Voluntary E-Poll Book Certification Requirements Version 0.9

January 19, 2023

U.S. Election Assistance Commission

Executive Summary

The purpose of the requirements is to provide a set of specifications against which e-poll book systems can be tested to determine if they provide accessibility and security capabilities. This document is the first iteration of national level e-poll book standards and is designed to ensure consistent security and accessibility in e-poll book systems utilized across the United States of America.

The cybersecurity of e-poll book systems has never been more important. Attacks from nation state actors against our election infrastructure have specifically targeted these systems in past elections [insert footnotes to published reports?] and the U.S. Election Assistance Commission (EAC) believes that attacks against these types of systems will increase in future elections.

Table of Contents

Executive Summary 2

Table of Contents 3

Introduction 4

Scope 4

Section 1 - Security Requirements 6

- **Section 1.1 – Access control** 6
- **Section 1.2 – Physical security measures** 10
- **Section 1.3 – System Integrity** 11
- **Section 1.4 – Network/Telecommunications Security** 13
- **Section 1.5 – Software Design and Architecture** 15
- **Section 1.6 – Logging** 18
- **Section 1.7 – Supply Chain Risk Management** 19

Section 2 – Accessibility and Usability Requirements 20

- **Section 2.1 – Core functionality** 20
- **Section 2.2 – Requirements for e-poll books supporting audio** 36
- **Section 2.3 – Requirements for e-poll books supporting additional languages** 39

Introduction

This document is the first version of national level e-poll book security and accessibility standards and was developed by the EAC to specifically address e-poll books. Adherence to these requirements is governed by state and territory-specific laws and procedures.

How the Requirements are to be Used

This document will be used primarily by e-poll book system manufacturers and Voting System Test Laboratories (VSTLs) as a baseline set of requirements for e-poll book system security and accessibility to which states or territories will add their specific requirements, as necessary. This audience includes:

- Manufacturers, who will use these requirements when they design and build new e-poll book systems.
- Voting system test laboratories, who will refer to this document when they develop test plans for the analysis and testing of e-poll book systems to verify whether the system meets these requirements.

Scope

The scope of this document is limited to e-poll book systems acquired by states and evaluated by the EAC. E-poll book systems are defined in this document as:

Equipment (including hardware, firmware, and software), materials, and documentation used to partially automate the process of checking in voters, assigning voters the correct ballot style, and marking off voters who have been issued a ballot.

E-poll books are used in a voting location to assist election workers in checking in voters, ensuring that they are eligible to vote and, in some places, managing updating voter records. Additionally, e-poll books also have administrative functions to prepare for an election and extract data reports afterwards. The same usability and accessibility feature important in the voting location will also support back-office workers. Additionally, e-poll books may use an air-gapped configuration at the precinct with a separate local copy of the registration list or can be connected (wired or wireless) via a public or private network with a central repository of registration information where records can be checked and updated in real time across the jurisdiction.

While e-poll books can provide additional functionality such as poll worker time keeping, ballot printing, or communications between a central office and polling places, the requirements in this document specifically apply to the following functionality **(where allowed by state, territorial, or jurisdictional laws or rules):**

- Allows voters to check-in electronically
- Allows poll workers to easily direct voters to the correct polling location
- Is capable of scanning voter identification to pull up a voter's information
- Allows poll workers to look up voters across precincts, enabling consolidated vote centers

- Allows real-time updates of voter history when operated in a connected configuration
- Notifies poll workers if a voter has already been issued an absentee or mail-in ballot
- Produces turnout numbers and lists of who voted
- Allows for same-day voter registration
- Can display a photo to verify a voter's identity
- Can produce information used to activate a ballot for voting machines that require this functionality (printed ballot number, activated electronic token, etc.)

There are some important differences between the context of use for voting systems and e-poll books that are important to keep in mind when considering VVSG requirements.

Election workers are the primary users. Unlike voters, they are trained in how to use the e-poll book. In contrast to voters who interact with a voting system for one brief session, election workers complete the basic tasks many times during a voting day. Election workers are also older than average. The 2018 Election Administration and Voting Survey (EAVS) jurisdictions said that more than two-thirds were 61 years or older and less than one-fifth were younger than 41 years old. This means they are more likely to have age-related visual or dexterity disabilities, making accessibility a priority.

Voters may also interact directly with the e-poll book. Depending on the design of the system, voters may be asked to:

- Confirm information on a screen
- Provide identification by handing an ID card to a worker or placing it in position for the system to read
- Sign their name on the main e-poll book screen or on a smaller device
- Be given information on paper, including information to authorize them to vote or activate the voting system or directions to a different voting location

Check-in is a public, not a private procedure. The list of voters is a public record, and in some locations, the names and even addresses of voters are announced for observer to hear. This means that the concerns about voter privacy that are central to the design of voting systems do not apply to e-poll books.

Check-in is an assisted task, with no expectation that it is done independently. The election worker and the voter work together to complete the check-in process. Election workers assist all voters, including those with language or accessibility needs. An important consideration in setting accessibility requirements for e-poll books is when (and what type of) assistance is acceptable and when it interferes with voter independence.

E-poll book hardware and software are different from voting systems. E-poll books are often assembled from standard computing devices, such as a laptop or tablet. They run on conventional operating systems rather than a custom platform. They often include several additional COTS devices including a printer, signature pad, or barcode scanner.

There is more flexibility in how e-poll books are set up for use. Unlike a voting system, they can be set up for the specific team of election workers who will use them during a voting day

- They are set up once at the start of the day and peripherals are attached at that time by someone familiar with the system
- E-poll books are typically placed on a working surface where they can be adjusted for physical reach and touch
- Like voting systems, lighting conditions may not be optimal, including poor lighting, reflections, or glare from lights and windows

Requirements that adjust the screen display are an important way to mitigate these issues and make sure that the information on the screen is clear.

There may be requirements for actions by election workers that affect the fundamental nature of the task. These actions may include:

- Reviewing of comparing a voter's signature to the image of one on file
- Reading information on an ID card
- Handling an ID card or a scanner to read the voter information into the system, a printed voter authorization form to be given to the voter, or turning the e-poll book screen so the voter can read it or sign their name

An e-poll book interface can assist election workers in performing some tasks. For example, they can include instructions for infrequent tasks, or may include design elements to draw attention to similar names or notifications of voter status in a way that would be considered bias under VVSG 2.0 requirement *5.2-A No bias* in a voting system. The report *Checklists for usability and accessibility of electronic pollbooks* includes a list of usability considerations specific to e-poll books that could be used for a heuristic examination as part of a certification or procurement process.

Section 1 - Security Requirements

Security requirements are organized based on the following security categories:

1. Access control
2. Physical security measures
3. System integrity
4. Network/telecommunications security
5. Software design/architecture standards
6. Logging
7. Supply chain risk management

Each numbered section below contains a brief explanatory description followed by the actual requirements, labeled 1.1, 1.2, etc. for section 1 or 7.1, 7.2, etc. for section 7.

Section 1.1 – Access control

Access to both physical and digital spaces containing EPB systems, voter information, and communication equipment must be strictly controlled during the entire EPB lifecycle from manufacturing and development to end-of-life disposal of the information and equipment to detect and prevent supply chain attacks.

EPB manufacturers must establish procedures and technical controls that reflect applicable federal and state laws, Executive Orders, regulations, directives, policies, standards, and guidance to control access to physical sites and networks containing EPBs and related communications equipment. Access control systems will be automated when possible.

An EPB system must be configured to:

- Implement account management
- Follow established account management procedures and processes
- Implement and enforce role-based access
- Implement and support multi-factor authentication
- Implement and enforce separation of duties
- Implement and enforce least privilege
- Implement and enforce session termination, device lock, and reauthentication
- Record unsuccessful logon attempts
- Implement system use notification

1.1.1 – Account management

EPB systems and related components such as databases or network communications equipment must authenticate each user with access to the system using an automated account management system. The account management system must require unique passwords for each user.

Discussion
The following are best practices for account management:

- Remove vendor access when no longer necessary
- Automatically remove temporary or emergency accounts after a specified date or period
- Automatically disable inactive accounts after a specific period
- Audit account creation, modification, enabling, disabling, and account removal actions with a notification to auditing personnel
- Limit the use of dynamic privilege management capabilities
- Do not allow the use of shared or group accounts
- Remove assigned privileges from accounts when removed from the group

References: NIST SP 800-53 rev. 5 (AC-2)

1.1.2 – Access control policies and procedures

The EPB system must have documentation for access control policies and procedures describing how the requirements in Section 1 are implemented.

References: NIST SP 800-53 rev. 5 (AC-1)

1.1.3 – Role-based access

The EPB system must implement role-based access control (RBAC) with least privilege. Each role must be limited to the functions, processes, and data authorized for the specific role.

References: NIST SP 800-53 rev. 5 (AC-2)

1.1.4 – Multi-factor authentication

The system shall enforce multi-factor authentication (MFA) for all privileged operations if the system has a multi-factor authentication option.

Discussion
Privileged operations can include account creation, deletion, permission modification, or when directly updating external databases such as voter registration databases. Additionally, Multi-factor authentication does not mean having multiple passwords.

References: NIST SP 800-63-3

1.1.5 – Separation of duties

The EPB system must be configurable to enforce separation of duties as defined by the jurisdiction.

Discussion
For example, changes to voter information or system configurations may need to be authorized by two or more personnel to mitigate insider threats.

References: NIST SP 800-53 rev. 5 (AC-5)

1.1.6 – Least privilege

The EPB system must enforce the concept of least privilege for accounts to restrict both privileged and non-privileged accounts to only permission required to carry out the role assigned to the account.

Discussion
A poll worker should be prevented from making configuration changes on the system. The concept of least privilege should also be applied to administrators and supervisor groups and accounts.

References: NIST SP 800-53 rev. 5 (AC-6)

1.1.7 – Session termination, device lock, and reauthentication

The EPB system must include session termination, device lock, and reauthentication functionality including:

1. a user-initiated or time configurable automatic lockout when a user is away from the system, which can be defined and implemented by the jurisdiction
2. a configurable mechanism to automatically terminate a user session after a defined period of inactivity and lock the device; which can be defined and implemented by the jurisdiction
3. requiring reauthentication of the authorized user after the session is terminated and the device locked; and
4. the account lockout must include a blank or configurable screen when the system is locked to obscure any data presented on the screen when terminated.

References: NIST SP 800-53 rev. 5 (AC-11, AC-12)

1.1.8 – Unsuccessful logon attempts

The EPB system must be configured to lock after a configurable number of login attempts for 15 minutes or until an administrator or technician can unlock the account.

References: NIST 800-53 rev. 5 (AC-7)

1.1.9 – System use notification

The EPB system must include a configurable logon banner or system use notification for the user to accept upon logon.

References: NIST SP 800-53 rev. 5 (AC-8)

1.1.10 – Information and data flow

Information flows between EPB systems and other systems connected to public networks must be limited to only the required information to protect voter data from being accessible by unauthorized users.

Discussion
The use of unique IDs not easily associated with a voter should be used to transmit information rather than using actual voter PII during data exchanges.

References: NIST 800-53 rev. 5 (AC-4)

Section 1.2 – Physical security measures

Physical security measures must be in place to prevent unauthorized access to devices, communications equipment, and voter information to include any database backups.

An EPB system must:

- Document asset management features
- Implement and enforce device disk encryption
- Enforce BIOS or firmware interface access restrictions
- Document the application of tamper evident sealing
- Document anti-theft controls, and emergency system decommissioning

1.2.1 – Documentation of asset management features

The EPB system documentation must detail the location and use of any unique serial numbers, part numbers, or other identifying features for each individual hardware component of the system that can be used for asset management.

References: NIST SP 800-53 rev. 5 (CM-8)

1.2.2 – Device disk encryption

Each component of the EPB system containing internal memory used to store voter or ballot information must enforce whole disk encryption.

References: NIST SP 800-53 rev. 5 (AC-19)

1.2.3 – Device BIOS or other firmware interface access

Each component of the EPB system containing BIOS or other firmware interface must require authentication to access the device BIOS or other firmware interface. If passwords/codes are used, they should follow strong password guidelines, and be changed from any manufacturer defaults.

References: NIST SP 800-53 rev. 5 (SI-7)

1.2.4 – Document the application of tamper evident sealing

The EPB system documentation must include information on how and where to apply tamper evident sealing of the physical components of the system that contain voter or ballot information. Additionally, any built-in tamper evident protections (lights, alarms, logging) must be documented.

References: NIST SP 800-53 rev. 5 (SR-5, SA-18)

1.2.5 - Document anti-theft controls, and emergency system decommissioning

The EPB system documentation must include information on anti-theft controls including functionality to remotely secure a stolen or lost device with access to pertinent data.

Discussion

When devices are lost or stolen, whether they have the data stored locally or access to cloud data, especially with the potential of admin privileges to manipulate said data, functionality must be put in place to remotely remove content or access from the device.

Section 1.3 – System Integrity

The EPB system must implement security measures to prevent malicious activity and protect the integrity, confidentiality, and availability of data. The system must be configured to:

- Support an EDR tool (public network connected EPB systems only)
- Support an antivirus tool to detect and alert on malicious code
- Support file integrity checking to monitor file changes

1.3.1 – Endpoint detection and response (EDR) tool

If the EPB system requires connection to a public network during election day operation, the system must support an EDR tool to prevent, detect, and respond to attempts to manipulate the system such as: cross-site scripting (XSS), code injection, or denial of service (DoS) attacks.

References: NIST SP 800-53 rev. 5 (SI-4)

1.3.2 – Antivirus tool

The EPB system must implement an antivirus tool to detect and alert on malicious code.

References: NIST SP 800-53 rev. 5 (SI-3)

1.3.3 – Authentication to access configuration file

The EPB system must allow only authenticated system administrators to access and modify device configuration files.

References: NIST SP 800-53 rev. 5 (SI-7), VVSG 2.0 13.1.1-A

1.3.4 – Verification of voter information

The EPB system must:

1. cryptographically verify the integrity and authenticity of all voter data;
2. immediately log any verification error; and
3. immediately present on-screen any verification errors.

Discussion

The process of verifying voter information is a defense in depth measure against accidental errors or a malicious incident regarding modified or false voter information.

References: VVSG 2.0 13.2-B

1.3.5 – Cryptographic module validation

The EPB system's cryptographic functionality must be implemented in a cryptographic module that meets current FIPS 140 validation, operating in FIPS mode.

This applies to:

1. software cryptographic modules, and
2. hardware cryptographic modules.

Discussion
Use of cryptographic modules validated at level 1 or above ensures that the cryptographic algorithms used are secure and correctly implemented. The current version of *FIPS 140[NIST01, NIST19a]* and information about the *NIST Cryptographic Module Validation Program* are available under *[NIST20e]* in Appendix C: References. Note that a device can use more than one cryptographic module, and quite commonly can use a software module for some functions and a hardware module for other functions.

References: VVSG 2.0 13.3-A

1.3.6 – Cryptographic strength

The EPB system's cryptography must employ NIST approved algorithms with a security strength of at least 112-bits.

Discussion
At the time of this writing, NIST specifies the security strength of algorithms in SP 800-57, Part 1. This NIST recommendation will be revised or updated as new algorithms are added, and if cryptographic analysis indicates that some algorithms are weaker than presently believed. The security strengths of SP 800-57 are based on estimates of the amount of computation required to successfully attack the particular algorithm. The specified strength should be sufficient for several decades.

This requirement is not intended to forbid all incidental use of non-approved algorithms by OS software or standardized network security protocols.

References: VVSG 2.0 13.3-C

1.3.7 – Cryptographic key management documentation

The EPB system documentation must describe how key management is to be performed.

Discussion
This documentation provides procedural steps that can be taken to ease the burden of key management and safely perform these operations.

References: VVSG 2.0 13.3-E

Section 1.4 – Network/Telecommunications Security

The EPB system must be configured to:

- Implement FIPS 140 approved encryption for the transfer of data
- Disallow connections to unapproved external networks
- Disallow connections to unapproved external devices
- Implement network firewall settings for approved communication (public network connected EPB systems only)
- Documentation of the network and communications architecture

1.4.1 – Network encryption

The system must be configured to utilize FIPS 140 approved network encryption for the transfer of data.

References: NIST SP 800-53 rev. 5 (AC-17)

1.4.2 – Disallow connections to unapproved external networks

If the system requires connection to a public network during election day voter check-in operations, the e-poll book must be configured to disallow connections to unapproved external networks. This may be accomplished through IP or MAC address allow listing or other configurations where external network access is explicitly granted.

References: NIST SP 800-53 rev. 5 (AC-3, AC-4)

1.4.3 – Disallow connections to unapproved external devices

The e-poll book must be configured to disallow connections to unapproved external devices.

Discussion
This requirement applies to devices that can be recognized as approved, such as only allowing connections to managed devices.

References: NIST SP 800-53 rev. 5 (AC-4, AC-20)

1.4.4 – Network firewall

If the EPB system requires connection to a public network during election day voter check-in operation, the e-poll book must implement a firewall configured to only allow approved communication with each device within the system.

References: NIST SP 800-53 rev. 5 (AC-3)

1.4.5 – Confidentiality and integrity of transmitted data

The EPB system must:

1. mutually authenticate all network connections;
2. cryptographically protect the confidentiality of all data sent over a network; and
3. cryptographically protect the integrity of all voter information sent over the network.

Discussion
Mutual authentication provides assurance that each electronic device is legitimate. Mutual authentication can be performed using various protocols, such as IPsec and SSL/TLS. This requirement includes network appliances such as switches, firewalls, and routers within its scope.

This does not prevent the use of "double encrypted" connections employing cryptography at multiple layers of the network stack. Data must be encrypted before transmission.

Integrity protection ensures that any inadvertent or intentional alterations to data are detected by the recipient. Integrity protection for data in transit can be provided through the use of various protocols such as IPsec VPNs and SSL/TLS. For more information about TLS implementations, see *NIST SP 800-52 rev. 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.

References: VVSG 2.0 13.4-A

1.4.6 – Documentation of the network and communications architecture

The EPB system documentation must include the network and communications architecture of any network used by any portion of the system.

Discussion
Documentation can assist with data flow analysis, proper network configuration, and architecture to properly support the system.

References: NIST SP 800-53 rev. 5 (PL-8, PM-7, SA-17); VVSG 2.0 15.4-A

1.4.7 – Secure network configuration documentation

The EPB system documentation must list security configurations and be accompanied by network security best practices according to the National Institute of Standards and Technology (NIST).

Discussion
A variety of documentation providing secure configurations for network devices is publicly available from the US government.

If outside manufacturers provide guidance and best practices, these need to be documented and used to the extent practical.

This documentation should include the use of wireless security protocols, firewalls and intrusion detection systems, and switch and/or router configuration.

References: NIST SP 800-53 rev. 5 (PL-8, PM-7, SA-17); VVSG 2.0 15.4-B

Section 1.5 – Software Design and Architecture

The EPB system or its documentation must:

- Execute on a supported operating system
- Support updates and patching
- Utilize recognized software standard(s)
- Perform client-side input validation
- Perform server-side input validation
- Document the use of third-party code or libraries
- Disable unneeded services and applications
- Document proper media sanitization

1.5.1 – Execute on a Supported Operating System

The EPB System software must execute on an operating system that is currently supported with updates and/or patches.

References: NIST SP 800-53 rev. 5 (SA-22)

1.5.2 – Support Updates and Patching

The EPB system's applications must have the ability to be updated and/or patched.

References: NIST SP 800-53 rev. 5 (SA-22)

1.5.3 – Utilize recognized software standards

Application logic must adhere to a published, credible set of coding rules, conventions, or standards (called "coding conventions") that enhance the workmanship, security, integrity, testability, and maintainability of applications.

Discussion

Coding conventions may be specified by the EAC in conjunction with voting system test labs.

The requirements to follow coding conventions serves two purposes. First, by requiring specific risk factors to be mitigated, coding conventions support integrity and maintainability of voting system logic. Second, by making the logic more transparent to a reviewer, coding conventions facilitate test lab evaluation of the logic's correctness to a level of assurance beyond that provided by operational testing.

References: NIST SP 800-53 rev. 5 (SI-2, SI-7); VVSG 2.0 2.1-C

1.5.4 – Input validation and error defense

The EPB system must:

1. monitor I/O operations;
2. validate all input against expected parameters, such as data presence, length, type, format, uniqueness, or inclusion in a set of whitelisted values;
3. report any input errors and how they were corrected; and
4. check information inputs to ensure that incomplete or invalid inputs do not lead to irreversible error.

Discussion

Input includes data from any input source: input devices (such as touch screens, keyboards, keypads, and assistive devices), networking port, data port, or file.

References: NIST SP 800-53 rev. 5 (SI-10); VVSG 2.0 2.5.2-A

1.5.5 – Escaping and encoding output

EPB system software output must be properly encoded, escaped, and sanitized.

Discussion

The output of a software module can be manipulated or abused by attackers in unexpected ways to perform malicious actions. Ensuring that outputted data is of an expected type or format assists in preventing this abuse. Additional information about this software weakness can be viewed at *MITRE CWE 116: Improper Encoding or Escaping of Output [MITRE20c].*

References: VVSG 2.0 2.5.3-A

1.5.6 – Sanitize output

The EPB system must sanitize all output to remove or neutralize the effects of any escape characters, control signals, or scripts contained in the data which could adversely manipulate the output source.

Discussion
Output includes data to any output source: output devices (such as touch screens, LCD screens, printers, and assistive devices), networking port, data port, or file.

References: VVSG 2.0 2.5.3-B

1.5.7 – Stored injection

The EPB system must sanitize all output to files and databases to remove or neutralize the effects of any escape characters, control signals, or scripts contained in the data which could adversely manipulate the system if the stored data is read or imported at a later date by another part of the system.

Discussion
A stored injection attack saves malicious data which is harmless when stored, but which is potent when read later in a different context or when converted to a different format. For example, a malicious script might be written to a file and do no harm to the EPB system, but later be evaluated and harmful when the file is transferred and read by the voter registration system. Input should also be filtered, but sanitizing stored output provides defense in depth.

References: VVSG 2.0 2.5.3-C

1.5.8 – Third-Party Code and Libraries

The EPB system documentation must identify and list all third-party code and libraries in a way that allows users to track against CVE listings. This should include software name, version, and manufacturer.

References: NIST SP 800-53 rev. 5 (SI-2)

1.5.9 – Application allowlisting

The EPB system must only run applications that have been verified against an allowlist.

Discussion
This requirement helps ensure only authorized applications run on the EPB system.

References: NIST SP 800-53 rev. 5 (SA-8); VVSG 2.0 14.3.2-C

1.5.10 – Integrity protection for software allowlists

The EPB system must protect the integrity and authenticity of the allowlist configuration files.

Discussion
If the allowlist is improperly modified, the software allowlisting mitigation can be defeated. The most common way of providing allowlist configuration file protection could be a digital signature.

References: VVSG 2.0 14.3.2-D

1.5.11 – Documentation of media sanitization procedures

The EPB system documentation must include instructions on the proper sanitization of storage media prior to transfer or disposal of equipment.

References: NIST SP 800-53 rev. 5 (MP-6)

Section 1.6 – Logging

The EPB system must be configured to log records for:

- General system usage
- Operational maintenance activity
- Resolving system issues
- Validating system integrity
- Generating reports

1.6.1 – General system usage

The EPB system must be configured to log records of general system usage including, but not limited to:

- Account management
- User logon attempts
- Application execution

References: NIST SP 800-53 rev. 5 (AU-2, AU-3, AU-6)

1.6.2 – Operational maintenance activity

The EPB system must be configured to log records including, but not limited to:

- Software updates or patching
- System startup and shutdown
- Changes in system configuration

References: NIST SP 800-53 rev. 5 (AU-2, AU-3, AU-6)

1.6.3 – Application errors

The EPB system must be configured to log all application errors. The system documentation must contain descriptions of error codes and messages for use in troubleshooting.

References: NIST SP 800-53 rev. 5 (AU-2, AU-3, AU-6)

1.6.4 – System integrity

The EPB system must be configured to log records including, but not limited to:

- EDR alerts
- Antivirus alerts
- File integrity monitoring
- Physical tamper alerts (if applicable)

References: NIST SP 800-53 rev. 5 (AU-2, AU-3, AU-6)

1.6.5 – Report Generation

The system must be configured to log the generation of all reports.

Section 1.7 – Supply Chain Risk Management

The EPB system documentation must detail the risk assessments and controls utilized to reduce the potential for supply chain compromises. The documentation must contain:

- List of approved suppliers
- Verification of authenticity of components
- Verification of provenance of system devices

1.7.1 – List of Approved Suppliers

The EPB system documentation must include a list of approved suppliers. If the supplier goes out of business or is purchased by another company, the EPB system documentation must be updated to include current information.

References: NIST SP 800-53 rev. 5 (SR-6)

1.7.2 – Authenticity of Components

The EPB system documentation must detail controls used to determine if the system's software, firmware, hardware, or other system components are authentic and unaltered. For software or firmware, this must include hash validation procedures. For hardware, this must include details on identifying manufacturer approved hardware through checking labeling, tamper evidence, or other characteristics.

References: NIST SP 800-53 rev. 5 (SR-4, SA-19)

1.7.3 – Provenance of Devices

The system documentation must detail the origin and ownership of any software, firmware, or hardware used within the system.

References: NIST SP 800-53 rev. 5 (SR-4)

Section 2 – Accessibility and Usability Requirements

The requirements for e-poll book usability and accessibility are based on the requirements for voting systems in the VVSG 2.0. They have been adapted for e-poll books with changes in wording as well as adding to or removing sections of the original requirement.

There are three groups of requirements:

1. Core functionality for all e-poll books
2. E-poll books with audio output for either election workers or voters
3. E-poll books that support alternative languages

In some cases, new requirements have been added to the end of each group.

Section 2.1 – Core functionality

2.1.1– User-centered design process

The manufacturer must submit a report providing documentation that the system was developed following a user-centered design process.

The report must include, at a minimum:

1. A listing of user-centered design methods used;
2. the types of voters and election workers included in those methods;
3. how those methods were integrated into the overall implementation process; and
4. how the results of those methods contributed to developing the final features and design of the system.

Discussion

The goal of this requirement is to allow the manufacturer to demonstrate, through the report, the way their implementation process included user-centered design methods.

ISO-9241-210:2019 Ergonomics of human-system interaction – Part 210: Human-centered design for interactive systems provides requirements and recommendations for human-centered principles and activities throughout the life cycle of computer-based interactive systems. It includes the idea of iterative cycles of user research to understand the context of

use and user needs, creating prototypes or versions, and testing to confirm that the product meets the identified requirements.

This requirement does not specify the exact user-centered design methods to be used, or their number or timing.

The ISO group of requirements, *Software engineering – Software product quality requirements and evaluation (SQUARE) – Common Industry Format (CIF) for Usability* includes several standards that are a useful framework for reporting on user-centered design activities and usability reports:

- *ISO/IEC TR 25060:2010: General framework for usability-related information*
- *ISO/IEC 25063: 2014: Context of use description*
- *ISO/IEC 25062:2006: Usability test reports*
- *ISO/IEC 25064:2013: User needs report*
- *ISO/IEC 25066:2016: Evaluation report*

References: 2.1.36, 2.1.37, VVSG 2.0 (2.2-A), ISO-9241-210:2019, ISO/IEC TR 25060:2010, ISO/IEC 25063:2014, ISO/IEC 25062:2006, ISO/IEC 25064:2013, ISO/IEC 25066:2016

2.1.2– Vote records

All records produced by the e-poll book must have the information required to support auditing by election workers and others who can only read English.

References: VVSG 2.0 (5.1-C), WCAG 2.0, and Section 508

2.1.3– Accessibility documentation

As part of the overall system documentation, the manufacturer must include descriptions and instructions for all accessibility features that describe:

- Recommended procedures for supporting the use of the system by voters with disabilities
- How the e-poll book system supports those procedures

Discussion

The purpose of this requirement is for the manufacturer not simply to deliver system components, but also to describe the accessibility scenarios they are intended to support, so that election offices have the information they need to effectively make accessibility features available to voters with disabilities.

References: VVSG 2.0 (5.1-F), WCAG 2.0, and Section 508

2.1.4 – Sound cues

Sound and visual cues must be coordinated so that sound cues are accompanied by visual cues.

Discussion

The equipment might beep if the election worker or voter makes an error. If so, there has to be an equivalent visual cue, such as the appearance of an icon or blinking element.

Audio output also supports non-written languages, voters with low literacy, or voters with low vision.

References: VVSG 2.0 (5.2-E), WCAG 2.0, and Section 508

2.1.5 – Reset to default settings

If the adjustable settings of an e-poll book have been changed by the election worker, the system must automatically reset to the default setting when the election worker signs out.

Discussion

This ensures that the system presents the same initial appearance to each election worker.

This requirement covers all settings that can be adjusted, including font size, color, contrast, audio volume, rate of speech, turning on or off audio or video, and enabling alternative input devices.

References: VVSG 2.0 (7.1-A)

2.1.6 – Reset by election worker

There must be a way for the election worker to restore the default settings while preserving the current state of any transaction or activity that the election worker is engaged in.

Discussion

This requirement allows a voter or election worker who has adjusted the system to an undesirable state to reset all settings with the information presented to the voter including any data already entered.

References: VVSG 2.0 (7.1-B)

2.1.7 – Default contrast

The default contrast ration must be at least 10:1 for all elements that visually convey information such as text, controls, and infographics or icons.

1. For electronic displays for voters and election workers, this is measured as a luminosity contrast ratio between the foreground and background colors of at least 10:1.
2. For paper records, the contrast ratio will be at least 10:1 as measured based on ambient lighting of at least 300 lx.

Discussion

This applies to information such as voter names or informational icons identifying election worker selections or other information.

Purely decorative elements that do not communicate meaning do not have to meet this requirement.

A 10:1 luminosity contrast ratio provides enough difference between the text and background to enable people with most color vision deficiencies to read the screen. This is higher than the highest contrast requirements of 7:1 in WCAG 2.0 Checkpoint 1.4.6 (Level AAA) to accommodate a wider range of visual disabilities. There are many free tools available to test color luminosity contrast using the WCAG 2.0 algorithm.

References: VVSG 2.0 (7.1-C), WCAG 2.0, and Section 508

2.1.8 – Contrast options

The e-poll book must provide options for high and low contrast displays, including the alternative display contrast options as listed below:

1. A high contrast option with a white background and dark text, with a luminosity contrast ratio of at least 20:1.
2. A high contrast option with a black background (between #000000 and #111111) and one of the following foreground options, including:
    a. yellow text similar to #FFFF00, providing a contrast ratio of at least 17.5:1,
    b. cyan text similar to #00FFFF, providing a contrast ratio of at least 15:1, and
    c. white text similar to #FAFAFA, providing a contrast ratio of at least 18:1.
3. A low contrast option, providing a contrast ratio in the range of 4.5:1 to 8:1.

Discussion

This requirement for options for the overall display contrast ensures that there is an option for the visual presentation for people whose vision requires either high or low contrast.

High and low contrast options apply to the entire screen, including decorative elements.

Examples of color combinations for low contrast options include:
- brown text similar to #BB9966 on a black background,
- black text on a background with text similar to #BB9966,
- grey text similar to #6C6C6C on a white background,
- grey/brown text similar to #97967E on a black background, and
- grey text similar to #898989 on a dark background similar to #222222

References: VVSG 2.0 (7.1-D), WCAG 2.0, and Section 508

2.1.9 – Color conventions

The use of color by the e-poll book must follow these common conventions:

1. Green, blue, or white is used for general information or as a normal status indicator;
2. Amber or yellow is used to indicate warnings or a marginal status;
3. Red is used to indicate error conditions or a problem requiring immediate attention.

References: VVSG 2.0 (7.1-E)

2.1.10 – Using color

Color coding must not be used as the only means of communicating information, indicating an action, prompting a response, distinguishing a visual element, or providing feedback on system actions or selections.

Discussion
While color can be used for emphasis, some other non-color design element is also needed. This could include shape, lines, words, text, or style. For example, an icon for "stop" can be red enclosed in an octagon shape. Or a background color can be combined with a bounding outline and a label to group elements on the screen.

References: VVSG 2.0 (7.1-F)

2.1.11 – Text size (electronic display)

An e-poll book's electronic display for check-in screens must be capable of showing all information in a range of selectable text sizes, with a default text size at least 4.8 mm (based on the height of the uppercase I), allowing the text to both increase and decrease in size.

The e-poll book may meet this requirement in one of the following ways:

1. Provide continuous scaling with a minimum increment of 0.5 mm that covers the full range of text sizes from 3.5 mm to 9.0 mm.
2. Provide at least four discrete text sizes, in which the main options fall within one of these ranges:
    a. 3.5-4.2 mm (10-12 points)
    b. 4.8-5.6 mm (14-16 points)
    c. 6.4-7.1 mm (18-20 points)
    d. 8.5-9.0 mm (24-25 points)

Discussion
The sizes are minimums. These ranges are not meant to limit the text on the screen to a single size. The text can fall in several of these text sizes. For example, primary instructions might be in the 4.8-5.6 mm range, secondary information in the 3.5-4.2 mm range, and titles or button labels in the 6.4-7.1 mm range.

References: VVSG 2.0 (7.1-G), WCAG 2.0, Section 508

2.1.12 – Text size (paper)

If the e-poll book provides printed materials to the voter, they must have a font size of at least 3.5 mm (10 points).

Discussion
Although the system can be capable of printing in several font sizes, local or state laws and regulations can also govern the use of various font sizes.

If the system includes a large-print display option, a good range for the text size is 6.4-7.1 mm matching the size in 2.*1.11 – Text size (electronic display)*.

References: VVSG 2.0 (7.1-I), WCAG 2.0, Section 508

2.1.13 – Scaling and zooming

When the text size is changed, all other information in the interface, including informational icons, screen titles, buttons, and entry fields, must change size to maintain a consistent relationship to the size of the text. Informational elements in the interface do not have to be scaled beyond the size of the text.

1. When the text is enlarged up to 200% (or 7.1 mm text size), the layout must adjust so that there is no horizontal scrolling or panning of the screen.

Discussion
The intention of this requirement is that all of the informational elements of the interface change size in response to the text size. However, some interface designs include elements that are already large enough that making them larger would distort the layout. In this case, this does not require those elements to grow proportionately beyond the size of the text.

Techniques for managing scaling and zooming an electronic interface while adjusting the layout to fit the new size are sometimes called responsive design or responsive programming.

This requirement does not preclude novel approaches to on-screen magnification such as a zoom lens showing an enlarged view of part of the screen (as long as it meets the requirements for the operability of the controls).

References: VVSG 2.0 (7.1-H), WCAG 2.0

2.1.14 – Toggle keys

The status of all locking or toggle controls or keys (such as the “shift” key) for the e-poll book that are available to the election worker or voter must be visually discernable, and discernable through either touch or sound.

Discussion
This applies to any physical controls or keys that have a locking or toggle function.

References: VVSG 2.0 (7.1-O), WCAG 2.0, Section 508

2.1.15 – Identifying controls

Buttons and controls used to operate the e-poll book must be distinguishable by both shape and color for visual and tactile perception.

Well-known arrangements or groups of keys may be used only for their primary purpose. For example, a full alphabetic keyboard may be used for entering text in a form, or navigation keys on the keyboard may be used by election workers.

Discussion
This applies to buttons and controls implemented either on-screen or in hardware. For on-screen controls, shape includes the label on the button. Redundant cues help those with low vision. They also help individuals who have difficulty reading the text on the screen, those who are blind but have some residual vision, and those who use the controls on a system because of limited dexterity. While this requirement primarily focuses on those with low vision, features such as tactile controls and on-screen controls intended to primarily address one kind of disability often assist others as well. The Trace Center's EZ Access design is an example of button functions distinguishable by both shape and color.

Some examples are:
- Color can be helpful to make different sets of functions visually distinct: groups of buttons can share a color, such as volume up/down.
- Tactile perception requires different shapes, so that finding a control does not rely solely on the layout: all the shapes cannot be squares, but two or four triangles can be used if they point in different directions.
- As a group of well-known keys, a full alphabetic keyboard is acceptable for entering information, but individual keys cannot be used for navigation or selection. Using these keys for functions would require and election worker or voter to see the visual labels or know the arrangement for those functions.

References: VVSG 2.0 (7.1-P), WCAG 2.0, Section 508

2.1.16 – Display and interaction options

The e-poll book must provide at least a visual format with enhanced visual options, supporting full functionality under all visual options.

Discussion
Full functionality includes at least instructions and feedback regarding:

- how to use accessibility features and settings;
- changes in the display format or control options
- navigating the screen
- activating options
- confirming choices

References: VVSG 2.0 (7.2-A), WCAG 2.0, Section 508

2.1.17 – Scrolling

If the amount of information that needs to be shown means that it does not fit on a single screen using the election worker's visual display preferences, the e-poll book must provide a way to view all of the information.

1. The e-poll book may display the information by:
    a. Pagination – dividing the list of voters or other information into "chunks," each filling one screen and providing ways for the election worker to navigate among the different chunks, or
    b. Scrolling – keeping all of the content on a single long display and providing controls that allow the election worker to scroll continuously through the content.
2. For either display method, the interface must:
    a. Have a fixed header or footer that does not disappear, so election workers always have access to navigation elements.
    b. Include easily perceivable cues in every display format to indicate that there is more information available.

Discussion

The ability to scroll through long lists of information on a single logical page can be particularly important when an election worker selects larger text.

Information elements that need not scroll might include instructions and general controls including preference settings or navigation controls.

A scrolling interface that meets this requirement offers election workers a combination of easily perceivable controls or gestures to navigate through long lists or other lengthy content. For example:

- Navigation does not rely on knowledge of any particular computer platform or interface standard.
- Navigation does not only rely on conventional platform scroll bars, which operate differently on two of the major commercial computer platforms.
- Controls have visible labels that include words or symbols.
- Controls are located in the election worker's visual viewing area at the bottom (or top) of the

scrolling area, for example in the center of a column of names or a paragraph of text. This is especially helpful for people with low digital or reading literacy.

References: VVSG 2.0 (7.2-D), WCAG 2.0, Section 508

2.1.18 – Touch screen gestures

E-poll books may use touch screen gestures (physical movements by the user while in contact with the screen to activate controls) in the interface if the following conditions are met:

1. Gestures are offered as another way of interacting with a touch screen and an optional alternative to the other touch interactions.
2. Gestures work consistently.
3. Gestures are used in a way that does not create accidental activation of an action through an unintended gesture.
4. Gestures are limited to simple, well-known gestures.
5. Gestures do not require sequential, times, or simultaneous actions.

Discussion

In relying on simple and common gestures, this requirement does not intend to fully duplicate the gestures for commercial mobile platforms used with an audio format for accessibility.

Tapping (touching the screen briefly) is the most basic gesture and is used on all touch screens. Other commonly used gestures include:
- Pinching or spreading fingers to zoom,
- swiping to scroll, and
- pressing and holding to drag.

Examples of gestures that require sequential or simultaneous actions are double-tapping, 2, 3, or 4 finger swiping, touch and hold for a set period of time, or those that require coordinated actions with fingers on both hands. On desktop systems, assistive preference options like Sticky Keys can make these complex gestures accessible, but they require familiarity beyond what is acceptable in an e-poll book system.

Examples of times gestures include differentiating between long and short touches, or which require touching twice in rapid succession to highlight and then activate a button or selection.

References: VVSG 2.0 (7.2-E)

2.1.19 – Accidental activation

Both on-screen and physical controls on the e-poll book must be designed to prevent accidental activation.

Discussion

There are at least two kinds of accidental activation:

- When a control is activated to execute an action as it is being "explored" by the user because the control is overly sensitive to touch.
- When a control is in a location where it can easily be activated unintentionally. For example, when a button is in the very bottom left corner of the screen where a user might hold the unit for support.

The draft for WCAG 2.1, the next version of WCAG 2.0, includes a similar requirement and offers guidelines for preventing accidental activation including that the activation be on the release of the control (an "up-event") or equivalent, or that the system provides an opportunity to confirm the action.

References: VVSG 2.0 (7.2-H), WCAG 2.1

2.1.20 – Touch area size

If the e-poll book has a touch screen, the touch target areas must:

1. Be at least 12.7 mm (0.5 inches) in both vertical and horizontal dimensions;
2. be at least 2.54 mm (0.1 inches) away from adjacent touch areas; and
3. not overlap another touch area.

Discussion

The requirements for touch size areas are larger than commercial standards for mobile devices:

- to ensure that the touch areas are large enough for users with unsteady hands;
- to ensure that systems allow full adjustment to the most comfortable posture; and
- to allow for touch screens that do not include advanced algorithms to detect the center point of a touch.

The required marking area size is within the sizes suggested in the draft WCAG 2.1 for target areas that accept a touch action.

An MIT Touch Lab study of Human Fingertips to Investigate the Mechanics of Tactile Sense found that the average human finger pad is 10-14 mm and the average fingertip is 8-10 mm.

References: VVSG 2.0 (7.2-I), WCAG 2.1

2.1.21 – Key operability

Physical keys, controls, and other manual operations on the system must be operable with one hand and not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys must be no greater than 5 lbs. (22.2 N).

Discussion
Users can operate controls without excessive force. This includes operations such as inserting a smart card or swiping magnetic stripe cards.

This does not apply to on-screen controls.

References: VVSG 2.0 (7.2-K), WCAG 2.0, Section 508

2.1.22 – Bodily contact

The e-poll book controls must not require direct bodily contact or for the body to be part of any electrical circuit. If some form of contact is required, a stylus or other device with built-in permanent tips will be supplied to activate capacitive touch screens.

Discussion
This requirement ensures that controls and touch screens can be used by individuals using prosthetic devices or that it is possible to use a stylus on touch screens for either greater accuracy or limited dexterity input.

One type of touch screen – capacitive touch panels – rely on the user's body to complete the circuit. They can be used if manufacturers supply a stylus or other device that activates the capacitive screen.

References: VVSG 2.0 (7.2-L), WCAG 2.0, Section 508

2.1.23 – No repetitive action

E-poll book keys or controls must not have a repetitive effect when they are held in an active position.

Discussion
This is to preclude accidental activation. For instance, if a user is typing a name, depressing and holding the "e" key results in only a single "e" added to the name.

References: VVSG 2.0 (7.2-M), WCAG 2.0, Section 508

2.1.24 – System response time

The e-poll book must complete a visual response or display in no more than 1 second or displays an indicator that a response is still being prepared.

Discussion
This is to allow the user to quickly perceive that an action has been detected by the system and is being processed. The user never gets the sense of dealing with an unresponsive or "dead" system.

References: VVSG 2.0 (7.2-N)

2.1.25 – System-related errors

The e-poll book must help election workers complete their duties accurately and effectively, ensuring that the features of the system do not lead to election workers making errors.

Discussion
This requirement is meant to encourage innovation in meeting usability principles while ensuring that any new design features not hinder election workers in understanding and completing their duties effectively.

References: VVSG 2.0 (7.3-A)

2.1.26 – Feedback

The e-poll book must provide unambiguous feedback confirming each election worker action.

References: VVSG 2.0 (7.3-E)

2.1.27 – Warnings, alerts, and instructions

Warning, alerts, and instructions issued by the e-poll book must be distinguishable from other information.

1. Warnings and alerts must clearly state, in plain language:
    a. The nature of the issue or problem,
    b. whether the election worker has performed or attempted an invalid operation or whether the e-poll book itself has malfunctioned in some way, and
    c. the responses available to the election worker.
2. Each step in an instruction or item in a list of instructions must be separated:
    a. Spatially in visual formats, and
    b. with a noticeable pause in audio formats.

Discussion
For instance, “Do you need more time? Select ‘Yes’ or ‘No’.” rather than “System detects imminent timeout condition.” In case of an equipment failure, the only action available to the voter might be to get assistance from an election worker.

References: VVSG 2.0 (7.3-K), WCAG 2.0, Section 508

2.1.28 – Icon labels

When an icon label is used in the electronic interface to convey information, indicate an action, or prompt a response, it must be accompanied by a corresponding label that uses text.

Discussion
While icons can be used for emphasis when communicating with a user, they are not to be the

only means by which information is conveyed since there is no widely accepted "iconic" language, and therefore, not all users might understand a given icon.

References: VVSG 2.0 (7.3-L), ADA Standards for Accessible Design (Chapter 7)

2.1.29 – Instructions for election workers

The e-poll book must include clear, complete, and detailed instructions and messages for setup, check-in, shutdown, and how to use accessibility features.

1. The documentation required for normal operation must be:
    a. Presented at a level appropriate for election workers who are not experts in e-poll books and computer technology, and
    b. in a format suitable for use in the polling place.
2. Printed procedural instructions, and on-screen instructions and messages must enable the election workers to verify that the e-poll book:
    a. Has been setup correctly (setup),
    b. is in correct working order to check-in voters (polling), and
    c. has been shut down correctly (shutdown).

Discussion

This requirement covers documentation for those aspects of system operation normally performed by election workers and other "non-expert" operators. It does not address inherently complex operations such as device configuration. The instructions are usually in the form of a written manual, but can also be presented on other media, such as a DVD or video. In the context of this requirements, "message" means information delivered by the system to the election workers as they attempt to perform setup, polling, or shutdown operations.

For instance, the documentation should not presuppose familiarity with personal computers. A single large reference manual that simply presents details of all possible operations would be difficult to use, unless accompanied by aids such as a simple "how-to" guide.

It is especially important that election workers and other non-expert workers know how to set up accessibility features which are not used frequently.

Overall, election workers should not have to guess whether a system has been setup correctly. The documentation should make it clear what the system "looks like" when correctly configured.

References: VVSG 2.0 (7.3-O)

2.1.30 – Plain language

Information and instructions for voters and election workers must be written clearly, following the best practices for plain language. This includes messages generated by the e-poll book for election workers in support of the operation, maintenance, or safety of the system.

Discussion

The plain language requirements apply to instructions that are inherent to the e-poll book system or that are generated by default.

Any legally required text is an exception to this plain language requirement.

Plain language best practices are guidelines for achieving clear communications and include:
- Using familiar, common words and avoiding technical or specialized words that election workers are unlikely to understand. For example, “There is additional information on the other side” rather than “Additional information is presented on the reverse.”
- Issuing instructions on the correct way to perform actions, rather than telling election worker what not to do. For example, “Select a voter to strike them off” rather than “If the voter is not selected, they will not be stricken.”
- Addressing the election worker directly rather than using passive voice when giving instructions. For example: “Insert activation card” rather than “the activation card must be inserted.”
- Stating a limiting condition first, followed by the action to be performed when an instruction is based on a condition. For example: “In order to select a voter, do X”, rather than “Do X, in order to select a voter.”
- Avoiding the use of gender-based pronouns. For example: “Select the voter directly on the tablet” rather than “Select his name directly on the tablet.”

References: VVSG 2.0 (7.3-P)

2.1.31 – Electronic display screens

If the e-poll book uses an electronic display screen, the display must have the following characteristics:

1. For all electronic display screens:
    a. Antiglare screen surface that shows no distinct virtual image of a light source or a means of physically shielding the display from such reflections, and
    b. Minimum uniform diffuse ambient contrast ratio for 500 lx luminance : 10 :1.
2. If the display is the primary visual interface for e-poll book functions:
    a. minimum display resolution: 1920 x 1080 pixels.

Discussion

This requirement does not apply to non-primary display screens such as those used by peripheral devices such as printers or signature pads.

References: VVSG 2.0 (8.1-A), WCAG 2.0, Section 508

2.1.32 – Flashing

If the e-poll book emits light in flashes, there must be no more than three flashes in any one-second period.

References: VVSG 2.0 (8.1-B), WCAG 2.0, Section 508

2.1.33 – Secondary ID and biometrics

If the e-poll book uses biometric measures for identifying or authenticating election workers, it must provide an alternative that does not depend on the same biometric capabilities.

Discussion
For example, if fingerprints are used for identification, another mechanism will be provided for users without usable fingerprints.

References: VVSG 2.0 (8.1-D), WCAG 2.0, Section 508

2.1.34 – Eliminating hazards

The e-poll book and all associated devices must be certified in accordance with the requirements of *IEC/UL 62368-1, Edition 3: Standard for Audio/video, Information and Communication Technology Equipment – Part 1: Safety Requirements* by a certification organization accredited by the Department of Labor, Occupational Safety and Health Administration's Nationally Recognized Testing Laboratory program.

The certification organization's scope of accreditation is acceptable if it includes *IEC/UL 62368-1*.

Discussion
IEC/UL 62368-1 is a comprehensive standard for IT equipment.

References: VVSG 2.0 (8.1-K), IEC/UL 62368-1

2.1.35 – Federal standards for accessibility

E-poll books and their software must meet federal standards for accessibility, including the version of *Section 508 Information and Communication Technology (ICT) Final Standards and Guidelines*, in effect as of January 18, 2018, and the *WCAG 2.0 Level AA checkpoints* included in that standard.

Discussion
Section 508 standards apply to electronic and information technology, including computer hardware and software, websites, multimedia, and other technology such as video, phone systems, and copiers. This requirement also supports the ADA.

References: VVSG 2.0 (8.2-A), WCAG 2.0, Section 508

2.1.36 – Usability testing with voters

The manufacturer must conduct usability tests on the e-poll book system with voters using the system to complete any actions to be taken by voters.

1. The tests must include checking-in participant voters who represent the following:
    a. General population
    b. Voters who are native speakers of the language being tested or for each language defined as being supported in the manufacturer's documentation
    c. Blind voters
    d. Voters with low vision
    e. Voters with limited dexterity
2. The manufacturer must submit a report of the results of their usability tests, including effectives, efficiency, and satisfaction measures, as part of their documentation using ISO/IEC 25062:2006: Common Industry Format (CIF) for usability test reports.

Discussion

E-poll book system developers are required to conduct realistic usability tests on their product before submitting the system to conformance testing. This is to ensure that the user-centered design process required for quality implementation has produced a usable and accessible system.

References: VVSG 2.0 (8.3-A), ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports

2.1.37 – Usability testing with election workers

The manufacturer must conduct usability tests of the e-poll book setup, operation during voting, and shutdown as documented by the manufacturer, with representative election workers, to demonstrate that election workers can learn, understand, and perform these tasks successfully.

The test must include handling all variations in voter check-in conditions and other tasks for election workers using the e-poll book at a voting location, including:

1. Setup and opening for polling
2. Operation during voting
3. Use of assistive technology or language options that are part of the system
4. Shutdown at the end of a voting day during a multi-day early voting period, if supported by the e-poll book
5. Setting up the e-poll book to use different display formats and interaction modes.

The test participants must include election workers representing a range of experience.

The manufacturer must submit a report of the results of their usability tests as part of their documentation using ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports.

Discussion

In the usability testing plan from the 2016 report *Usability testing for e-pollbooks: A test protocol* outlines a method for efficiently testing an e-poll book using scenarios for checking in voters that cover variations in this task. The same scenarios can be adapted for usability testing with voters in *1.36 – Usability testing with voters*.

The report, *Checklists for usability and accessibility of electronic pollbooks*, includes checks for a heuristic review of the poll worker interface.

References: VVSG 2.0 (8.4-A), ISO/IEC 25062:2006: Common Industry Format (CIF) for Usability Test Reports

2.1.38 – Physical manipulation

The check-in steps of the e-poll book must allow for assistance from the election worker if the voter needs to manipulate or use any aspect of the e-poll book, including attached devices.

Section 2.2 – Requirements for e-poll books supporting audio

2.2.1 – Information in all modes

Instructions, warnings, and messages must be presented to election workers in the display formats and interaction modes supported by the system.

Discussion

For audio mode, this requirement can be met with audio that includes cues to help users know what to expect. For example, announcing the number of voters in the list makes it easier to jump from one item to another without waiting for the audio to complete. Audio cues can also ensure the election worker is aware of notifications or error conditions.

References: VVSG 2.0 (5.2-C), WCAG 2.0, Section 508

2.2.2 – Audio synchronized

The e-poll book must provide the option for synchronized audio output to convey the same information that is displayed visually to the election worker or voter.

Discussion

This requirement covers all information, including information entered by an election worker or voter unless the information is not easily readable, such as a voter's signature.

This requirement applies to any audio output, whether it is recorded or generated as text-to-speech.

Any differences between audio and visual information are for functional purposes only, with variations only based on differences in the display format and interaction mode, especially for instructions.

This feature can assist voters with cognitive disabilities.

References: VVSG 2.0 (5.2-D), WCAG 2.0, Section 508

2.2.3 – Audio settings

The e-poll book's audio format interface must meet the following requirements:

1. The settings for volume and rate of speech are followed regardless of the technical means of producing audio output.
2. The default volume for each election worker's log-in session is set between 60 and 70 dB SPL.
3. The volume is adjustable from a minimum of 20 dB SPL up to a maximum of 100dB SPL, in increments no greater than 10dB.
4. The rate of speech is adjustable throughout a voter check-in transaction while preserving the current state, with 6 to 8 discrete steps in the rate.
5. The default rate of speech is 120 to 125 words per minute (wpm).
6. The range of speech rates supported is from 60-70 wpm to 240-250 wpm (or 50% to 200% of the default rate), with no distortion.
7. Adjusting the rate of speech does not affect the pitch of the voice.

Discussion

The top speech rate is slower than some audio users prefer for narrative reading to ensure that names are pronounced clearly and distinctively.

Note that the calculation of rate of speech can vary based on the length of the words in the sample, so requirements are stated as a small range.

Speech rates as slow as 50 wpm and as fast as 300 wpm can be included if this can be done without distortion or flanging.

This requirement is intended to be tested using "real ear" measurements, not simply measurements at the point of the audio source.

According to an explanation written by the Trace Center, 60dB SPL is the volume of ordinary conversation.

FCC regulations for hearing aids, *47 CFR Parts 20 and 68: Hearing Aid Standard*, includes useful information about how to test audio volume and quality.

References: VVSG 2.0 (7.1-K), WCAG 2.0, Section 508

2.2.4 – Speech frequencies

The e-poll book's audio format interface must be able to reproduce frequencies over the audible speech range of 315 Hz to 10 KHz.

Discussion

The required frequencies include the range of normal human speech. This allows the reproduced speech to sound natural.

This is not a requirement for the capability of the system so that it is possible to create intelligible audio.

References: VVSG 2.0 (7.1-L), WCAG 2.0, Section 508

2.2.5 – Audio comprehension

The e-poll book's audio format interface must be capable of presenting audio content so that it is comprehensible to people who have normal hearing and are proficient in the language with:

1. Proper enunciation, normal intonation, accurate pronunciation in the context of the information, and the capability to pronounce voter names as intended;
2. low background noise; and
3. recording or reproduction in dual-mono, with the same audio information in both ears.

Discussion

This requirement covers both recorded and synthetic speech. It applies to those aspects of the audio content that are inherent to the system or that are generated by default. To the extent that election officials determine the audio presentation, it is beyond the scope of this requirement.

Support for non-written languages and low literacy includes audio output that is usable by voters who can see the screen.

The International Telecommunications Union (ITU) provides a set of freely available test signals for testing audio quality in *Rec. ITU-T P.50 Appendix I*.

References: VVSG 2.0 (7.1-M), WCAG 2.0, Section 508, ITU-T (P.50 Appendix I)

2.2.6 – Audio control

The e-poll book must allow the election worker to control the audio format either through custom controls or using the platform or device controls, including:

1. Pausing and resuming the audio; and
2. repeating any information.

Discussion
These features can also be useful for users with cognitive disabilities.

References: VVSG 2.0 (7.2-G)

2.2.7 – Standard audio connectors

If audio output is supported by the system, the e-poll book hardware platform must provide its audio signal for the audio format interface through an industry standard connector using a 3.5 mm (1/8 inch) stereo headphone jack to allow voters and election workers to use their own audio assistive devices for private listening.

References: VVSG 2.0 (8.1-E)

Section 2.3 – Requirements for e-poll books supporting additional languages

2.3.1 – Languages

The e-poll book must be capable of displaying and printing all the information contained in the e-poll book and e-poll book instructions in all languages the manufacturer has declared the system supports, in visual formats, and in audio formats for e-pollbooks that support audio formats.

Discussion
Both written and unwritten languages are within the scope of this requirement.

The system will be tested in all languages that the manufacturer claims it is capable of supporting.

References: VVSG 2.0 (5.1-B), Voting Rights Act

2.3.2 – Presenting content in all languages

All information that is presented to the election worker and information presented to the voter in English must also be capable of being presented in all other languages that are supported, whether the language is in visual or audio format (for e-poll books that include audio). This includes instructions, warnings, and messages.

Discussion
It is not sufficient simply to present options in an alternative language. All of the supporting information election workers or voters need to complete their tasks is also covered in this requirement.

References: VVSG 2.0 (5.1-B), Voting Rights Act

2.3.3 – Language selections

It must be possible to select languages separately for the election worker screens and for screens or information presented to the voter.

1. Changing the language for the election worker must not cause any language changes in the e-poll book interface or attached devices that are viewed by voters.
2. Changing the language used for any voter-facing interface of the e-poll book or by attached devices must not cause any language changes to the interface used by election workers.

Discussion

It is possible for an election worker to use a translator or other assistance while helping a voter check-in. Additionally, a voter may understand an election worker's instructions but feel more comfortable with written instructions requiring a signature to be provided in their native language.

References: VVSG 2.0 (5.1-B), Voting Rights Act