. It covers data transmission from election preparation through preservation of data and audit trails after the election, including voter authentication, ballot definition, vote transmission, vote counts, and lists of voters, and other transmissions relating to voting-system operation. Requirements are the same as those contained in Section 3 for accuracy, durability, reliability, maintainability, and availability. For wide-area networks (WANs),[57]

[52] The *VVSG* defines firmware as "computer programs (software) stored in read-only memory (ROM) devices embedded in the system and not capable of being altered during system operation." (*VVSG*, vol. 1, p. A-16). One example is the BIOS programs on a personal computer that are used to start the operating system when the device is first booted up. However, in practice firmware alteration may be possible, as happens for example when a BIOS is upgraded.

[53] This is to prevent code from being changed after certification except for certain security purposes.

[54] This is software designed in discrete, autonomous components or modules that can be connected together and managed independently by computer programmers (see, for example, *Webopedia*, "What is modular architecture?" 30 October 2001, [http://www.webopedia.com/ TERM/m/modular_architecture.html]).

[55] This is not defined but includes such things as verification of software and hardware status before votes are counted, testing for the correct installation of ballot formats, and checking memory locations and data paths.

[56] This includes such things as error messages, zero totals, and other critical status information, and operator interventions.

[57] This is simply a computer network that spans a comparatively wide geographic area, as opposed to a local-area network (LAN). A WAN often consists of 2 or more LANs and is

(continued...)

outside providers or subscribers are not permitted access inside the network boundary, no control resources for the network are permitted outside the border, and the system cannot be vulnerable to a single point of failure. The system must notify users of successful and unsuccessful transmission and actions taken if transmission is unsuccessful.

Section 6 addresses essential security capabilities for all voting systems components regardless of source, ownership, or location, and includes controls to minimize errors and accidents, protect from malicious manipulation, identify fraudulent or erroneous changes, and protect voting secrecy. The section cites the importance of effective security practices by jurisdictions but does not address them.[58] Topics covered include

- *access control,* including general access control and individual privileges, and specific measures such as passwords and encryption;
- *equipment and data security,* including physical security for polling places and ballot-counting locations;
- *software security*, including installation requirements and testing of firmware, protection against malicious software,[59] and software distribution and validation requirements to ensure that no unauthorized modifications have been made (this is a new set of detailed requirements)[60];
- *telecommunications and data transmission,* including access control, integrity of transmission, use of encryption to protect data from interception, use of intrusion detection methods, protection against external threats to COTS software, and specific requirements for DREs that transmit data over public networks and for wireless communications (this latter subsection is new), including the caution that the use of wireless communications should be approached with "extreme caution"[61];
- *optional requirements for voter-verified paper trail (VVPAT),* including requirements for handling spoiled and accepted paper records, preserving voter privacy and vote secrecy, audit and election data such as linking electronic and paper records, machine readability of paper records, tamper protection, printer reliability and maintenance, and durability of the paper record, as well as usability and accessibility requirements (this subsection is new). Section 7 requires that vendors and third-party suppliers implement quality-

[57] (...continued)
often connected through a public network such as a telephone system (*Webopedia*, "Wide-area network," February 12, 2003, [http://www.webopedia.com/TERM/W/wide_area_network_ WAN.html]).

[58] They are intended to be covered in a forthcoming set of best practices.

[59] These include viruses, Trojan horses, and so forth.

[60] This includes the requirement to deposit a copy of the software in an EAC-designated repository for comparison during the validation process.

[61] *VVSG,* vol. 1, p. 6-26.

assurance programs to help ensure conformance with *VVSG* requirements. It includes testing, inspection, and documentation requirements.

Section 8 describes requirements for configuration management, including descriptions of the policy, identification and acquisition of component items; procedures used to decide what components are included in the product as it is developed, submitted for certification, and throughout its useful life cycle; how configuration is controlled to prevent unauthorized changes; product release; configuration audits; and any automated tools used in configuration management.

Appendix A is a glossary, which has been substantially expanded in the *VVSG*. It now lists sources and keywords (called "association") for each entry as well as definitions.

Appendix B lists reference documents that have been incorporated into the guidelines in whole or in part. Several new references have been added and others updated.

Appendix C describes suggested best practices for election officials with respect to usability and security requirements added in the *VVSG*. These are drawn from the TGDC draft, in which they were embedded in Sections 2 and 6.[62]

Appendix D describes independent dual verification (IDV) systems, of which VVPAT is one type. Such systems produce at least two separate, independent ballot records that voters can verify before casting and that can be compared in a post-election audit. Examples include

- *split-process architecture,* where the vote is captured on paper or another medium and then taken to a verification station, where a separate, voter-verified record is made and stored;
- *end-to-end systems,* which permit voters to verify ballot choices, even after casting, without compromising ballot secrecy. Voters are typically given a receipt with a code number that they can check later, such as on a website. The use of cryptographic techniques prevents voters from using the receipt to prove how they voted while ensuring accurate verification with a very high degree of probability;
- *witness systems,* which independently record voters' choices through a means such as a camera that takes a picture of the choices displayed on a DRE screen; and
- *direct systems,* such as VVPAT, which produce a second record that the voter may directly verify before casting.

[62] Some recommended best practices relating to language proficiency, usability, and voter-verified paper ballots appear to have been omitted from the EAC *VVSG* draft. This may have been a result of typographical error.

The appendix also discusses issues in handling records produced by IDV systems, such as how to structure records to ensure comparability in audits, and describes desirable characteristics for each type.[63]

Appendix E is a NASED technical guideline produced to assist vendors in meeting requirements originally in the 2002 *VSS* to improve readability for persons with low vision or color blindness.

Volume II

Section 1 provides an overview of the certification testing process, which focuses on operational accuracy and failure, system performance under normal and abnormal conditions, and the quality of documentation. There are five different categories of testing: functionality, hardware, software, system integration, and documentation of practices for quality assurance and configuration management. Testing is to be performed according to a test plan and in a designated sequence — from initial examination through delivery of the test report to the EAC — that follows specified practices. Vendors are required to submit for testing the specific system configuration that will be offered to election jurisdictions, and testing is required for both new systems and previously certified ones that have been modified. Some hardware is exempt from some aspects of testing, including certain kinds of commercial equipment that meet established standards and other criteria of compatibility and function. If more than one laboratory is involved in testing, one must be designated as the lead laboratory. Testing activities must be observed by one or more independent, qualified observers. A test lab must witness the final system build by the vendor for certification. The EAC is to develop a process for resolving issues that arise about interpretation of the *VVSG* for testing.

Section 2 describes the documentation, called the Technical Data Package (TDP), that the vendor must submit at the beginning of the certification process. The TDP includes descriptions of system design (including specifications and constraints); functional capabilities; performance specifications; applicable standards; requirements for compatibility, operation, maintenance, and support; and quality assurance and configuration management practices. The TDP must identify any proprietary information that is not to be publicly released and must include a security specification, among other things. Previously certified systems that have been modified must be submitted with notes including a summary and specification of the changes to the system, changes to documentation, and documentation of vendor testing.

Section 3 describes testing to confirm functional capabilities as required by Volume I, Section 2. It stresses the importance of flexibility in testing to accommodate variations in design and technology and any additional capabilities not described in the *VVSG*.

[63] These characteristics are written in the same basic form as requirements are in the new parts of the *VVSG* sections, and they presumably could be incorporated as requirements in a future version.

Section 4 describes testing of hardware components to confirm that they function properly according to the requirements in Volume I, Section 3. It includes both operational tests and environmental tests of nonoperating equipment, including responses to handling, vibration, low and high temperature, and humidity, as well as response to temperature and power variation during operation and other electrical disturbance. Testing is also done for maintainability and reliability. For accuracy testing, a system will be rejected if it makes an error before correctly counting 26,997 ballot positions consecutively, and will be accepted if it makes no errors in consecutively counting 1,549,703.[64] Systems that fall between these two thresholds are discussed in Appendix C.

Section 5 describes testing for proper software functioning. Code examination is not required for unmodified COTS software, and if it is also general-purpose, and not used for voting, detailed examination is not required. Source code is examined for conformance to vendor specifications, adherence to requirements in Volume I, Section 4, and use of specified control constructs[65] and coding conventions.

Section 6 describes testing to confirm proper functioning of integrated voting-system components, under normal and abnormal conditions, and including telecommunications, security capabilities, accessibility, and any functions that exceed *VVSG* requirements. Testing includes configuration audits comparing components and functions with technical documentation of them provided by the vendor.

Section 7 describes examination of a vendor's documented configuration management and quality assurance processes, to verify conformance to *VVSG* requirements. However, on-site examination is not required.

Appendix A contains a recommended outline for the laboratory's testing plan, called the National Certification Test Plan, which is intended to document the development of certification tests. The plan is to be developed after the receipt of a TDP from the vendor and is therefore specific to a particular system being submitted for certification.

Appendix B contains a recommended outline for the laboratory's test report, called the National Certification Test Report. A full report is required on initial certification of a system, but partial reports can be prepared for certification of subsequent modifications. The report is to include a recommendation to the EAC for approval or rejection of the application for certification, as well as descriptions of any uncorrected deficiencies. Those deficiencies not involving loss or corruption of data will not necessarily lead to rejection.

[64] These are chosen based on the assumption that errors occur according to a binomial probability distribution and to provide 95% confidence that the test yields neither a false positive (the system actually meets the accuracy standard but is rejected) or a false negative (the system does not actually meet the accuracy standard but is accepted).

[65] They include typical computer routines such as "if-then-else" and "do-while" (*VVSG*, Vol. II, p. 5-3).

Appendix C, on test-design criteria, describes the principles used to design the testing process. Design must balance the need to produce sufficient data to support the validity of the test, on the one hand, with the need for reasonable cost of testing, on the other. The design approach used in the *VVSG* is to determine if the object being tested achieves or exceeds a minimum threshold of performance. Tests are continued until that threshold is reached or the object fails.

Appendix 2. Abbreviations

ANSI. The American National Standards Institute, a private, nonprofit organization that administers and coordinates the U.S. voluntary private-sector standardization system.

BIOS. Basic Input/Output System, a form of ROM used in computers to provide basic functions such as control of disk drives.[66]

COTS. Commercial Off-the-Shelf, referring to readily available, commercial software or hardware.

DRE. Direct (or Digital) Recording Electronic Voting System, a kind of voting system where ballot choices a voter makes are recorded directly onto electronic media rather than paper.

EAC. The federal Election Assistance Commission, a four-member, bipartisan commission, established by HAVA, that replaced the former Office of Election Administration in the Federal Election Commission.

FEC. The Federal Election Commission, which was responsible for federal guidance and information relating to election administration before the enactment of HAVA.

FISMA. The Federal Information Security Management Act, first enacted as part of the Homeland Security Act of 2002 (P.L. 107-292) and later in modified form in the E-Government Act of 2002 (P.L. 107-347).

HAVA. The Help America Vote Act of 2002, which, among other things, established the EAC, required it to develop the *VVSG*, and established a mechanism for that.

IDV. Independent Dual Verification refers to "electronic voting systems that produce multiple [at least two] records of ballot choices whose contents are capable of being audited to high levels of precision."[67]

IEC. The International Electrotechnical Commission, a standards organization for electrical, electronic and related technologies.

IEEE. The Institute of Electrical and Electronics Engineers, an international professional organization that is also involved in the development of standards.

IESG. The Internet Engineering Steering Group is part of the Internet Society, a professional organization. The IESG is responsible for the technical management of IETF activities.

[66] "BIOS," *Webopedia,* [http://www.webopedia.com/TERM/B/BIOS.html], n.d.

[67] *VVSG,* Vol. 1, p. D-1.

IETF. The Internet Engineering Task Force, a community of professionals involved in the evolution of Internet architecture, with the goal of improving Internet operations through the development of standards, best practices, and other information.

ISO. International Organization for Standardization, a federation of the principal standards bodies from countries around the world.

ITA. Independent Testing Authority, a laboratory accredited by NASED to perform certification testing of voting systems.

LAN. Local-Area Network, referring to a computer network that spans a comparatively small area, such as an office or building, as opposed to a wide-area network (WAN).

MTBF. Mean Time Between Failures, defined in the *VVSG* as "the value of the ratio of the operating time [of a voting system] to the number of failures which have occurred in the specified time interval."[68]

NASED. The National Association of State Election Directors, a professional association that, before HAVA, administered the national certification program for voting systems.

NIST. The National Institute of Standards and Technology, required by HAVA to provide assistance to the EAC in the development of the *VSS* and the process for certification of voting systems.

NVLAP. The National Voluntary Laboratory Accreditation Program, a NIST program involved in the identification and assessment of candidates testing laboratories for the *VVSG* certification program.

OEA. The former Office of Election Administration within the FEC. OEA was abolished upon the establishment of the EAC.

ROM. Read-Only Memory, a kind of computer memory in which data has been prerecorded and which is retained when the computer is turned off. It often contains small BIOS programs necessary to start the computer when power is turned on.[69]

TDP. Technical Data Package, the "vendor documentation relating to the voting system required to be submitted with the system as a precondition of certification testing."[70]

TGDC. Technical Guidelines Development Committee, a 15-member committee established by HAVA and chaired by the Director of NIST. The main function of the TGDC is to make recommendations to the EAC on the *VVSG*.

[68] *VVSG*, Vol. 1, p. 3-22.

[69] See "ROM," *Webopedia*, [http://www.webopedia.com/TERM/R/ROM.html], n.d.

[70] *VVSG*, Vol. 1, p. A-30.

VSPR. Voting System Performance Rating, an independent project designed to develop performance rating standards for U.S. voting systems.

VSS. The federal voluntary *Voting Systems Standards* (*VSS*) developed by the FEC.

VVPAT. Voter-Verified Paper Audit Trail, a printed record of all of a voter's ballot choices that the voter can review before the ballot is cast. This term is usually used to refer to an IDV method used with DREs, rather than standard paper-based ballot systems such as optical scan.

VVSG. The federal *Voluntary Voting System Guidelines,* developed by the EAC with assistance from NIST, as required by HAVA.

WAN. A Wide-Area Network, referring to a computer network that spans a comparatively wide geographic area, as opposed to a local-area network (LAN).