Core Requirements and Testing Subcommittee Task 1

"Due Diligence"

Confidential and pre-decisional – for discussion use only

David Flater

Rev. 2004-11-24

Preface

This document is a pre-decisional memo for use by the Core Requirements and Testing Subcommittee. It was begun based on actions accepted at the 2004-11-03 teleconference. It is expected that the information contained herein will have reference value to the subcommittee and may be recycled in some form in the final deliverable.

Actions left for others to do are underlined and italic.

FIXMES (unfinished business) are shown in red.

Writing requirements

Several stakeholders (e.g. [Shamos 2004-09-20]) have expressed a need for quantitative evaluation of voting systems that yields something more than a simple pass-fail verdict. To enable this, many of the requirements in [2002VSS] will need to be rewritten. The following examples illustrate the issue.

Example requirement text	Impact on testing
The unit shall respond to all user input in a timely fashion.	Vague requirement leaves tester in the position of determining what is considered "timely," creates opportunities for inconsistent evaluation and challenges by vendors.
The unit shall respond to all user input in 3 seconds or less.	Good requirement leading to pass-fail verdict. Vendor could still challenge that the set of user inputs chosen by the ITA is atypical or argue about what constitutes a response.
The ITA shall measure and report the mean response time and worst response time over the following set of user inputs, employing the test ballot form defined in Section XYZ: opening the ballot; voting for one randomly selected candidate in each contest; […]. Units with worst response time of 1 second or less shall be graded "Acceptable" on this criterion. Units with worst response time of 3 seconds or less shall be graded "Marginal" on this criterion. Units with worst response time exceeding 3 seconds are non-conforming.	Excellent requirement leading to informative and difficult-to-challenge results. In addition to a general pass/fail verdict, stakeholders will receive a report identifying specific areas of marginal or unacceptable performance as well as quantitative measurements of that performance.

Some argue against having any pass/fail criteria at all. [5.0 Comments 2003-10-16] Comment 279 comments: "The standard should not be judging what is acceptable, but rather setting technical criteria and measurement techniques to allow systems to be evaluated." This is a matter to be resolved in discussion with stakeholders. However, it seems unlikely that they would want to do away with the pass/fail baseline that protects against significant failures being buried among masses of quantitative data.

Another issue has been the use of requirements that specify design elements (e.g., the unit shall use memories with parity bits) instead of the desired qualities / performance (e.g., single-bit errors shall be detected and corrected). Design-constraining requirements are controversial because vendors would like the freedom to provide the desired qualities / performance in different ways. However, in cases where vendors are unable to determine for themselves whether or not a given design is conforming, they may welcome design constraints as a way to avoid repeated failures and costly retesting of their products.

Sources of requirements (references)

Standards, draft standards, regulations, and guidelines

[2002VSS] 2002 Voting Systems Standards, available from http://www.fec.gov/pages/vssfinal/vss.html.

[P1583/D5.3.1] IEEE Draft Standard for the Evaluation of Voting Equipment, draft 5.3.1, 2004-10-08, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

[CoE 2004-09-30] Council of Europe, Committee of Ministers to member states on legal, operational, and technical standards for e-voting, adopted by the Committee of Ministers on 2004-09-30 at the 898th meeting of the Minister's Deputies, e-mail from Lori Steele, 2004-11-10.

[HAVA] Help America Vote Act of 2002, Public Law 107-252, 2002-10-29.

[EML3] Election Markup Language v3.0, 2003-02-24, available from http://www.oasis-open.org/committees/election/index.shtml.

Accessibility/usability punted to Sharon, but I am aware of the following references:

[SP 500-256] Sharon J. Laskowski et al., "Improving the Usability and Accessibility of Voting Systems and Products," NIST SP 500-256, 2004-05.

[508] Section 508 of the Rehabilitation Act: Electronic and Information Technology Accessibility Standards, 2000-12-21, available from http://www.access-board.gov/508.htm.

[ADA] ADA Checklist for Polling Places, 2004-02, available from http://www.usdoj.gov/crt/ada/votingchecklist.htm.

[CIF] ANSI/INCITS 354-2001, Common Industry Format (CIF) for Usability Test Reports, 2001-12-12.

[ISO 13407:1999] Human-centred design processes for interactive systems.

[ISO 9241] Ergonomic requirements for office work with visual display terminals (VDTs) (many parts).

Security punted to Nelson.

[CC] Common Criteria.

… many NIST pubs …

See also [2002VSS] Vol. I Appendix B.

Issue lists

[D5.3.1 Comments 2004-10-19] Comments for d5-3-1 dated 10-19-2004 revC.xls, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

Older issue lists remain relevant because some issues are dismissed without a solution, for various reasons. Also, comments that were applicable to earlier IEEE drafts remain applicable to [2002VSS].

[5.0 Software Comments 2004-09-01] Software comments 5.0 (9-01-04).xls, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

[5.0 Security Comments 2004-08-18] Security extract V5 Comments – 2nd NJ Meeting.xls, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

[5.0 Reliability Accuracy Comments 2004-09-06] 5.0 Comments Section 5.2 & 6.2 (9-6-04).xls, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

[5.0 Accessibility Comments 2004-08-01] V5 Ballot Accessibility Comments – TG3 (8-1-04) .xls, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

[5.0 Environmental 2004-08-15] 5.0 Comments Section 5.4 & 6.4.xls, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

[5.0 EMC 2004-08-23] 5.0 Comments Section 5.5 (8-23-04).xls, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

[5.0 Provisional 2004-09-10] Gough-Provisional Ballot Comments.xls, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

[5.0 COTS 2004-06-18] Resolutions for COTS Comments for Draft 5.0 of IEEE P-1583, http://www.lipsio.com/COTS/docs/COTS.resolved.html.

(Skipping VVAT spreadsheets since they have no applicability to [2002VSS])

[5.0 TDP 2004-04-23] 5.0 p1583 _TDP-Proposed resolution_Apr04.xls, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

[5.0 Comments 2003-10-16] Ballot Comment Form 5-0 10-16-2003.xls, available from http://grouper.ieee.org/groups/scc38/1583/private/ (password-protected).

Requests for proposals

[AZ] "OCR and DRE Voting Equipment – Statewide," Request for Proposal, Arizona, 2003. E-mail from Allan Eustis, 2004-10-12.

[CO-REG] "Statewide Voter Registration System," Request for Proposals # DOS-HAVA-0001, Colorado, 2004-01-16, formerly available from http://www.sos.state.co.us/pubs/hava/hava_main.htm (now gone).

[CO-IVV] "Independent Verification and Validation for SCORE Project," Request for Proposals # DOS-HAVA-0002, Colorado, 2004-06-03, formerly available from http://www.sos.state.co.us/pubs/hava/hava_main.htm (now gone).

[GA] Request for Proposal GTA000040, Georgia, 2001. E-mail from Merle King via Allan Eustis, 2004-10-11.

[MD] "Direct Recording Electronic Voting System and Optical Scan Absentee Voting System for Four Counties," Project Number SBE-2002-01, Maryland, 2001-07-17, available from http://www.elections.state.md.us/citizens/voting_systems/voting_system_procurement.html.

[MI] Invitation To Bid # 071I4001011, Michigan, 2003, available from http://www.michigan.gov/sos/0,1607,7-127-1633_11619_27151-77943--,00.html.

[OH-VOT] "Statewide Voting System(s)," Request For Proposal # SOS0428365, Ohio, 2003-05-23, available from http://www.sos.state.oh.us/sos/hava/index.html.

[OH-REG] Request For Proposal # SOS032786279, Ohio, 2003-04-09, available from http://www.sos.state.oh.us/sos/hava/index.html.

[UT] "Executive Summary: Voting Equipment Selection Committee Request for Proposal," Utah. E-mail from Allan Eustis, 2004-10-07.

Testimony

[Coney 2004-09-22] Lillie Coney, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Conrad 2004-09-22] Frederick Conrad, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Deutsch 2004-09-21] Herb Deutsch, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Fischer 2004-09-20] Eric A. Fischer, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Gaston 2004-09-20] Charles A. Gaston, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Golden 2004-09-22] Diane Cordry Golden, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Jones 2004-09-20] Douglas W. Jones, testimony to EAC, available from http://www.cs.uiowa.edu/%7Ejones/voting/nist2004.shtml.

[Jones 2004-09-23] Douglas W. Jones, supplemental testimony to EAC, available from http://www.cs.uiowa.edu/%7Ejones/voting/nist2004supp.shtml.

[King 2004-09] Merle S. King, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Noren 2004-09] Wendy S. Noren, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Redish 2004-09-22] Janice Redish, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Relton 2004-09-21] Joy Relton, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Saltman 2004-09-20] Roy G. Saltman, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Shamos 2004-09-20] Michael I. Shamos, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

[Wallach 2004-09-20] Dan S. Wallach, testimony to EAC, available from http://vote.nist.gov/PanalistandPublicTestimony.html.

Categories

Requirements and issues can be categorized according to several different taxonomies. *The definition and maintenance of these taxonomies is part of Task 2.*

Taxonomy 1: the election management process

Process model: Anatomy of a Vote21.ppt as received from Mr. Schutzer 2004-10-27.

This model is currently being revised.

Registration	Process new registrations and change requests, process lists of ineligible voters, deliver certified registration lists to precincts.
Pre-planning stage	Specify requirements, select vendors/products, store machines.
Planning stage	Prepare guidelines, conduct training, design ballot.
Set-up stage	Deliver, install, test equipment; adjust settings, parameters; train administrators.
Execute stage	Authenticate voters, administer voting process, transport votes to central counting locations, dispute resolution/recount.
Post analysis stage	Store machines, analyze/learn/adjust, revise training, modify equipment/procedures.

Other process models that may be of interest have been forwarded for posting on the TGDC web site:

An elaborate draft model by Roy Morgan (ed.) et al., NIST.doc, 2001-04.

OASIS model from EML v??, votemdloasis.jpg and votemdloasis2.jpg.

Process model of software qualification from SysTest, systest_software_qualification_flowchart.doc, 2003-08-01.

Flowchart from ESS, Visio-ESSFLOW2.pdf, 2003-06-16.

Flowchart of VoteHere election verification scheme, in C. Andrew Neff and Jim Adler, "Verifiable e-Voting: Indisputable electronic elections and polling places," 2003-08-06.

Taxonomy 2: roles in the voting system

Roles are not always mutually exclusive. For example, voting equipment and tabulating equipment might be the same equipment.

Role	Description
Voting equipment	Equipment that the voter uses to cast a ballot.
Assistive equipment	Equipment to enhance accessibility. *Punted to Sharon.*
Tabulating equipment	Equipment that is used to count votes.
Archiving equipment	Equipment that is used to maintain an archival record of the audit trail to be used in case of recount.
Audit trail	That which is archived.
Networking equipment	Equipment used to transmit registration data, voter input, ballot forms, ballot images, counts, etc.
Testing equipment	Equipment used for testing and diagnosis of problems.
Voter registration system	The subsystem used to maintain registration data. [2002VSS]: "A set of processing functions and data storage that maintains records of eligible voters."
Registration data	Data about voters and their eligibility to vote.
Election database	(From [2002VSS]) "A data file or set of files that contains geographic information about political subdivisions and boundaries; all contests and questions to be included in an election; and the candidates for each contest." (N.B., it is possible to design a voting system that does not have an election database, but the applicable standards all assume that it exists.)
Ballot form	The blank ballot template that voters must fill in. There may be many different ballot forms applicable in a given election. (C.f. "ballot configuration" and "ballot format" in [2002VSS].)
Ballot image	A filled-in ballot form, in either physical or electronic representation. The record of all votes produced by a single voter. (C.f. "ballot set" in [2002VSS], "cast vote record" in [P1583/D5.3.1].) Flavors: absentee ballot; provisional ballot; challenged ballot; spoiled ballot; etc.
Accreditation body	(From [P1583/D5.3.1]) "An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard." FIXME: substitute NVLAP terminology?
Testing authority	An independent organization responsible for assessing the conformance of voting systems against a recognized standard, and for formally confirming the status of those that meet the standard. (C.f. "ITA")
Interpretation authority	A standards organization responsible for issuing binding interpretations of voting systems standards when vendors challenge the interpretation of a testing authority, and for revising the standard to eliminate the offending ambiguities.
Political	(From [2002VSS]) "Any unit of government, such as counties and cities but often excepting

subdivision	school districts, having authority to hold elections for public offices or on ballot issues."
Election official	A public official with the authority to perform certain election administration duties, pursuant to federal, state, and local election law.
Certifying authority	An election official who formally confirms that a voting system meets all applicable requirements for use within some jurisdiction.
Voter	One who casts a ballot.
Poll worker	One who is authorized to perform certain election administration duties at a particular polling place.
Poll observer	One who watches the process at a precinct or central tabulating location but is not otherwise involved.
Vendor	One who manufactures, maintains, and/or repairs the equipment and associated software, and/or provides training in its use. An equipment contractor.
Candidate	One who is running/standing for office.
Judge	One with the judicial authority to interpret, enforce, or overturn the rules governing an election.
Lawmaker	One with the legislative authority to create or alter the rules governing an election.
Plaintiff	One who challenges some aspect of an election, including the eligibility of individual voters or the validity of individual ballots.
The public	Everyone else. This role is used in defining what information should/shall be published openly.

Taxonomy 3: qualities of the voting system

Functionality	Functionality refers to the scope of functions that the system is designed to perform. For example, can it handle instant runoff voting? This is separable from the concern of whether it performs all of these functions correctly, verifiably, securely, etc.
Correctness	Correctness encompasses all logical constraints on the recording of votes, registration of voters, etc. At http://www.coyotewind.com/voting/SecureVoting.htm (as of 2004-11-09), Andrew Glassner of Coyote Wind, LLC breaks out the following sub-categories with respect to the recording of votes: Completeness: every vote is recorded. Accuracy: every vote is recorded correctly. Parsimony: each vote is recorded only once. Actuality: only actual votes are recorded. Persistence: recorded votes cannot be lost. Indelibility: recorded votes cannot be changed.
Testability and verifiability	Correctness should be testable and verifiable. Design and administrative practices can help or hinder the ability to test the equipment or to verify the correctness of the count. C.f. transparency, simplicity.
Trustworthiness (transparency and security)	*Security punted to Nelson* What is necessary is for the voters and the losing candidates to be satisfied that the results are valid. Transparency and security are means to that end.
Reliability	Reliability includes reliability of equipment, including shelf-stability; reliability of software, including error recovery; and systemic reliability, including availability. Machinery that does not work after a period of storage is a straightforward example of hardware unreliability. However, in more complex cases that are possibly attributable to operator error, it is nontrivial to decide whether the problem is actually a badly designed or buggy user interface (c.f. Usability). *Aspects of the voting system less amenable to testing under controlled conditions*

	(e.g., voters, poll workers) should be addressed by those with experience managing elections, and/or Sharon.
Accessibility	*Punted to Sharon*
Usability (ease of use)	*Punted to Sharon*
Capacity	Throughput, volume testing, stress testing.
Simplicity	Simplicity of design facilitates independent review.
Privacy	To prevent coercion, most jurisdictions require that the voter be enabled to cast a ballot without anyone else knowing how he or she voted.
Secrecy	To prevent vote selling, most jurisdictions require that no one, including the voter, should receive proof of how any particular voter voted.
Portability	Equipment must be movable.
Maintainability	Equipment must be maintainable.
Compatibility	Including forward and backward compatibility and interoperability.
Compliance	All behaviors of the voting system, including the deployment and maintenance of voting equipment at the precinct level, must remain in compliance with applicable federal, state, and local election law.
Localization	States may place additional requirements on voting systems or vendors that reflect issues that are completely local. These may nonetheless be of interest for their possible ramifications in the context of federal guidelines.

Taxonomy 4: "by the book"

Requirements can be categorized according to which section of the applicable standard they relate to. This is expedient if only one standard is applicable, as it simplifies traceability. For examples, see FVSS 2002 Vendor Testing and TDP Trace Rev 04.doc from Wyle and 2002 Standards Checklist.xls from Ciber (put on web site).

Taxonomy 5: testing and verification activities

Requirements can be categorized according to which testing and verification activities are applicable. For an example, see FEC VSS Requirements Trace.xls from Steve Freeman of ?? (put on web site).

Survey of requirements

Taxonomy 1: the election management process

Registration

[2002VSS] N/A

[P1583/D5.3.1] N/A

[D5.3.1 Comments 2004-10-19] N/A

[CoE 2004-09-30] Sec. 2 (registration shall not be an impediment), Sec. 39-41 (registration requirements), Sec. 86 (authenticity, integrity, availability of register), Sec. 88 (registration time limits).

[HAVA] Sec. 303 requires computerized registration.

[AZ] N/A

[CO-REG] Categories V-1 through 5 (voter registration).

[CO-IVV] Testing of registration system.

[GA] Sec. 2.4.5, p. 20 (election management system import/export of “voter registration information”).

[MD] Sec. 3.3.3, EMS import of voter registration totals.

[MI] p. 37 item i, EMS import/export of voter registration totals.

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] Supplement 2 (system requirements).

[UT] Nothing new.

Pre-planning stage

All applicable regulations and standards for voting equipment and qualification impact pre-planning by constraining the selection of vendors and equipment.

All state RFPs are examples of pre-planning in their entirety.

[2002VSS] Vol. I Sec. 2.6, Sec. 3.2.2 and Sec. 3.3.3 discuss storage. Vol. II Sec. 1.1 states: “Voting officials in many jurisdictions will use Volume II to guide system certification, procurement and acceptance requirements and processes, which may include additional requirements and adjustments to those requirements included in the Standards.”

[P1583/D5.3.1] Sec. 5.4 conditions apply to storage.

[D5.3.1 Comments 2004-10-19] N/A

[CoE 2004-09-30] Sec. 111-112 (certification).

[HAVA] N/A

Planning stage

[2002VSS] Vol. I Sec. 2.2.6; Sec. 2.3.1; Sec. 2.3.2; Sec. 3.2.3.

[P1583/D5.3.1] Sec. 7.10 (personnel deployment and training). Sec. 4.2 defines Election Management System, but this is out of scope according to the Abstract (page ii).

[D5.3.1 Comments 2004-10-19] N/A

[CoE 2004-09-30] Sec. 86-89 (security requirements in pre-voting stages).

[HAVA] N/A

[AZ] Sec. 4.20.1 (training), Sec. 6.4 (election management system).

[CO-REG] Categories A-1 (address library management), D-1 (district and precinct file management), E-1 through 8 (election management), P-1 through 4 (petition management).

[CO-IVV] N/A

[GA] Sec. 2.4.5 (election management system), Sec. 2.5.1 (training).

[MD] Sec. 3.3.3 (integration of election management component with state system), Sec. 3.3.10 (training and voter education).

[MI] pp. 36-38 (EMS), Sec. II-D (training and user information).

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] pp. 52-, some requirements on election management system and petition processing, if either one is provided.

[UT] Nothing new.

Set-up stage

[2002VSS] Vol. I Sec. 2.2.6; Sec. 2.2.7, “Accessibility;” Sec. 2.3.3 through 2.3.6; Sec. 6.

[P1583/D5.3.1] Sec. 7.10 (personnel deployment and training).

[D5.3.1 Comments 2004-10-19] N/A

[CoE 2004-09-30] N/A

[HAVA] N/A

[AZ] Sec. 6.1.3 and 6.2.1 (logic and accuracy testing).

[CO-REG] N/A

[CO-IVV] N/A

[GA] N/A

[MD] Sec. 3.3.13, transportation is to be provided by the vendor.

[MI] N/A

[OH-VOT] N/A

[OH-REG] N/A

[UT] Nothing new.

Execute stage

[2002VSS] Vol. I Sec. 2.2.7, “Accessibility;” Sec. 2.4, “Voting Functions,” and 2.5, “Post-Voting Functions;” Sec. 3.2.4 through 3.2.8; Sec. 6.

[P1583/D5.3.1] Requirements are spread throughout Sec. 5 (organized similar to Taxonomy 3).

[D5.3.1 Comments 2004-10-19] Many comments affecting security, usability, accessibility, reliability, and VVAT.

[CoE 2004-09-30] Requirements are spread throughout (organized similar to Taxonomy 3).

[HAVA] Title III.

[AZ] Section 6.

[CO-REG] N/A

[CO-IVV] N/A

[GA] Sec. 2.

[MD] Sec. 3.3.

[MI] Sec. II-B.

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] N/A

[UT] Nothing new.

Post analysis stage

[2002VSS] Vol. I Sec. 2.6, Sec. 3.2.2 and Sec. 3.3.3 discuss storage.

[P1583/D5.3.1] Sec. 5.4 conditions apply to storage.

[D5.3.1 Comments 2004-10-19] N/A

[CoE 2004-09-30] Paragraph 60 (the conclusions drawn from the audit process shall be applied in future elections and referendums).

[HAVA] Title II, Subtitle C authorizes the EAC to collect and publish data regarding election administration issues and lessons learned in previous elections.

[AZ] Sec. 6.1.5.3.14 and 15 (storage).

[CO-REG] N/A

[CO-IVV] N/A

[GA] N/A

[MD] Sec. 3.3.13, storage, transportation, and insurance are to be provided by the vendor.

[MI] N/A

[OH-VOT] N/A

[OH-REG] N/A

[UT] Nothing new.

Taxonomy 3: qualities of the voting system

FIXME: inconsistent treatment of "the vendor shall document" and drive-by references in minor text.

FIXME: [5.0 Comments 2003-10-16] contains 1019 comments applicable to [2002VSS] covering many aspects of the system. Some or all are redundant with the other issue lists.

Abbreviations

MTBF = Mean Time Between Failures

COTS = Commercial off-the-shelf, meaning hardware or software that is widely available and used without modification.

(VSS and IEEE) DRE = Direct Recording Electronic.

(IEEE) CVR = Cast Vote Record, record of all votes cast by a single voter, a.k.a. ballot image, ballot set.

(IEEE) VVAT = Voter-verifiable audit trail.

HAVA = Help America Vote Act.

NVRA = National Voter Registration Act of 1993.

ADA = Americans with Disabilities Act.

UPS = Uninterruptible Power Supply.

Functionality

[2002VSS] Section 2.2, "Overall System Capabilities," mentions election management, vote tabulation, and data retention. Requirements on election management functionality are given in Section 2.2.6; vote tabulation in Section 2.2.8; data retention in 2.2.11. Subsequent sections give requirements on the following subprocesses:

- 2.3 Pre-voting Functions
  - 2.3.1 Ballot Preparation
  - 2.3.2 Election Programming
  - 2.3.3 Ballot and Program Installation and Control
  - 2.3.4 Readiness Testing
  - 2.3.5 Verification at the Polling Place
  - 2.3.6 Verification at the Central Location
- 2.4 Voting Functions
  - 2.4.1 Opening the Polls
  - 2.4.2 Activating the Ballot (DRE Systems)
  - 2.4.3 Casting a Ballot
- 2.5 Post-Voting Functions

2.5.1 Closing the Polling Place (Precinct Count)
2.5.2 Consolidating Vote Data
2.5.3 Producing Reports
2.5.4 Broadcasting Results

Additional functional requirements are split up across the sections dealing with different hardware components in Vol. I Sec. 3 and Sec. 5.2.7. (C.f. Taxonomy 2.)

[P1583/D5.3.1] Functional requirements for DRE equipment only are embedded within Sec. 4 (system description), organized according to the subsystem affected. Additional functional requirements appear in Sec. 5.6 (software and functionality) and Appendix I (VVAT).

[D5.3.1 Comments 2004-10-19] Minor corrections proposed for Sec. 4, incl. possible expansion of some requirements to non-DRE systems. Many comments on VVAT functionality.

[5.0 Provisional 2004-09-10] Discussion of adding provisional ballot handling requirements to previous version applicable to [2002VSS].

[CoE 2004-09-30] Appendix II, "Operational standards," includes requirements for voter notification, voter registration, candidate nomination, voting, and counting.

[HAVA] Sec. 301 (a) (1) contains functional requirements for general voting. Sec. 302 (a) contains functional requirements for provisional voting. Sec. 302 (b) addresses voter notification ("voting information requirements"). Sec. 303 deals with registration.

[AZ] Portions of Sec. 6 echo the standard template of [GA], [MD], etc., but there are also numerous original and clarified requirements. [AZ] describes a blended DRE/OCR system.

[CO-REG] 87 pages of specific functional requirements for voter registration and election management.

[CO-IVV] N/A

[GA] Sec. 2.4.4 (system requirements, performance and capabilities), 2.4.5 (election management system), 2.4.8 (absentee voting), 2.4.9 (early voting), 2.4.10 (provisional voting), 2.4.11 (election reporting).

[MD] Sec. 3.3.1.2 (misc), 3.3.3 (import/export), 3.3.6 (absentee voting), 3.3.7 (election reporting). [MD] describes a blended DRE/OCR system, with the OCR designated for absentee ballot processing.

[MI] Sec. II-B, Specific Requirements, follows an outline similar to [GA] and [MD] but is tailored to precinct-count optical scan (no DREs). Subheadings: Precinct Count Optical Scan Voting System (Performance Capabilities, Programming), Election Management System (Ballot Definition and Data, Election Result Accumulation and Reporting (Local and State)).

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] Supplement 2, 26 pages of specific functional requirements for voter registration, election management, and petition processing.

[UT] Nothing new.

[King 2004-09] need power consumption and status indicators, expanded flexibility in report generation, pragmatic (not abstract) standards.

[Noren 2004-09] standards must accommodate blended systems.

Correctness

[2002VSS] Several aspects of correctness appear in Vol. I Sec. 2.4.2, Sec. 2.4.3.3, Sec. 2.5.3.1 g, and Sec. 2.5.3.2 d. See also Vol. I Sec. 2.2.2, "Accuracy;" Sec. 3.2.1; Sec. 3.2.3.1; Sec. 3.2.4.3.3; Sec. 3.2.5.2; Sec. 3.2.6.1.1; Sec. 3.2.6.2.2; Sec. 5.2.1; and Vol. II Sec. 4.7.1.1, "Data Accuracy." Vol. II Appendix C Sec. C5 specifies accuracy assessment procedures.

[P1583/D5.3.1] Requirements analogous to those in [2002VSS]: aspects of correctness appear in Sec. 4.4.1, Sec. 5.6.8.2, Sec. 5.6.8.3.3, Sec. 5.6.9.2 f and j. See also Sec. 5.2.1 and 5.2.2 (accuracy) and accuracy assessment procedures in Sec. 6.2.1.

[D5.3.1 Comments 2004-10-19] Comments 108 (accuracy of audit trails and paper ballots), 109 (define what an "error" is), 129 (VVAT must pass accuracy test).

[5.0 Reliability Accuracy Comments 2004-09-06] Discussion on reliability and accuracy; some comments remain applicable to current version.

[CoE 2004-09-30] Appendix I, Sec. A II (equal suffrage).

[HAVA] Sec. 301 (a) (5), "Error rates," points to [2002VSS]. Sec. 303 (a) (4) and (5) require the voter registration database to be kept accurate.

[AZ] Sec. 6.3.1.1 (accurate data transfer); Sec. 6.3.2.1 (vote count); several indirect references and misc. requirements copied from [2002VSS].

[CO-REG] Req. A-1-5 (accurate address registration), Req. A-1-11 (address correction), Req. V-1-64 (duplicate detection).

[CO-IVV] N/A

[GA] Sec. 2.4.4, subheading Accuracy (record each vote accurately, error detection and correction); Sec. 2.4.7 (accurate data transfer).

[MD] Sec. 3.3.1 (accuracy); Sec. 3.3.5 item 3 (accurate data transfer).

[MI] p. 34, tabulator programming; item a (accurately report all votes cast), item i (accurate data transfer). p. 74 (i), "record correctly and count accurately each vote properly cast." Various other requirements on pp. 73-74 about how you can vote and preventing voting twice. p. 74 (d), voting for more than one party in a primary is considered an error.

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] p. 43, duplicate detection logic. p. 51, vendor must document procedures for testing accuracy of data conversion. p. 56, detect invalid data, do not reactivate cancelled registration. pp. 58-59, several constraints on correct handling of absentee ballots. pp. 61-62, same for petition processing.

[UT] Nothing new.

Testability and verifiability

[2002VSS] Vol. I Sec. 2.2.5 (system audit), Sec. 2.2.9 (ballot counter), Sec. 2.3.4 (readiness testing), Sec. 2.3.5 (verification at the polling place), Sec. 2.3.6 (verification at the central location), Sec. 2.4.3.3 s and t (test ballots); Sec. 2.5.1 b though d (closing the polling place); Sec. 4.3 (data and document retention) and 4.4 (audit record data). 22-month data retention/stability requirements appear in Sec. 2.2.11, Sec. 3.2.3.2, Sec. 3.2.6.1.2, Sec. 3.2.6.2.3, Sec. 3.2.7.1, and Sec. 4.3 a.

[P1583/D5.3.1] adds the normative annex "Voter Verifiable Audit Trail" and has fewer exemptions for COTS. Requirements analogous to those in [2002VSS] appear in Sec. 4.3.2 (pre-delivery testing), Sec. 4.3.3 (tests at the polling place), Sec. 4.3.7 (closing the polling place), Sec. 4.5.4 (system audit log), Sec. 5.1.3.5 (system audit), and Sec. 5.6.6 (ballot counter). 22-month data retention/stability requirements appear in Sec. 4.5.1, Sec. 4.5.2, Sec. 5.1.3.5.6 a 7, Sec. 5.2.2.2, Sec. 5.2.2.3, and Sec. 5.6.3 a. Test ballots are mentioned in Sec. 5.1.3.5.4 e and f and in some Annexes.

[D5.3.1 Comments 2004-10-19] VVAT related comments, both technical and editorial, form the largest portion of the list. Numerous comments on lack of "objective test criteria" in VVAT. Comment numbers 169, 171, and 189, VVAT capacity requirements are not testable. Comment 27, "excessive" for maintenance cost is untestable.

[5.0 COTS 2004-06-18] COTS-related changes to prior version, applicable to [2002VSS] (don't have the original issues).

[5.0 TDP 2004-04-23] Changes to Technical Data Package requirements, applicable to [2002VSS].

[CoE 2004-09-30] Appendix I, Sec. B II (verifiability and accountability); Appendix II, Paragraph 59 (the e-voting system shall be auditable); Appendix III, Sec. E (audit).

[HAVA] Sec. 301 (a) (2) contains a requirement for a paper audit record that has been subject to differing and controversial interpretations.

[AZ] Sec. 2.10.6 (source code escrow), Sec. 6.1.2.1, 6.1.2.2, 6.1.3, 6.2.1, and 6.3.7.1 (diagnostic, logic and accuracy testing), 6.1.5.3.7 and 6.3.7.4 (built-in diagnostics), 6.1.5.5.5 (vote count audit log), 6.2.4 (system audit log), 6.3.4.3 and 6.3.7.3 (manually recountable audit trail), 6.3.7.9 and 6.3.7.17 (test ballots).

[CO-REG] Req. I-1-8 (allow time to verify conversion).

[CO-IVV] N/A

[GA] Sec. 2.4.4, p. 16 (diagnostic testing, logic and accuracy tests), subheading Audit and Security, esp. "detailed print record of each ballot cast;" Sec. 2.4.5, subheading Ballot Validation; Sec. 2.4.12 (system audit log); Sec. 2.4.16 ("method to immediately detect if a voting unit is not operating properly"). P. 44 (source code escrow).

[MD] Analogous to [GA], with additions and deletions. Sec. 3.3.1, items 5 and 7 (diagnostic testing, logic and accuracy tests), Sec. 3.3.2 (audit and security), esp. item 1 ("detailed print record of each ballot image cast"), Sec. 3.3.9.2 item 3 (detect if not operating properly). Ballot validation and system audit log were deleted. Sec. 4.6 (source code escrow). p. 63 (code of Maryland regulations, "Audit Trail Required").

[MI] Sec. I-SS (source code escrow). Sec. II-B analogous to [GA] and [MD], tailored to optical scan. p. 34, item m (detect malfunctions). p. 35, Audit ("The system shall produce a paper audit log…"). p. 36 (c) (verify correctness of tabulator programming) and (d) (detect and correct errors). p. 74 (j), "provide an audit trail." p. 81 Sec. 797c, source code escrow.

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] p. 45, audit trail. p. 52, audit trail.

[UT] Nothing new.

[Jones 2004-09-23] distinguishes "audit trail" from "event log;" observes that most of the time "audit trail" is used in current standards it is really just an event log; calls for abolition of infrared mark-sense machinery because mark-sense machinery using visible light (more easily verified) is now available.

[Saltman 2004-09-20] opposes COTS exemptions and the use of multi-tasking operating systems.

Trustworthiness (transparency and security)

Security punted to Nelson

In general, it should be observed that most concerned citizens / voting activists are heavily in favor of maximizing the transparency of voting systems and the elections process to enhance public trust.

Many of the citations above for testability and verifiability also apply for transparency.

[2002VSS] Vol. I Sec. 2.2.1 (security), Sec. 6 (security). Vol. II Sec. 2.1.3 requires ITAs to refrain from disclosing any information designated as proprietary by a vendor.

[P1583/D5.3.1] Sec. 5.1 (security and confidentiality). Sec. 5.1.3.5.1 specifies that audits, audit documentation, and the methods and software used to produce them shall be public and may not be treated as proprietary.

[D5.3.1 Comments 2004-10-19] Numerous technical and editorial changes are proposed by Security Task Group.

[5.0 Security Comments 2004-08-18] Comments on previous version, applicable to [2002VSS].

[CoE 2004-09-30] Appendix I, Sec. B I (transparency) and III (reliability and security); Appendix III, Sec. C (systems operation) and Sec. D (security).

[HAVA] Sec. 303 (a) (3) requires "adequate technological security measures" for the registration database.

[AZ] Sec. 6.1.4.2 (receipt capability), 6.1.4.3 (ballot image printing capability), 6.1.5.2 (ballot box security), 6.3.1.2 (encrypted telecom), 6.3.7 (audit and security).

[CO-REG] Req. S-1-8 (audit log), Category S-4 (security).

[CO-IVV] N/A

[GA] Sec. 2.4.4, subheading Audit and Security; Sec. 2.4.16 (tamper-proof in storage).

[MD] Sec. 3.3.2 (audit and security), Sec. 3.3.9.1 item 4 (tamper-proof in storage). p. 63 (code of Maryland regulations, "Audit Trail Required").

[MI] p. 35 (audit and security), p. 41 (audit and security).

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] p. 45, role-based access control, audit trail. p. 52, audit trail. p. 56, limit write access.

[UT] Nothing new.

[Deutsch 2004-09-21] has some recommendations for revised security standards (end-to-end, customized to type and architecture of system), opposes public review of source code, supports releasing redacted ITA reports to public.

[Fischer 2004-09-20] notes that 20% of voters still use lever machines and hand-counted paper ballots (not covered by current guidelines, were in 1990 VSS?), warns against taking a purely technical approach, and reviews current thinking and best practices.

[Gaston 2004-09-20] favors complete transparency.

[Jones 2004-09-20] enumerates many failings in the status quo and advises: "What I believe we need is a reference model, well above the level of specific details of file format and system function, documenting the data paths within the voting system, from election definition to post-election audit, and for each path, documenting the threat model and security mechanisms appropriate for addressing those threats. This model must also document the assumptions made about the public's right to observe, so that election laws and election conduct can be evaluated against it."

[Jones 2004-09-23] distinguishes "audit trail" from "event log," observes that most of the time "audit trail" is used in current standards it is really just an event log.

[King 2004-09] need improved methods for securing deployed units.

[Noren 2004-09] calls for standardized, open "data set" (meaning tabulation algorithm); need more transparency in development, testing and audit; observes lack of standards for the printing function of paper-based systems.

[Saltman 2004-09-20] highlights the lack of "chain of custody" controls in the current processes.

[Shamos 2004-09-20] observes that the guidelines development process and the qualification process could be more transparent, and that security cannot be evaluated properly except *in situ*, in the full context of the safeguards that are actually used in different places. "It is conceivable that a given system will be secure when used in County A but not in County B. A laboratory test will never reveal this."

[Wallach 2004-09-20] enumerates several threats and supports VVAT as mitigation.

Reliability

In informal conversations with NIST staff, poll workers have repeatedly identified reliability of voting equipment as a major concern, and there is much anecdotal evidence supporting that concern. The pending EAC Election Day Data Survey of secretaries of state and state election directors may help to confirm or repudiate the significance of this issue overall in a more scientific manner. FIXME insert the data when we have it. See also forthcoming GAO report.

[2002VSS] Vol. I Sec. 2.2.3 (error recovery), Sec. 2.2.4 (integrity), Sec. 2.4.3.1 e and f (power supply), Sec. 2.6 (maintenance, transportation and storage), Sec. 3.2.2.4 through 3.2.2.14 (electrical and environmental), Sec. 3.2.3.2 (memory stability), Sec. 3.2.4.3.4 (recording reliability), Sec. 3.2.5.1.4 b (multiple feeds prevention), Sec. 3.2.6.1.2 (memory stability), Sec. 3.2.6.2.3 (memory stability), Sec. 3.4.1 a (design for reliability), Sec. 3.4.2 (durability), Sec. 3.4.3 (reliability), Sec. 3.4.5 (availability), Sec. 5.2.2 (telecom durability), Sec. 5.2.3 (telecom reliability), Sec. 5.2.5 (telecom availability), Sec. 5.2.6 c (no single point of failure in networking), Sec. 7 (quality assurance), Sec. 8 (configuration management). Vol. II Sec. 2.12 requires vendors to document their quality assurance program; Vol. II Sec. 7.5 requires ITAs to review it. Vol. II Sec. 4 enumerates specific "shake and bake" tests for hardware reliability. MTBF shall be at least 163 hours. Vol. II Sec. 4.7.2 describes assessment of availability. Vol. II Appendix C Sec. C4 specifies MTBF assessment procedures.

[P1583/D5.3.1] Analogous in Sec. 4.3.6 (error recovery), Sec. 5.2.2.2 (memory stability), Sec. 5.2.3 (integrity), Sec. 5.2.4 (durability), Sec. 5.2.4.1 a (design for reliability), Sec. 5.2.5 (reliability), Sec. 5.6.8.3.1 e and f (power supply), Sec. 5.4 (environmental), Sec. 5.5 (electrical), Sec. 5.7 (availability). Sec. 6.2.2 describes assessment of MTBF (163 hours); Sec. 6.2.3, availability. Shake and bake are in Sec. 6.4 (environmental). Quality assurance and configuration management don't appear until Sec. 7 (Technical Data Package).

[D5.3.1 Comments 2004-10-19] Comment 51 asserts that 163 hour MTBF implies a 9.2% probability of failure per machine during an election, proposes raising standard to 1500 hours.

[5.0 Reliability Accuracy Comments 2004-09-06] Discussion on reliability and accuracy; some comments remain applicable to current version.

[5.0 Environmental 2004-08-15] Changes to shake and bake requirements.

[5.0 EMC 2004-08-23] Few technical corrections to EMC requirements, mostly editorial.

[CoE 2004-09-30] Appendix I, Sec. B III (reliability and security); Appendix III, Sec. C (systems operation).

[HAVA] N/A

[AZ] Sec. 6.1.2.3 (retain votes after failure), 6.1.5.3.13 and 14 (environmental), 6.3.1.1 (telecom reliability).

[CO-REG] Req. S-1-1 and 2, configuration management and quality assurance, S-1-7, backup and recovery.

[CO-IVV] N/A

[GA] Sec. 2.4.6 (UPS), Sec. 2.4.16 (rough duty).

[MD] Sec. 3.3.4 (UPS), Sec. 3.3.9.1 items 2 and 3 (rough duty).

[MI] p. 34 f (retain votes after failure), l (survive transport), p. 36 (system back-up).

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] p. 19, quality assurance.

[UT] Nothing new.

[Noren 2004-09] observes lack of standards for the printing function of paper-based systems.

Accessibility

Punted to Sharon

In email to crt_members 2004-11-04, Dr. Harding reported "Based on my experience in South Florida (on election day), we specifically [need to] address disability issues in all of our work. Some areas handled it well in relationship to other areas, but all voting locations had much room for improvement!"

[2002VSS] Vol. I, Sec. 2.2.7 (accessibility), Sec. 3.4.9 (human engineering – controls and displays).

[P1583/D5.3.1] Sec. 5.3 (usability and accessibility) and Sec. 6.3 (testing thereof) are considerably more developed than comparable text in [2002VSS]. [P1583/D5.3.1] also adds informative annexes "Derivation of Audio Frequency Spectrum Limits," "Proposed Approach to Testing the IEEE Usability/Accessibility Standards," and "Accessibility of Voter Verifiable Audit Records."

[D5.3.1 Comments 2004-10-19] Accessibility issues with VVAT.

[5.0 Accessibility Comments 2004-08-01] Comments on previous version, applicable to [2002VSS].

[CoE 2004-09-30] Appendix I, Sec. A I (universal suffrage); Appendix III, Sec. A (accessibility).

[HAVA] Sec. 301 (a) (3) and (4) contain accessibility requirements.

[AZ] Sec. 6.1.5.7 (accessibility).

[CO-REG] Req. S-7-16 (ADA compliance).

[CO-IVV] N/A

[GA] Sec. 2.4.15 (disabled voter comfort).

[MD] Sec. 3.3.8.1 (disabled voter comfort).

[MI] p. 74 (h), "accommodate the needs of an elderly voter or a person with 1 or more disabilities." HAVA accessibility requirements are specifically deferred to a future RFP. p. 73, Sec. 795 (a), secrecy clause makes exception for assisted voters.

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] N/A

[UT] Nothing new.

[Gaston 2004-09-20] observes that requiring a proportional font rules out a plain text mode voting machine, which could have many advantages (standard text-readers would work).

[Golden 2004-09-22] says there is a need for consensus on accessibility requirements for voter-verifiable audit records.

[Relton 2004-09-21] identifies some specific accessibility and usability requirements.

Usability (ease of use)

Punted to Sharon

[2002VSS] Vol. I Sec. 2.4.3.1 a (minimum text size), Sec. 2.4.3.2.1 a (identifiable fields on paper), Sec. 2.4.3.2.2 a (undervote/overvote feedback for precinct count paper-based systems), various under Sec. 2.4.3.3 (misc. DRE behaviors), Sec. 3.4.9 (human engineering – controls and displays), Appendix C (general usability).

[P1583/D5.3.1] Sec. 5.3 (usability and accessibility) and Sec. 6.3 (testing thereof) are considerably more developed than comparable text in [2002VSS]. [P1583/D5.3.1] also adds informative annexes "Presentation of Ballot Information," "Defining a Summative Usability Test for Voting Systems," "Proposed Approach to Testing the IEEE Usability/Accessibility Standards."

[D5.3.1 Comments 2004-10-19] Technical and editorial changes proposed by Usability Task Group.

[CoE 2004-09-30] Appendix I, Paragraph 1 (the voter interface of an e-voting system shall be understandable and easily usable); Appendix II, Paragraphs 46-50 (voting).

[AZ] Sec. 6.1.5.6 (voter comfort), 6.1.5.8 (portability / ease of use), 6.4.3.14 (languages).

[CO-REG] Misc. references to "easy to use" features.

[CO-IVV] N/A

[GA] Sec. 2.4.14 (voter comfort), 2.4.16 and 17 (poll workers etc. comfort).

[MD] Sec. 3.3.8 (voter comfort), 3.3.9 (poll workers etc. comfort). Sec. 3.3.8.2, as added in Addendum 2 (separate document), requires support for 5 languages of audio ballots at one time. The languages in Sec. 3.3.11 are deleted by Addendum 2.

[MI] Sec. II-B, General Requirements, incorporates Voting Rights Act of 1965 for "alternative language accessibility." P. 74 (g), "suitably designed for the purpose used."

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] N/A

[UT] Nothing new.

[Conrad 2004-09-22] provides input on usability testing.

[Noren 2004-09] observes lack of standards for the printing function of paper-based systems; calls for self-teaching voting systems to overcome training difficulties.

[Redish 2004-09-22] calls for usability standards for ballot design and polling place signage.

[Relton 2004-09-21] identifies some specific accessibility and usability requirements.

Capacity

[2002VSS] Vol. I Sec. 3.2.5.1.1 (vendor shall document central count capacity), Sec. 3.2.6.2.1 b (DRE "speed" a.k.a. response time). Vol. II Sec. 6.2.3, "For all systems, the total number of ballots to be processed by each precinct counting device during these tests shall reflect the maximum number of active voting positions and the maximum number of ballot styles that the TDP claims the system can support."

[P1583/D5.3.1] Sec. 6.6.6.1.2 (testing volume), Sec. 7.3 (vendor shall document maximum throughput), Sec. I.3.2.1.2.1.8, I.3.2.1.2.2.3, I.3.2.1.2.5.3, I.3.2.2.2.1.10 and I.3.2.3.2.1.8 (VVAT related capacities).

[D5.3.1 Comments 2004-10-19] Comment numbers 169, 171, and 189, VVAT capacity requirements are not testable.

[CoE 2004-09-30] N/A

[HAVA] N/A

[AZ] Sec. 6.1.5.3.8 (15 jurisdictional splits per precinct), Sec. 6.4.3.8 (6000 active ballot styles and 150 active voting positions).

[CO-REG] Req. E-7-4 (election management system must accommodate at least 500 "item types"), P-1-3 (200,000 registered voters per petition), P-1-7 (200 active petitions, 1000 archived petitions), P-1-8 (50 petitions simultaneously being processed), P-2-6 (manage 100 petitions simultaneously for each of 64 counties), Q-2-1 (up to 100 custom reports), Category S-5 (sizing and performance), Req. V-1-43 (four unique addresses per voter), V-1-48 (1024-char comment field in each voter record), V-5-7 (five signatures).

[CO-IVV] N/A

[GA] N/A

[MD] Sec. 3.3.8.2, as added in Addendum 2 (separate document), requires support for 5 languages of audio ballots at one time. The languages in Sec. 3.3.11 are deleted by Addendum 2.

[MI] N/A

[OH-VOT] N/A

[OH-REG] p. 42, unlimited storage capacity.

[UT] Nothing new.

Simplicity

[2002VSS] Vol. I Sec. 4.2 (software design and coding standards). Vol. II Sec. 5 constrains the programming language constructs that may be used in voting system software.

[P1583/D5.3.1] Analogous requirements in Sec. 5.6.2 (software design and coding standards) and 6.6.4 (source code review).

[D5.3.1 Comments 2004-10-19] Comment numbers 235 through 241 propose technical changes to the software design and coding standards.

[5.0 Software Comments 2004-09-01] Comment 1: "This section requires rewriting from stem to stern." Numerous detailed issues with design and coding standards and source code review procedures.

[CoE 2004-09-30] N/A

[HAVA] N/A

[AZ] N/A

[CO-REG] N/A

[CO-IVV] N/A

[GA] N/A

[MD] N/A

[MI] N/A

[OH-VOT] N/A

[OH-REG] N/A

[UT] N/A

[Gaston 2004-09-20] says that the software design and coding standards should be abolished, and observes that requiring a proportional font rules out a plain text mode voting machine, which would be simpler.

[Saltman 2004-09-20] says multi-tasking operating systems are an unnecessary complication.

Privacy and Secrecy

These two concepts are not well distinguished in the cited references, so it is not possible to separate them here.

[2002VSS] Vol. I Sec. 2.4.1.2.1 b, for paper-based systems, Sec. 2.4.3.1 b (casting ballots), Sec. 2.4.3.2.1 d (paper-based), Sec. 2.4.3.3 q (DREs), Sec. 3.2.4.1 c (voting booths), Sec. 3.2.4.3.2 e (DREs general storage and processing), Sec. 4.5 (DREs must erase previous selections), Sec. 6.6.1 a (telecom).

[P1583/D5.3.1] Sec. 4.4.1 o (general precinct voting) and r (provisional ballots on DREs), Sec. 4.5.5 (provisional ballots), Sec. 5.1.3.2.5 (expanded requirements for DREs), Sec. 5.1.3.5.4 and 5.1.3.5.6 (privacy in audit records), Sec. 5.3.1 (usability testing includes confidence of privacy), Sec. 5.4.4 (power failures), Sec. 5.6.4.1 (error reporting shall preserve privacy), Sec. 5.6.7.2.2 c (paper-based systems), Sec. 5.6.8.1.2 (paper-based systems), Sec. 5.6.8.3.1 b (casting ballots), Sec. 5.6.8.3.2 d (paper-based), Sec. 5.6.8.3.3 m, o and q (DREs), Sec. 7.3 c (vendor shall document), Sec. I.3.1.1, I.3.2.1.2.1.2, I.3.2.1.2.1.3, I.3.2.1.2.4.4.1, I.3.2.1.2.5.2, I.3.2.2.2.1.4, I.3.2.2.2.4, I.3.2.3.2.1.2, and I.3.2.3.2.3 d (privacy in VVAT).

[D5.3.1 Comments 2004-10-19] Comment 1, include compromise of secrecy among the threats; 67 and 73, some secrecy requirements for DREs should be for all systems. Repeated issues with VVAT conflicting with secrecy. Various tangential references to privacy.

[CoE 2004-09-30] Appendix I Sec. A IV (secret suffrage); Appendix II Paragraph 54 (no discovery of individual ballots); Appendix III Paragraphs 78 (general privacy) and 93 (residual information).

[HAVA] Sec. 301 (a) (1) (C) notifications must preserve privacy and confidentiality of the ballot.

[AZ] Sec. 6.1.5.5.3, 6.1.5.5.4, 6.3.7.6, 6.3.7.13.

[CO-REG] Req. Q-2-6 (suppress personal information in reports unless authorized by state system administrator), Req. V-3-21 (confidentiality indicator on voter's registration record).

[CO-IVV] N/A

[GA] Sec. 2.4.4, p. 17 ("provide that each voter's ballot is secret"), p. 18 ("Protect the secrecy of the vote"); Sec. 2.4.14, p. 24 (voting booth privacy),

[MD] Sec. 3.3.2 item 3 ("provide that each voter's ballot is secret"), Sec. 3.3.8 item 9 (voting booth privacy), p. 63 (code of Maryland regulations, "The voting system shall ensure voting in secrecy").

[MI] Sec. II-B, General Requirements, incorporates HAVA. p. 73, Sec. 795 (a), secrecy with exception for assisted voters.

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] p. 46, protect social security numbers. p. 56, protect social security numbers and registration source.

[UT] Nothing new.

[Coney 2004-09-22] Calls for increased privacy protections.

[Jones 2004-09-23] questions whether the intent is absolute secrecy or provisional secrecy (a distinction for law to clarify).

Portability

[2002VSS] Vol. I Sec. 3.3 (physical characteristics); shake and bake testing for tolerance of transport stress.

[P1583/D5.3.1] No analogous text for [2002VSS] Vol. I Sec. 3.3. Environmental tests ensure tolerance of transport stress.

[D5.3.1 Comments 2004-10-19] N/A

[CoE 2004-09-30] N/A

[HAVA] N/A

[AZ] Sec. 6.1.5.8 (portability / ease of use; 6.1.5.8.1, "each component weigh less than 50 pounds each").

[CO-REG] N/A

[CO-IVV] N/A

[GA] Sec. 2.4.16 and 17 (transportable, lightweight, fits through doorways).

[MD] Sec. 3.3.9 (transportable, lightweight, fits through doorways).

[MI] p. 34 item l (transportable).

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD].

[OH-REG] N/A

[UT] Nothing new.

Maintainability

[2002VSS] Vol. I Sec. 3.4.1 (design for maintainability, approved parts list), Sec. 3.4.4 (maintainability), Sec. 3.4.6 (product marking), Sec. 5.2.4 (telecom maintainability). Vol. II Sec. 2.9 requires vendors to document maintenance procedures. Vol. II Sec. 4.7.2, "Maintainability Test."

[P1583/D5.3.1] Sec. 5.2.4.1 (design for maintainability, approved parts list), Sec. 5.2.6 (maintainability), Sec. 5.4.8 (product marking), Sec. 6.2.4 (maintainability test), Sec. 7.9 (system maintenance procedures).

[D5.3.1 Comments 2004-10-19] Comment 27, "excessive" for maintenance cost is untestable.

[CoE 2004-09-30] N/A

[HAVA] N/A

[AZ] Sec. 6.1.5.3.15 (low maintenance in storage), 6.1.5.4 (malfunctions and troubleshooting), 6.3.8 (third party support).

[CO-REG] N/A

[CO-IVV] N/A

[GA] N/A

[MD] N/A

[MI] N/A

[OH-VOT] N/A

[OH-REG] N/A

[UT] Nothing new.

[King 2004-09] need maintenance documentation and training.

Compatibility

[2002VSS] N/A

[P1583/D5.3.1] N/A

[D5.3.1 Comments 2004-10-19] N/A

[CoE 2004-09-30] Appendix III, Section B, "Interoperability," mandates the use of open standards (EML).

[HAVA] N/A

[AZ] Sec. 6.1.1 and 6.4 require interoperability between OCR (optical character recognition) and DRE equipment and integration of EMS with other functions.

[CO-REG] Category I-1 (data conversion – migration from old systems), Req. S-2-19 (XML, but not EML, mandated), Category S-3 (hardware/software/network), Req. S-7-10 (optional compatibility with common desktop applications), Req. V-1-5, 30 and 31 (interface with driver license system and social security number database), Req. V-1-41 (optional interface with Address Change Service), Category V-2 (interfaces).

[CO-IVV] N/A

[GA] Sec. 2.4.11 (election results to desktop software). p. 45, preference given to open architectures.

[MD] Sec. 3.3.3 (integration with state system), Sec. 3.3.7 item 11 (election results to desktop software).

[MI] p. 39 item i (election results to desktop software).

[OH-VOT] p. 17, proposed system *shall not* require an interface to any voter registration system. p. 39, preference given to open architectures. Repeats language seen before about open architecture and election results to desktop software.

[OH-REG] p. 50 (data conversion – migration from old systems).

[UT] Nothing new.

[King 2004-09] need upward compatibility and integration with voter registration systems.

Compliance

Inasmuch as the deployment of voting equipment and software is part of the larger system that includes all election administration processes, to prevent the deployment of uncertified equipment and software is an issue for the system. (c.f. California audit, 2003-12, reported in Wired News, "E-Voting Undermined by Sloppiness," 2003-12-17, available at http://www.wired.com/news/evote/0,2645,61637,00.html?tw=wn_story_related).

All state RFPs require compliance with applicable state law.

[2002VSS] Vol. I Sec. 9 and Vol. II deal with qualification testing.

[P1583/D5.3.1] Sec. 6 gives testing criteria.

[D5.3.1 Comments 2004-10-19] N/A

[CoE 2004-09-30] Appendix III, Sec. C (systems operation); Paragraph 85 (electoral authorities have overall responsibility for compliance with security requirements); Sec. F (certification).

[HAVA] Sec. 209 clarifies that the EAC has no regulatory power. Sec. 231 addresses the accreditation of testing labs and the testing, certification, decertification, and recertification of voting system hardware and software. Title IV authorizes enforcement of the statutory requirements (in HAVA) by the Attorney General.

[AZ] Sec. 2.6 (offeror qualifications).

[CO-REG] Req. S-2-10 (HAVA and NVRA), S-7-16 (ADA).

[CO-IVV] IVV contractor responsible for testing compliance of registration system.

[GA] Sec. 2.4.1 and 2.4.2 (VSS compliant, ITA qualified, GA certified).

[MD] Sec. 2 (VSS compliant).

[MI] p. 55 ("All EMS shall be ITA approved" and approved by Department of State). Similar on p. 76.

[OH-VOT] Repeats language seen before; nothing new relative to [GA] and [MD] except compliance with Ohio laws.

[OH-REG] is HAVA-driven. p. 52, comply with federal and OH election law. p. 53, comply with NVRA.

[UT] Nothing new.

[Gaston 2004-09-20] opposes expensive testing and certification requirements because they stifle innovation.

[Jones 2004-09-23] writes: "What the current system lacks is a channel for the problems uncovered in state testing to be disseminated to other states, the ITAs, those maintaining the voting system standards and the public. When one state uncovers a problem with a voting system, this should warn other states and the ITAs that they may have overlooked something, and it should warn those who set voting system standards that there may be a deficiency in the standards."

Localization

Several states require support for ballot rotation. State requirements to support split precincts, write-in voting, and other, similar complications are standard. Some jurisdictions require the ability to cast a blank ballot while others (e.g. [MI], p. 74 (f)) specifically prohibit it.

[2002VSS] N/A

[P1583/D5.3.1] N/A

[D5.3.1 Comments 2004-10-19] N/A

[CoE 2004-09-30] N/A

[HAVA] Sec. 301 (a) (6) requires each state to "adopt uniform and nondiscriminatory standards that define what constitutes a vote."

[AZ] Extra requirements for compatibility in blended system and ability to produce paper receipts and ballot images. Sec. 6.4.3.10, ballot stock should be available from multiple vendors.

[CO-REG] Many Colorado-specific requirements.

[CO-IVV] N/A

[GA] Sec. 2.5.3 and 2.5.4 require warranty support and election administration support from the vendor, with some interesting QoS details.

[MD] Similar to [GA], but with additional burdens for the contractor. Sec. 3.3.10, vendor must provide public service announcements for voter education. Sec. 3.3.13, storage, transportation, and insurance are to be provided by the vendor. Sec. 4.8, there's a certification fee.

[MI] Sec. I-O, "time is of the essence." Sec. I-P, the state reserves some control over contractor staffing ("Key Personnel"). Sec. I-SS, source code escrow requirements are more elaborate than other states'. p. 35, "DOS has a preference for the use of ovals." p. 76 (2)(a), there's an application fee.

[OH-VOT] p. 17, proposed system *shall not* require an interface to any voter registration system.

[OH-REG] pp. 61-62 discusses the possibility of an automated petition processing system.

[UT] Nothing new.

Summary

For the most part, the state RFPs reviewed repeat certain generally stated requirements for accuracy, security, etc. that were copied from some common source, without adding any depth relative to each other or to [2002VSS]. Notable exceptions include portions of [AZ] Sec. 6 and all of [CO-REG] and [OH-REG].

State RFPs require functionality for such things as (e.g., list taken from [UT]) closed primaries, multi-member districts, write-in votes, straight party voting, split precincts, combined precincts, absentee and early voting and recounts, which are allowed and/or supported by [2002VSS] but not addressed specifically or in detail by the federal

guidelines. In revised guidelines, these functions could be defined formally in profiles to which states could make normative references, without being mandatory for all systems.

States generally require the vendor to provide training and to supply their source code to an escrow agent. These requirements were outside the scope of [2002VSS] but surely belong in any revised guidelines that cover the broader elections process.

Finally, some states seek to clarify the audit trail requirement of HAVA by specifying more precisely what must be committed to paper, and when.

[CoE 2004-09-30] stands out as a concise yet comprehensive statement of general principles for voting systems, usable as a manifesto for revised guidelines. Although it contains no quantitative, testable requirements ("depth"), its coverage of important points ("breadth") is easily superior to any of the other sources reviewed. Some of the principles accepted by the Council of Europe may be unacceptable to some of the U.S.

Testimony to the EAC overwhelmingly focused on trustworthiness (transparency and security), making it clear that this should be addressed in all aspects, including the guidelines development process.