Volume I, Appendix C
Table of Contents

Best Practices for Voting Officials

Many requirements for human factors and security (e.g., wireless communications, software distribution, and setup validation, voter verified paper audit trails) depend not only on voting systems providing specific capabilities but on voting officials developing and carrying out appropriate procedures. Consequently, the Voluntary Voting System Guidelines (VVSG) Version 1 provides guidance in the form of best practices for voting officials. These best practices provide adjuncts to the technical requirements for voting systems in order to ensure the integrity of the voting process and to assist States in properly setting up, deploying, and operating voting systems.

This appendix contains a list of best practices that have been extracted from the body of the VVSG Version 1. The section numbering and introductory text from the VVSG has been retained to provide the context for the best practice as well as to indicate from where it was extracted.

C.1 Best Practices for Human Factors

2.2.7 Human Factors

Human factors is concerned with the understanding of interactions among humans and other elements of a system. The importance of human factors in the design of voting systems has become increasingly apparent. It is not sufficient that the internal operation of these systems is correct; in addition, voters and poll workers must be able to use them effectively. The challenge, then, is to provide a voting system and voting environment that all voters can use comfortably, efficiently, and with justified confidence that they have cast their votes correctly.

2.2.7.1 Accessibility

The Help America Vote Act (HAVA) Section 301 (a)(3) reads in part:
"Accessibility for individuals with disabilities - The voting system shall:
(A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;
(B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place."

Ideally every voter would be able to vote independently and privately.

Best Practices

- When the provision of accessibility involves an alternative format for ballot presentation, then all the other information presented to voters in the case of non-disabled English-literate voters (including instructions, warnings, messages, and ballot choices) is also presented in that alternative format.

- When the primary means of voter identification or authentication uses biometric measures that require a voter to possess particular biological characteristics, the voting process provides a secondary means that does not depend on those characteristics.

- Polling places are subject to the appropriate guidelines of the Americans with Disabilities Act (ADA) of 1990 and of the Architectural Barriers Act (ABA) of 1968.

- On all voting stations, the default color coding maximizes correct perception by voters and operators with color blindness.

- A sanitized headphone or handset is made available to each voter.

- If the normal procedure is for voters to submit their own ballots, then the voting process provides features that enable voters who are blind to perform this submission.

- The Acc-VS provides a clear floor space of 30 inches (760 mm) minimum by 48 inches (1220 mm) minimum for a stationary mobility aid. The clear floor space is level with no slope exceeding 1:48 and positioned for a forward approach or a parallel approach.

- All controls, keys, audio jacks and any other part of the Acc-VS necessary for the voter to operate the voting system are within the reach regions as specified in the VVSG Volume I, Section 2.2.7.1.4.3.

- The Acc-VS incorporates the features listed in the VVSG Volume I, Section 2.2.7.1.2.2.3 (audio presentation) to provide accessibility to voters with hearing disabilities.

- The voting process is made accessible to voters with cognitive disabilities.

2.2.7.2 Limited English Proficiency

HAVA Section 301 (a)(4) reads in part:

"Alternative language accessibility - The voting system shall provide alternative language accessibility pursuant to the requirements of section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a)."

Ideally every voter would be able to vote independently and privately, regardless of language.

Best Practices

- Regardless of the language, candidate names are displayed or pronounced in English on all ballots. For written languages that do not use Roman characters (e.g. Chinese, Japanese, Korean, Arabic), the ballot includes transliteration of candidate names into the relevant language.

2.2.7.3 Usability

HAVA Section 301 begins by addressing the interaction between the voter and the voting system. In addition to these mandates, HAVA Sections 243 and 221 (e)(2)(D) address support for improved usability. Usability is defined generally as a measure of the effectiveness, efficiency, and satisfaction achieved by a specified set of users with a given product in the performance of specified tasks. In the context of voting, the primary users are the voters (but also poll workers), the product is the voting system, and the task is the correct representation of one's choices in the election.

Best Practices

- The voting station does not visually present a single race spread over two pages or two columns.

- The ballot clearly indicates the maximum number of candidates for which one can vote within a single race.

- The ballot presents the relationship between the name of a candidate and the mechanism used to vote for that candidate in a consistent manner.

2.2.7.4 Privacy

Voter privacy is strongly supported by HAVA - Sections 221 (e)(2)(C) and 301 (a)(1). Privacy in the voting context, including the property of the voter being unable to disclose his or her vote, ensures that the voter can make choices based solely on his or her own preferences without intimidation or inhibition. Among other practices, this forbids the issuance of a receipt to the voter that would provide proof to another how he or she voted.

Note that these best practices address privacy concerns in relation to human factors issues and not with respect to the processing of cast ballots.

Best Practices

- The ballot and any input controls are visible only to the voter during the voting session and ballot submission. Poll workers need to take into account such factors as visual barriers, windows, permitted waiting areas for other voters, and procedures for ballot submission when not performed at the voting station, e.g. submission of optiscan ballots to a central reader.

- The audio interface is audible only to the voter.

- As mandated by HAVA 301 (a)(1)(C), the voting system notifies the voter of an attempted overvote in a way that preserves the privacy of the voter and the confidentiality of the ballot.

- Appropriate procedures are needed to ensure that absentee balloting enable the voter to preserve privacy. There is no practical means to prevent a voter from revealing an absentee paper ballot to others. But the procedures should ensure that if a voter chooses to maintain privacy, it is not violated at a later stage, in particular when the ballot is received by voting officials.

C.2 Best Practices for Security

VVSG Version 1 addresses four new aspects of voting systems security. The first, independent dual verification is informative and provide characteristics of these systems. It does not yet contain any best practices. There are best practices for the other three sections: Voter Verified Paper Audit Trails, Wireless Requirements, and Software Distribution and Setup Validation.

6.0.2 Requirements for Voter Verified Paper Audit Trails

VVSG Version 1 provides requirements for voter verified paper audit trails (VVPAT) so that States that choose to implement VVPAT or States that are considering implementation can utilize these requirements to help ensure the effective operation of these systems.

6.0.2.4 Approve or Spoil the Paper Record

Best Practices

- Appropriate procedures are needed for reconciling the number of spoiled paper records with the number of spoiled electronic records and for addressing any discrepancies after the close of polls.

- Appropriate procedures are needed to permit the voter to cast a ballot if the maximum number of spoiled ballots occurs.

- Appropriate procedures are needed to address situations in which a voter is unable to review the paper record.

- Appropriate procedures are needed to address situations in which a voter indicates that the electronic and paper records do not match. If the records do not match, a potentially serious error has occurred. Election officials should first verify that the records do not match and then take appropriate actions such as removing the voting station from service and quarantining its records for later analysis.

6.0.2.5 Preserve Voter Privacy and Anonymity

Best Practices

- Appropriate procedures are needed to ensure the privacy and anonymity of voters whose paper records contain any of the alternative languages chosen for making ballot selections.

- Appropriate procedures are needed to prevent voters from leaving the voting area with a paper record that can directly reveal the voter's choices.

6.0.2.7 Equipment Security, Reliability, and Maintainability

Best Practices

- Appropriate procedures are needed to ensure that voting systems are physically secured from tampering and intentional damage.

6.0.3 Wireless Requirements

Wireless is defined as any means of communication that occurs without wires. This includes radio frequency (RF), infrared, (IR) and microwave. The use of wireless technology within a voting system introduces risk and should be approached with caution. Wireless communication is susceptible to disruption, eavesdropping, and interference from other wireless signals. The combination of technical features and functionality built into the voting system along with procedural practices in using and handling the voting system can mitigate the risks of using wireless communications.

6.0.3.2 Controlling Usage

Best Practices

- When using encryption to ensure that the wireless communication is secure, appropriate procedures are needed for cryptographic key management.

6.0.3.6 Protecting The Voting System From A Wireless-Based Attack

Best Practices

- Appropriate procedures are needed to ensure that wireless communication actions are logged and capture at least the following information: times wireless is activated and deactivated, services accessed, identification of device to which data was transmitted to or received from, identification of authorized user, successful and unsuccessful attempts to access wireless communications or service.

6.0.4 Distribution of Voting System Software and Setup Validation

The goal of software distribution requirements is to ensure that the correct voting system software has been distributed without modification. The goal of setup validation requirements, including requirements for verifying the presence of qualified software and the absence of other software, is to ensure that voting system equipments is in a proper initial state before being used.

6.0.4.1 Software Distribution Methodology Requirements

Best Practices

- Voting software used to install the qualified voting systems can be obtained on write-once media from the voting system vendor or an EAC accredited test authority.

- The reference information produced by the NSRL or other EAC designated repository can be used to verify that the correct software has been received.

6.0.4.2 Generation and Distribution Requirements for Reference Information

Best Practices

- To ensure that the write-once media contains the correct information, a digital signature can be used. The digital signature can replace secure storage of reference information since the digital signature can be used to verify that the reference information media has not been modified or corrupted.

- The vendor's documented values can be used to verify that all voting systems' static and initial register and variable values are correct prior to an election.

- The reference information can be used to verify that voting system software is the correct version of the software prior to an election.

- If differences between the reference information and voting system software are found, then appropriate procedures are needed to handle and resolve these anomalies.