Public Comments for EAC concerning the proposed VVSG 2.0 2023 Update

May 20, 2023

Dear Chair McCormick and Director Hovland,

We respectfully submit the comments attached below on the next iteration of the Voluntary Voting System Guidelines (VVSG 2.0 2023) for review and consideration.

We write as members of the State Audit Working Group (SAWG), an ad hoc group of individuals concerned about election integrity issues in general and election audits in particular. The SAWG has been meeting regularly via teleconferences since 2008, and has produced documents such as the *Principles and Best Practices for Post-Election Tabulation Audits*.

As the U. S. Election Assistance Commission (EAC) reviews these important guidelines, we wish to express our appreciation for the thoughtful and deliberate work that has gone into their development. The VVSG 2.0 represents a quantum leap in improved security, accessibility and auditability requirements for election technology. Yet they could be improved to enhance integrity and increase justified confidence in elections.

We also believe the VVSG can be further improved through the recommendations we detail in our attached document. We highlight these broad areas where the requirements should be updated or strengthened:

1. Component Testing

There should be testing by component (i.e., separate testing of BMDs, scanners and Election Management Systems) – first, in order to reduce the time and cost of initial certification and any updates and, second, in order to give jurisdictions more voting system options.

Component testing will allow new players to enter the market without having developed an entire voting system. For instance, new entrants may develop and offer only BMDs. Also, jurisdictions could use components from different vendors in their voting systems. VVSG requirements should be added to support component testing. For example, there should be a separate requirement for common data formats for ballot definition files.

2. Compliance and Tabulation Audits

Robust compliance and tabulation audits are key for election security and, therefore, are integral to VVSG 2.0. These audits rely on evidence provided by both hand-marked and BMD-printed paper ballots as a representation of voter intent. For instance, the requirements should:

- Improve the usability of paper ballots so that voters may easily check that their intent is correctly represented.
- Increase the percentage of voters who verify voter intent on BMD-printed paper ballots.

- Mandate the creation and retention of ballot images as well as their hashes or digital signatures.
- Test the voting systems for their support of efficient audits so that states can conduct robust audits without undue burden.
- Ensure that ballot sheets, rather than entire ballots, can be separately audited.

3. Protect from Electronic Attack

VVSG requirements should protect each voting system component from attack by forbidding the use of any hardware that provides capability for a wireless network or connection to external networks. Any electronic connectivity greatly increases the attack surface and creates the possibility of attack from anywhere in the world.

Ballot images must be protected by hashes and digital signatures.

4. Protect Against Insider Threats and Strengthen Voter Confidence

The VVSG requirements should strengthen protection against insider threats:

- In order to protect ballot secrecy, no indirect associations between the vote selections and voters should be allowed. The chance that votes can be associated with a voter creates too great a risk for our democracy. Preventing any link between the voters and their votes is key for reducing vote buying and selling and coercion. Voters fear that people, even officials, might know how they vote, and this fear detracts from voter confidence.
- Critical system actions should allow election officials to require two-person (bipartisan) access in addition to two-factor authentication.
- BMDs should no longer be allowed to resemble DREs by storing or exporting electronic records of voter intent.
- Voters' selections can be read from ballots prior to Election Day, but tabulation and aggregation should be delayed until the close of polls to reduce any possibility or pressure to leak results.

5. Recommendations for Improving the Clarity of the Document

The wording and form of the wording used in the document should be consistent with the wording in the glossary.,

- "Electronic Remote Ballot Marking" is not consistently used and defined.
- "Cast" is used incorrectly in some places and should conform to the glossary meaning. Feeding of ballots is usually a voting machine function often performed by officials,

while casting is an irrevocable act of a voter, for instance, by feeding the ballot to a machine or submitting an absentee ballot.

- "Ballot" is used incorrectly as implying a single sheet, a single ballot image or one CVR per voter. A ballot can consist of multiple ballot sheets.

Sincerely,

Note: All affiliations are for reference only and do not constitute an endorsement b

Luther G. Weeks
Moderator, State Audit Working Group
Computer Scientist and Executive Director, Connecticut Citizen Election Audit

Harvie Branscomb, Publisher, http://electionquality.com,
Coloradans For Voting Integrity

John L. McCarthy, retired computer scientist (Lawrence Berkeley
National Laboratory)

Paul Burke, http://VoteWell.net , retired from HUD

Celeste Landry, MS in Operations Research,
registered lobbyist on Colorado voting and election bills

Tim White, Election Watcher, WA state

Lynn Bernstein
Member, SAWG
Systems Integration & Test Engineer and Founder, Transparent Elections NC

Neal McBurnett
Computer Scientist and election auditor since 2004

Voluntary Voting System Guidelines VVSG 2.0

PROPOSED CHANGES BY SAWG (State Audit Working Group) submitted May of 2023.

Yellow highlight reflects suggested replacement or additional explanatory text intended to be added *Green italicized highlight* designates commentary to support our suggestions. ~~Grey highlight and strikethrough~~ indicates text to be deleted. **indicate most critical comments.

Note: Only portions of the original document with suggested changes or comments are included in this document.

Requirements for the Voluntary Voting System Guidelines 2.0

February 10, 2021

Prepared for the ***Election Assistance Commission***

At the direction of the

General Comments:

**Securing Records Without Jeopardizing Ballot Secrecy

There is a tension between safeguarding the digital records and preventing voters being tied to their votes, i.e., ballot secrecy. As mentioned in the discussion in 13.2.A, cryptographic hashes alone provide insufficient protection to stored election records. Whereas digital signatures may include information such as timestamps and public keys that could be combined with other information to associate voters with their votes.

This tension appears in these requirements:

13.2 in the summary
1.1.5-I – Ballot Image Hashes, Digital Signatures and Exports
9.1.2-B –Tamper-evident record creation
13.2 Source and Integrity of Election Records
13.1.2-A – Integrity protection for election records
13.2-A – Signing stored election records

The requirements in the revised VVSG should be specific enough to ensure that the digital records are secured without jeopardizing ballot secrecy.

**Ballot Sheets and Ballot Sides

The document should be consistent when using the terms "ballot", ballot sheet" and "ballot side". We have added definitions of "ballot sheet" and "ballot side" in the Glossary. For instance, an image is commonly associated with one ballot sheet (typically with both sides, even if the back is blank, but sometimes only one side is provided) and a CVR record typically references both sides of that sheet, but not the entire ballot if there are multiple sheets. Some older systems saved the sides of the sheets in separate files, but would link them by name. Multiple-sheet ballots are normally included as separate CVR records, one record per sheet. BMD ballots, when multiple sheets are used for hand-marked paper ballots, will include all sheets and sides in its ballot summary. The term "ballot" typically refers to the combination of all sheets. "Page" normally means one side of a sheet.

**Cast and Cast Ballot

In many places the Guidelines reference Cast or Cast Ballot when the act is feeding a ballot into a voting machine, however, there needs to be a distinction between a voter's act of casting a ballot and an official feeding a ballot into a voting machine.As defined in the Glossary,

cast

*(v) The final action a **voter** takes in selecting **contest options** and irrevocably confirming their intent to **vote** as selected.*

cast ballot

***Ballot** in which the **voter** has taken final action in selecting **contest options** and irrevocably confirmed their intent to **vote** as selected.*
Synonyms: voted ballot

Voters cast their absentee ballots when they irretrievably submit their ballots, yet some ballots may later be revoked by officials, in the case of absentee ballots not correctly cast. Often the feeding is done by an official which is a distinct act. This is always the case when votes are cast in a polling place and later centrally counted.

Introduction

How the VVSG is to be Used

Scope

The scope of the *VVSG 2.0* is limited to equipment acquired by states and certified by the EAC. The *VVSG 2.0* covers pre-voting, voting, and post-voting operations consistent with the definition of a ***voting system*** in the *Help America Vote Act (HAVA) Section 301 [HAVA02]*, which defines a voting system as the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment), that is used to define ballots; cast and count votes; report or display election results; and maintain and produce any audit trail information.

The ***voting system*** as defined in the *VVSG 2.0* is:

Equipment (including hardware, firmware, and software), materials, and documentation used to enact the following functions of an election:

1. *define elections and ballot styles,*
2. *configure voting equipment,*
3. *identify and validate voting equipment configurations,*
4. *perform logic and accuracy tests,*
5. *activate ballots for voters,*
6. *record votes cast by voters,*
7. *count votes,*

8. *label ballots needing special treatment,*
9. *generate reports,*
10. *export election data including election results,*
11. *archive election data, and*
12. *produce records in support of audits.*

As part of the voting system scope, *HAVA Section 301 [HAVA02]* mandates five additional functional requirements to assist voters. Although these requirements may be implemented in a different manner for different types of voting systems, all voting systems must provide these capabilities, which are reflected in the *VVSG 2.0* requirements:

1. Permit the voter to verify (in a private and independent manner) their choices before their ballot is cast and counted.
2. Provide the voter with the opportunity (in a private and independent manner) to change their choices or correct any error before their ballot is cast and counted.
3. Notify the voter if they have selected more than one candidate for a single office, inform the voter of the effect of casting multiple votes for a single office, and provide the voter an opportunity to correct their ballot before it is cast and counted.

Note: HAVA gives an exception to #3 for central count voting systems. This requirement is only applicable when the voter is submitting their own ballot in a polling place.

Note: VVSG requirement #3 requires modification for Approval Voting, Score Voting, etc., since voters often intend to make marks for several candidates for a race for a single office

4. Be accessible for individuals with disabilities in a manner that provides the same opportunity for access and participation (including privacy and independence) as for all voters.
5. Provide alternative language accessibility pursuant to *Section 203* of the *Voting Rights Act [VRA65]*.

Section 301(a)(3)(B) [HAVA02] also states that there should be "… at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place". However, the *Americans with Disabilities Act of 1990 [ADA10]* requires that voters with disabilities be provided with auxiliary aids that allow them to participate equally in the voting process without discrimination. This is consistent with *Section 301* of HAVA cited above that requires a voting system to be accessible for individuals in a manner that provides the same opportunity for access and participation (including privacy and independence). If a majority of voters utilize hand-marked paper ballots, a sufficient number of accessible voting stations (including alternative language ballot features) must be available in each polling place to ensure their consistent availability in case of malfunctions. A sufficient number of machine marked ballots must also be produced by those voting stations to ensure non-discrimination and ballot secrecy, particularly when the ballots produced by the accessible voting system differ in size, shape, and/or content from the hand-marked ballots and are thus readily identifiable. Procedures and training for poll workers on the operation of the accessible voting stations are also necessary to support this usage.

There is substantial experience[1] showing that having one accessible voting machine per polling place used only for voters with disabilities has worked poorly for voters with disabilities and may not be sufficient to provide equal access as required by law. For instance, data collected in recent elections highlight how difficult it is to ensure that a sufficient number of voters use the accessible voting machines to preserve the secrecy of machine-marked ballots and that poll workers are able to operate the machines successfully. To support best practices, states should consider legislation and additional resources to ensure balanced access to accessible voting machines wherever voting technology is deployed and used for elections.

The *VVSG 2.0* definition of a voting system does not expand the HAVA definition but focuses it on election processes. The *VVSG 2.0* principles, guidelines, and requirements apply to the election process functions and, by extension, to the voting devices that implement these functions.

The scope of most *VVSG 2.0* requirements apply to the entire voting system as opposed to specific devices, thus permitting the manufacturer more freedom to implement the requirements as they choose. However, when the scope of a requirement is limited to a specific function, that information is included in the text of the requirement, for clarity. For example:

- “A voting system’s electronic display must be capable of...”
- “Scanners and ballot marking devices must include…”
- “The cryptographic E2E protocol used in the voting system must…”

Implications for Networking and Remote Ballot Marking

Traditionally, ballots have been cast at polling places or through mail-in absentee ballots. There has been a growing trend to provide flexibility for voters to vote early and in-person at

[1] For more details, see:
a) “Disability, Voter Turnout, and Voting Difficulties in the 2012 Elections” (Rutgers) **https://smlr.rutgers.edu/sites/default/files/images/Disability%20and%20voting%20survey%20report%20for%202012%20elections.pdf**; **b)** “Experience of Voters with Disabilities in the 2012 Election Cycle” (National Council on Disability) **https://ncd.gov/rawmedia_repository/8%2028%20HAVA%20Formatted%20KJ%20V5%20508.pdf**; and
c) “The Blind Voter Experience: A Comparison of the 2008 and 2012 Elections” (National Federation of the Blind) **https://nfb.org/images/nfb/documents/word/2012_blind_voter_survey_report.docx**.

vote centers or at home using remote ballot marking applications. These innovative methods of voting provide additional paths to voting independently and privately for voters including those with disabilities. Likewise, advances in technology have led to efficiencies in election administration, including increasing the use of e-pollbooks for easy check-in and electronic election results reporting for timely aggregation of unofficial election results.

These additional election systems require network access to synchronize voter records, access remote ballot marking applications, and transmit unofficial election results. The measures taken to secure ~~securing~~ these systems falls outside the scope of *VVSG 2.0*. However, the benefits and risks associated with the use of these technologies were ~~was~~ carefully considered when developing the Guidelines, and ~~whereas~~ the associated ~~and~~ requirements were created and developed to ensure that the voting system is isolated from these additional election systems.

This section clarifies the boundary between the external election systems and the voting system as well as the use of wireless technologies within polling places or vote centers.

External Network Connections

VVSG 2.0 does not permit devices or components using external network connections to be part of the voting system. There are significant security concerns introduced when networked devices are then connected to the voting system. This connectivity provides an access path to the voting system through the Internet and thus an attack can be orchestrated from anywhere in the world (e.g., nation state attacks). The external network connection leaves the voting system vulnerable to attacks, regardless of whether the connection is only for a limited period or if it is continuously connected. These types of attacks include the following:

- The loss of confidentiality and integrity of the voting system and election data through malware injection or eavesdropping.
- The loss of availability to access data or perform election process (e.g., ransomware attack).

The *VVSG 2.0* requirements address the concerns of external network connections (see *14.2-E – External network restrictions* and *15.4-B – Secure network configuration documentation)*. Externally networked devices or components, such as those used for e-pollbooks or transmission of election results, must be physically **and electronically isolated from the voting system. This physical isolation can be described as an *air gap* between any systems that have an external network connection.

**Electronic Remote Ballot Marking

“Electronic Ballot Marker” is already mentioned under Ballot Marking Device in the Glossary.”Electronic Remote Ballot Marking” should be entered separately in the Glossary.

Electronic remote ballot marking is defined as an election system for voters to mark their ballots electronically outside of a voting center or polling place. These systems are to be used as a tool which enables ~~”no excuse”~~ absentee voting. This allows a voter to receive a blank ballot to mark electronically, print, and then cast by returning the printed ballot to an election office. A voter may electronically fill out their ballot with a state-provided web application. Electronic remote ballot marking applications provide another path to voting independently and privately for voters including those with disabilities but they involve significant ballot secrecy risks as well as integrity and operational challenges.
The *VVSG 2.0* requirements apply to devices used to mark ballots inside a polling place or vote center. They do not apply to remote ballot marking devices and applications. The *VVSG 2.0* requirements affect only those voting system devices that constitute a voting system and that are submitted for testing and certification. For remote ballot marking, the voter uses a web application, their own personal device, and an external network (i.e., the Internet).

It should be noted that remote ballot marking applications need to comply with accessibility laws such as the *Americans with Disabilities Act of 1990 [ADA10]*. *VVSG 2.0* requirements that address the accessibility and usability for the electronic interface of a remote ballot marking software application can serve as an informative resource for developers of these systems.   For example, *8.2-A — Federal standards for accessibility*, identifies the WCAG Level AA checkpoints in the *Section 508 [USAB18] – Standards* as a requirement for voting system electronic interfaces.

Major changes from VVSG 1.1 to VVSG 2.0

Principle 11 - Access Control

- Prevents the ability to disable logging
- Bases access control on voting stage (pre-voting, activated, suspended, post-voting)
- Does ~~not~~ require role-based access control (RBAC)

Clearly this is an error since the document does require role-based access control, as it should.

- Requires multi-factor authentication for critical operations:
  - Software updates to the certified voting system
  - Aggregating and tabulating
  - Enabling network functions
  - Changing device states, including opening and closing the polls

- Deleting the audit trail
- Modifying authentication mechanisms

Conformance Information

Implementation Statement

A voting system conforms to the VVSG Principles and Guidelines if all stated requirements that apply to that voting system and all of its devices are fulfilled. The implementation statement documents the requirements that have been implemented by the voting system, the optional features and capabilities supported by the voting system, and any extensions (that is, additional functionality) that it implements.

The implementation statement may take the form of a checklist to be completed for each voting system submitted for conformity assessment. It is used by test labs to identify the conformity assessment activities that are applicable.

The implementation statement must include:

- Full product identification of the voting system, including version number or timestamp
- Separate identification of each device that is part of the voting system
- Device capacities and limits
- List of languages supported
- List of accessibility capabilities
- List of voting variations supported

”Vote Variation” instead of “Voting Variations” is defined in the Glossary. The wording should be consistent in all instances in the document.

- Devices that support the core functions and how they do it
- List of requirements implemented
- Any extensions also included in the voting system
- Signed document that the information provided accurately characterizes the system submitted for testing

The VVSG 2.0 - Principles and Guidelines

The *VVSG 2.0* consists of 15 principles and 53 guidelines. Together these principles and guidelines cover voting system design, development, and operations.

Principle 8: ROBUST, SAFE, USABLE, AND ACCESSIBLE

The voting system and voting processes provide a robust, safe, usable, and accessible experience.

8.1 - The voting system's hardware, software, and accessories are robust and do not expose users to harmful conditions.

8.2 - The voting system meets currently accepted federal standards for accessibility.

8.3 - The voting system is evaluated for usability with a wide range of representative voters, including those with and without disabilities.

8.4 - The voting system is evaluated for usability for the role of ~~with~~ election workers.

Principle 13: DATA PROTECTION

The voting system protects data from unauthorized access, modification, or deletion.

13.1 –The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, ~~or~~ audit records, or data associated with extended features.

13.2 - The source and integrity of electronic tabulation reports are verifiable.

13.3 - All cryptographic algorithms are public, well-vetted, and standardized.

13.4 - The voting system protects the integrity, authenticity, and confidentiality of sensitive data transmitted over all networks.

Principle 1
High Quality Design

Principle 1 HIGH QUALITY DESIGN

The voting system is designed to accurately, completely, and robustly carry out election processes.

The requirements for *Principle 1* and its guidelines include functional requirements for election definition and preparation through all voting processes concluding with closing of the polls, tabulating, and reporting. The requirements deal with how voting systems are designed to operate during election processes, including limits for stress and volume. Other principles provide more detailed requirements in other areas including accessibility, security, and usability.

The requirements for ***Guideline 1.1*** are arranged into sections by election process with requirements containing the basic core requirements for conducting an election:

1 – Election definition which deals with the capabilities of the voting system to define an election, that is, manage items such as election districts, contests, candidates, and to define ballots for the election that may be specific to various combinations or splits of precincts. Support for the specifications described in the Election Results Common Data Format Specification *(NIST SP 1500-100) [NIST16]* is required for imports and exports.

2 – Pre-election testing which deals with capabilities of the voting system to configure and verify correctness of devices before opening the polls. Logic and accuracy (L&A) testing is covered here, as well as new requirements to check that cast vote records (CVR) and extended features are created properly and that any encoded data such as barcodes is accurately recorded.

3 - Opening the polls which deals with capabilities of the voting system to ensure that the voting system is properly configured so that polls can be opened.

4 - Casting which deals with the capabilities of the voting system to enable a voter to activate and cast a ballot. If ballot activation occurs on an electronic pollbook, one cannot test and verify whether these requirements are satisfied unless the entire pollbook is also tested. Additionally, the requirements deal with capabilities needed for common vote variations, ballot measures, and write-ins.

5 - Recording voter choices which deals with casting ballots and how equipment will handle ballots as they are cast, including the processes involved in recording votes in cast vote records. This mandates recording the selected contest options, and other information needed for linking the CVR with the device that is creating the CVRs and for auditing.

6 – Ballot handling for vote-capture devices which deals with functions that scanners will provide, including separating ballots for various reasons, for example, because of write-ins on manually-marked paper ballots and handling mis-fed ballots. It deals with the behavior of batch-fed scanners and voter-facing scanners when scanning ballots that need manual handling or inspection, such as for write-ins or unreadable ballots.

7 – Exiting or suspending voting which deals with exiting the voting mode (closing the polls), that is, stopping voting and preventing further voting. This applies to those systems located at a remote location such as the polling place or vote centers.

8 – Tabulation which deals with how tabulation processes will handle voting variations, including those methods used most commonly across the United States.

9 - Reporting results which deals with the need for the voting system to have the capability of creating all required precinct post-election reports. This includes recording ballots such as absentee ballots and Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) ballots.

1.1.2 – Pre-election testing

1.1.2-F – Testing codes and image creation

The voting system must include the capability to verify that encoded versions or images of voter selections on a ballot and any other encoded information on a ballot are created correctly by permitting election officials to compare the encodings and images with the test ballots.

Discussion

The purpose of this requirement is to give election officials the capability, prior to opening the polls, to audit encoded versions of voter selections. This process may include the review of created ballots and encoded information on each ballot to ensure that the images correctly match the ballot, thus validating accuracy in ballot creation. and that the ballot was created accurately. will include such as provided by a ballot marking device (BMD) using QR codes and gain assurance that the QR codes and any encoded data represented by the QR codes contains the voter's selections exactly as made. Likewise, to audit any image of the ballot made by a scanner to gain assurance that the image correctly matches the ballot. And, to audit any encoded information on the ballot to gain assurance it is being created correctly.

Check for sentence fragments above.

Related requirement: 1.1.2-C – Use of test ballots

1.1.5 – Recording voter choices

1.1.5-A – Reading ~~Casting~~ and recording

The voting system must support reading ~~casting~~ a ballot, recording each vote precisely as indicated by the voter subject to the rules of the election jurisdiction, and creating and retaining ballot images and ~~a~~ cast vote records that can be tabulated and audited.

In VVSG 2.0 ballot images do not seem to be a requirement for the functionality of voting systems. They seem to be treated as an extension. If ballot images are included as required functionality, then they need to be included in many parts of the VVSG including testing for precision and accuracy, pre-election testing/equipment set-up, recording voter choices, and data protection.

This section includes an example of the issues in the misuse of the words "cast" and "ballot" that occur in several places in the guidelines. "Cast" refers to the final act of physically or electronically submitting the ballot, not "reading" which is the actual intent of this section. For each side of a ballot sheet, a separable ballot image is created. For each ballot sheet, a separate cast vote record is created. We have suggested what might be a correct way of stating the requirement.

1.1.5-G – Record audit information

The voting system must be capable of recording audit-related information in the CVR or collection of CVRs as they are created, that includes:

It is very problematic for a CVR to tie too much information to voter marks. The explicit requirement should be limited to supporting efficient auditing by being able to associate a CVR with a paper ballot. All the rest should be eliminated. Any information included in the CVR must not jeopardize ballot secrecy. Having the voting machine location and serial number could help tie the corresponding ballot image to a voter.

1. ~~identification of the specific creating device such as a serial number;~~

2. ~~identification of the geographical location of the device;~~

3. identification of the ballot style corresponding to the CVR;

***A single ballot can consist of multiple styles and multiple sheets. This will affect anonymity because it might prevent more than one ballot style from being assigned to a ballot- thus preventing or making difficult the separation of ballot content into* *independently tabulated styles. However, if it is made clear that multiple CVRs and multiple styles can be associated with a voter, this problem would be eliminated.*

4. identification of the corresponding voted ballot (or ballot sheet if multiple sheets exist);

5. for multi-sheet ballots, identification of the individual sheet corresponding to the CVR, along with the identification of the ballot style;

6. identification of the batch containing the corresponding voted ballot, when applicable; and

7. sequence of the corresponding voted ballot in the batch, when applicable.

Discussion

~~Item 2 can be any identification scheme that is preferential in the jurisdiction, e.g., polling place name, address, geographical coordinates, etc.~~

Item 4 can be satisfied by printing a unique ID on ~~the~~ each ballot sheet as it is scanned and including that ID in the corresponding CVR.

Item 5 ensures that every sheet of a multi-sheet ballot contains the sheet number as well as a ~~the~~ ballot style or ballot sheet style ID. This way, a ballot style ID could be defined to include all sheets, or each sheet could be defined with a unique ballot style.

Items 6 and 7 are necessary when ballot batching is in effect.

1.1.5-H – Store and link corresponding image

The voting system must ~~be capable of storing~~ store an image of a side or a sheet of a paper ballot and link~~ing~~ this image to the specific associated CVR.

Discussion

The image could be linked to the CVR by, for example, creating a filename for the image that is the same as the identifier from item 4 in Requirement *1.1.5-G – Record audit information*.

Federal regulation requires that electronic records created must be retained for 22 months.

**1.1.5-I -- Ballot Image Hashes, Digital Signatures and Exports

The core bit image of each separable unit of the ballot should be hashed to help ensure that any alteration of the image thereafter will be detectable, and the images, when presented in other forms, such as PDF or PNG, can be compared bit-by-bit with the originally scanned image, which was digitally signed by the device.

Scanners must provide a means to export the ballot images as separable sheets if not as sides of sheets. Separately, a file containing hashes is created for which a digital signature is also created,

Tying individual auditable entities to unnecessarily detailed information like the device which generated them can make it impossible to publish the information, and imperil the even more important requirement for transparency of the data. Without transparency, audits are just more unverifiable claims from election officials.

This should require hashes of all these individual entities (images etc), and then require signatures of collections of those hashes in batches which are designed to be safe to release to the public.

1.1.8 – Tabulation

1.1.8-A – Tabulation

The voting system must support the tabulation function for all voting variations indicated in the ~~implantation~~ implementation statement. This function includes:

1. extracting the valid votes from each ballot cast according to the defined rules;

2. creating and storing a CVR that contains the disposition of each contest selection as well as the disposition of each contest choice that is eligible to be cast; and

3. accumulation and aggregation of contest results and ballot statistics~~.~~; and

4. delay of aggregation and reporting of any total or partial contest results until close of polls on Election Day.

   ***Scanners shall be able to create ballot images. Steps 1, 2 & 3 may be done in the scanner or Election Management System, and may be delayed until Election Day. Step 4, performing aggregation, shall be delayed until Election Day. That way the votes may be captured and stored early in the process to protect the chain of custody, but the results cannot be easily leaked.*

   While precinct scanners do tabulation and produce poll tapes, they shouldn't be permitted to be used in that way during early voting.

Discussion

Results accumulation and aggregation takes place at multiple levels within the voting system. Each tabulation unit must perform this function and must have the ability to transmit the CVRs and results to the election management system (EMS) for jurisdiction wide accumulation and aggregation.

Interoperability: Dumb scanners are widely available and let interpretation be done in the voting system outside of the scanner. This lets different vendors use the images from dumb scanners.

Principle 2 High Quality Implementation

Principle 2 High Quality Implementation

2.5.1-D – Prevent tampering with data

All voting devices must prevent access to or manipulation of configuration data, vote data, ballot images and ~~or~~ audit records (for example, by physically tampering with the medium or mechanism containing the data, by other programs on the system, or by faulty code) except where this access is necessary to conduct or verify integrity of the voting process. Also, voting systems must not have "back doors" such as unused ports where an attacker might insert a drive and take over the voting system.

Discussion

This requirement can be satisfied through a combination of:

- the memory protection implemented by most popular COTS operating systems,
- error checking, and
- access and integrity controls.

Systems using mechanical counters to store vote data need to protect the counters from tampering. If vote data are stored on paper, the paper needs to be protected from tampering. Modification of audit records after they are created is never necessary.

Principle 3
Transparent

Principle 3 TRANSPARENT

The voting system and voting processes are designed to provide transparency.

Guideline 3.1 contains requirements for the documentation that manufacturers supply to jurisdictions that use their systems. In this context, "user" refers to election officials, and "system" refers to a voting system or individual voting device. The user documentation is also included in the technical date package (TDP) given to test labs. The sections in *3.1* cover

1 - System overview documentation covers documentation that explains the physical and logical structure of the system, its components, how it is structured, details about the software, and so forth.

2 - System performance documentation gives details on how the system performs in normal operation as well as its constraints and limits.

3 - System security documentation describes the features of the system that provide or contribute to its security and includes how to operate the system securely. Physical security instructions to protect evidence for both compliance and tabulation audits are included in this documentation.

4 - Software installation documentation describes in exact detail what software is installed, how it is installed, and how it is to be maintained.

5 - System operations documentation deals with operating and using the equipment to conduct elections, including setup, testing, voting operations, reporting, and so forth.

6 - System maintenance documentation deals with proper maintenance of the voting equipment and how to correct various issues or problems.

7 - Training material documentation lists what the manufacturer needs to cover about the personnel resources and training required for a jurisdiction to operate and maintain the system.

It is not the intent of these requirements to prescribe an outline for user documentation. Manufacturers are encouraged to innovate in the quality and clarity of their user documentation.

In 3.2, Setup inspection documentation explains how to verify that the system is properly setup and configured, and how to monitor its operations.

In 3.3, Public documentation requirements cover details of how a manufacturer codes the election event log, implements a CDF, builds barcodes, and supports ~~implements~~ audits.

Manufacturers do not implement audits. They provide systems that provide the data to support audits.

3.1 – The documentation describing the voting system design, operation, accessibility features, security measures, and other aspects of the voting system can be read and understood.

3.1.1 – System overview documentation

3.1.1-C – System description

System overview documentation must include written descriptions and diagrams that present the following, as applicable:

1. a description of the functional components (or subsystems) as defined by the manufacturer (for example, environment, election management and control, vote recording, vote conversion, reporting, and their logical relationships);
2. a description of the operational environment of the system that provides an overview of the hardware, firmware, software, and communications structure;
3. a concept of operations that explains each system function and how the function is achieved in the design;
4. descriptions of the functional and physical interfaces between components;

5. identification of all COTS products (both hardware and software) included in the system or used as part of the system's operation, identifying the name, manufacturer, and version used for each such component;

6. communications (dial-up, network) software;

7. interfaces among internal components and interfaces with external systems;

8. for components that interface with other components for which multiple products may be used, file specifications, data objects, or other means used for information exchange including the public standard used for such file specifications, data objects, or other means; and

9. benchmark directory listings for all software, firmware, and associated documentation included in the manufacturer's release in the order in which each piece of software or firmware would normally be installed upon system setup and installation.

10. specifications of the performance and limitations in capacity of the voting system or device,e.g. number of contests, number of contest options per screen, limitations on transition between contests/options/screens etc.

These limitations have caused significant issues in some states. For instance the number of candidates that can be listed on each screen of a BMD should be clear so that all candidates are treated equally.

Discussion

The diagrams could be engineering renderings or photographs.

3.1.2-B – Maximum read and tabulation rates

System performance documentation must include the maximum read and tabulation rates for a ~~bulkfed~~ scanner. This documentation must include the maximum read and tabulation rates for individual components that impact the overall maximum tabulation rate.

Discussion

The capacity to convert the marks on individual ballots into signals is uniquely important to central count systems. Scanner processing time must be quoted for a variety of election setup conditions (# contests, # contest options, # sheets, size and layout of sheet, etc.)

3.1.2-D – Processing capabilities

System performance documentation must include a listing of the system's functional processing capabilities, encompassing capabilities required by the VVSG, and any additional capabilities provided by the system, with a description of each capability. Therefore, this documentation must include the following attributes:

1. an explanation regarding the capabilities of the system that were declared in the implementation statement;

2. additional capabilities (extensions) must be clearly indicated;

3. required capabilities that may be bypassed or deactivated during installation or operation by the user must be clearly indicated;

4. additional capabilities that function only when activated during installation or operation by the user must be clearly indicated; and

5. additional capabilities that normally are active but may be bypassed or deactivated during installation or operation by the user must be clearly indicated.

6. After configuration, the system must provide documentation of the current status of any optionally activated capabilities and the parameters associated with them.

For example, one vendor's configuration parameter that is set by hand during election definition and that deserves to be reported back upon request is the range in target pixel density that triggers human adjudication of voter intent on scanned HMPB. The upper and lower bounds of this range are entered at setup time but in some cases are difficult to discover thereafter.

3.1.3 – System security documentation

3.1.3-D – Audit procedures

The system security document must include an explanation of how to conduct compliance and tabulation audit procedures to determine whether tabulation is accurate. The explanation should include details such as information about how to locate specific paper ballot sheets from a CVR entry and vice versa, how to export ballot images and CVRs, how to locate and redact rare styles or to redact contests that produce rare styles in coordinated elections.

For information about means to achieve anonymity of CVRs please refer to this article: https://www.sos.state.co.us/pubs/elections/VotingSystems/riskAuditFiles/2018/20180309PreservingAnonymityOfCVR.pdf

3.1.7 – Training documentation

3.1.7-D – Training requirements

The manufacturer must specify requirements for the orientation and training of administrators, central election officials, election judges, ~~and~~ election workers, equipment maintenance personnel, contractors, and any other individuals who need to interact with the election equipment and/or software.

3.2 – The processes and transactions, both physical and digital, associated with the voting system are readily available for inspection.

3.2-R – Accessible election evidence

The manufacturer's design must facilitate physical and digital access to all election data including records containing voter intent such as paper ballot sheets, cast vote records, and any ballot images.

Discussion

The goal should be to ensure constructive sharing and publication of election evidence to support various forms of public verification of the election process. Not all jurisdictions will have the same policies for access but the voting device must support the most transparent of the policies of local officials.

Some possible areas of concern include:

Records are free of unnecessary links to any voter so that ballot secrecy is maintained,

Sometimes voters can be identified if they are voting in a very small contest and/or jurisdiction. The ballots or sheets should be able to be organized so that such information is consolidated into locations such that redaction is inexpensive and quick, and rarely needed.

Ballot images may be in convenient storage formats, such as PDF, PNG, and TIF, and other standards.

Formats for export are convenient and efficient, and data is well indexed, filterable and sortable. For example, election records are not exported in formats that defy digital or human recognition (e.g., image pdf from which digital text can only be obtained via OCR).

More suggestions about voting system exports to support accessible election evidence are found here: http://electionquality.com/ballot-anonymity-strategies/

3.3 – The public can understand and verify the operations of the voting system throughout the entirety of the election.

3.3-C – Bar and other codes

Manufacturers must provide publicly available documentation that fully specifies the barcode, how barcoded data is formatted, and any other encoding standards or methods used on ballots or audit material and allows them to be decoded with COTS devices. (See 4.2-A Standard Formats.)

Discussion

The voting system documentation needs to include the name and version of the standard used for barcodes or for any other codes that encode information that the public sees on ballots or other material that can be used in audits or verification of the election. The documentation also needs to include how the data may be packed or compressed within the encoding. The report should be sufficient for a voter to understand the barcoded contents and for an auditor to ~~develop applications that~~ examine and fully understand the barcoded contents with minimal need for application development.

Principle 4
Interoperable

Principle 4 INTEROPERABLE

The voting system is designed to support interoperability in its interfaces to external systems, its interfaces to internal components, its data, and its peripherals. The voting system and individual voting system components (e.g., EMS, Scanners, BMD) are designed so that individual voting system components can be separately tested and certified. Testing components does not preclude integration testing for entire voting systems.

****The new version of the VVSG should include all requirements necessary to test and certify individual voting system components (EMS, Scanners, BMD …)*

4.1 – Voting system data that is imported, exported, or otherwise reported, is in an interoperable format.

4.1-A – Election programming data input and output

The voting system must include support for CDF specification(s)

regarding:

1. import and export of election programming data, and
2. import and export of ballot programming data.
3. **The ballot definition files must be in a common data format.

Having the election programming data in a common data format is necessary but not sufficient for having true interoperability and testing by component. The ballot definitions themselves must be in a common data format.

Discussion

This requirement concerns import and export of pre-election data into an election definition device, such as for identification of political geography, contest, candidate, ballot data, and other preelection information used to setup an election and produce ballots. This also includes reports of preelection data from the election definition device that can be used to verify the election programming setup. More information can be found in *SP 1500-100 Election Results Common Data Format Specification [NIST16].*

Principle 5
Equivalent and Consistent Voter Access

Principle 6 Voter Privacy

Principle 7
Marked, Verified, and Cast as Intended

7.1-G – Text size (electronic display)

A voting system's electronic display must be capable of showing all information in a range of text sizes that voters can select from, with a default text size at least 4.8 mm (based on the height of the uppercase I), allowing voters to both increase and decrease the text size.

Readability depends as much on space between lines as on height of letters. Standard for distance from bottom of one line to bottom of next line would be more useful than height of I.

The voting system 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 ballot 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 text size requirements have been updated from the *VVSG 1.1 [VVSG2015]* requirement to better meet the needs of voters who need larger text, including older voters, voters with low literacy, and voters with some cognitive disabilities.

This requirement also fills a gap in the text sizes required in *VVSG 1.1* which omitted text sizes needed or preferred by many voters. Although larger font sizes assist most voters with low vision, certain visual disabilities such as tunnel vision require smaller text.

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, candidate names or voting options 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.

The default text size of 4.8 mm is based on *WCAG 2.0 [W3C10]* and *Section 508 [USAB18].*

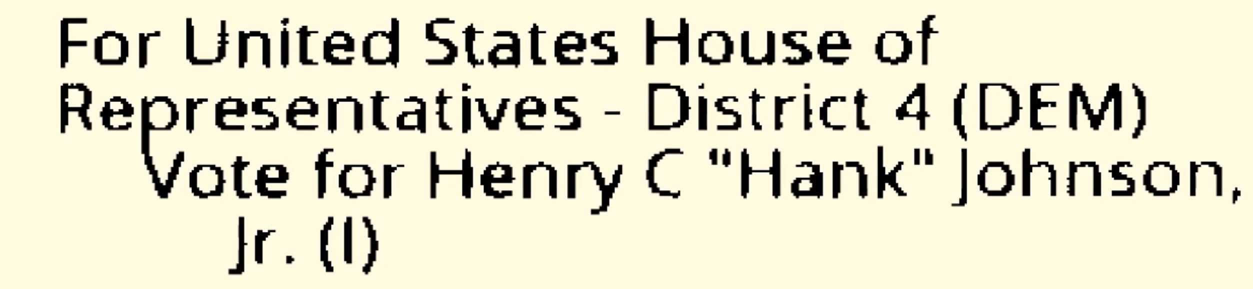
Applies to:	Electronic interfaces
Related requirements:	5.2-A – No bias 5.2-F – Preserving votes 7.2-D – Scrolling 7.3-B – No split contests

7.1-I – Text size (paper)

The voting system must be capable of printing paper ballots, both ballots for hand marking and BMD-printed ballots, that are easily understandable by the voter. Hand marked paper ballots, BMD-printed ballots and other paper records should have ~~with~~ a font size of at least 3.5 mm (10 points). Font and layout on paper should support potential use of optical character recognition on ballot images for use as a means of verification, tabulation, or supplemental audit review.

The VVSG document seems to put much more focus on the usability and readability of the electronic interface than the usability of a hand-marked paper ballot or BMD-printed ballot that the voter is supposed to check.

Current standards allow the following BMD-printed ballots with no interline distance, so, in the example below, the descender of p is continuous with capital V (DeKalb 2022 primary, Dominion).



For United States House of
Representatives - District 4 (DEM)
Vote for Henry C "Hank" Johnson,
Jr. (I)

There must be usability testing to see if BMD-printed ballots are printed in such a way to facilitate voters noticing differences between the ballot and their intentions.

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

If typography changes such as text size or display style are used to differentiate languages on a multilingual ballot, the requirements in *5.2-A – No bias* (and relevant state election law for ballot design) still apply.

Applies to:	Printed Material
Related requirements:	5.1-E – Reading paper ballots 7.1-G – Text size (electronic display)

7.1-J – Sans-serif font

The voting system must be capable of presenting text intended for the voter in a sans-serif font.

Discussion

This requirement ensures that systems are capable of best practice while allowing them to also meet local or state laws or regulations that might differ.

In general, sans-serif fonts are easier to read on-screen, look reasonably good when their size is reduced, and tend to retain their visual appeal across different platforms. Examples of sans-serif fonts with good readability characteristics include Arial, Calibri, Microsoft Tai Le, Helvetica, Univers, Clearview ADA, Atkinson Hyperlegible or Open Sans.

WCAG 2.0 [W3C10] and *Section 508 [USAB18]* require that at least one mode of characters displayed on the screen be a sans-serif font.

Atkinson Hyperlegible was developed in 2019, so EAC may not be aware of this font. https://brailleinstitute.org/freefont

7.3-I – Undervotes

The voting system must notify voters in both visual and audio formats of the specific contest in which they select fewer than the allowable number of options (that is, for undervotes).

1. Both electronic interfaces and scanners must allow the voter to submit an undervoted ballot without correction.

2. The voting system may allow election officials to disable the notification of undervotes on a scanner.

Discussion

For electronic interfaces, this notification can be incorporated into the review feature.

This requirement supports *HAVA [HAVA02]*.

Applies to:	Electronic interfaces and scanners
Related requirements:	7.2-C – Voter control 7.3-K – Warnings, alerts, and instructions

7.3-II - Voter verification of BMD-printed ballots

A voting system with an electronic interface must inform the voter that the paper ballot is the official record of their vote and that the voter should check the BMD-printed ballot before casting it.

The voting system must be evaluated for usability by voters both in terms of the rate at which voters thoroughly review their ballots and in terms of how successful voters are in discovering any discrepancies between the ballot and their intended selections.

Studies have shown that few voters actually verify their BMD-printed ballot.

[Insertion of this section requires renumbering.]

Principle 8
Robust, Safe, Usable, and Accessible

Principle 9
Auditable

Principle 9 AUDITABLE

The voting system is auditable and enables evidence-based elections.

The requirements for *Principle 9* include ensuring that an error in the voting system cannot cause an undetectable change in the election results, that the system produces records that are resilient and can be checked and produces records that enable an efficient compliance audit. Delivery, return, and non-voting equipment process used for vote-by-mail fall out of the scope of the VVSG and is often based on jurisdictional procedure.

The sections in *Guideline 9.1* cover:

1 - Software independence requires that the voting system provide proof that the ballots have been recorded correctly and are compliant within the Paper-based System Architecture or Cryptographic E2E System Architectures. In addition, the manufacturer documents the mechanism used to provide software independence. These requirements ensure that failures in voting system software can be detected and rectified

2 – Tamper-evidence requires the records used to record ballet selections cannot be undetectably altered. These records are needed to enable detection of incorrect election outcomes. They need to capture the voter's ballot selection when each ballot is cast.

3 – Voter verification requires that voting machines allow voters the opportunity to verify that the system correctly interpreted their ballot selections, identify errors with their selections, and restart a voting session if a ballot is unacceptable. Records that protect against software failures only work if voters can verify their selections are correct.

4 – Auditable means the voting system generates records that enable external auditors to verify that ballots are correctly tabulated, even if the system is compromised or there are faults in components. The manufacturer is to provide a procedure to verify that cast records are correctly tabulated.

5 – Paper records covers the requirements that paper-based (not cryptographic end-to-end verifiable) voting systems produce a verifiable paper record of the voter's ballot selection and retain a copy of that selection which has a unique identifier. The voter needs to be able to understand the recorded ballot selection and it needs to agree with the selections made by the voter.

6 - Cryptographic E2E verifiable deals with cryptographic protocols used in cryptographic E2E verifiable (not paper-based) voting systems, requiring that they be publicly available for review for 2 years before being used in a voting system. Individuals who vote on a cryptographic E2E verifiable system will get a receipt and be able to confirm that the system correctly interpreted their ballot selections. Voters will also be able to verify that their ballots are included in the tabulation results.

In 9.2 – Audit support requires that manufacturers identify the types of audits supported by a voting system, ensuring the system can handle audits held by election officials. The manufactures are also required to include any artifacts that the voting system produces to support the identified audits.

In 9.3 - Resilient records requires the data protection requirements under *Principle 13: Data Protection* are followed to ensure that voting system records are resilient in the presence of both intentional forms of tampering and accidental errors.

In 9.4 - Efficient audits covers requirements that ensure the system that will produce the records that allow election officials to conduct compliance and tabulation audits including risk-limiting audits. Risk-limiting audits can detect the accuracy of a vote count within this specified margin of error.

9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

9.1.2 – Tamper evidence

9.1.2-B – Tamper-evident record creation

Paper records or other tamper-evident electronic records of the voter's ballot selections must be captured when each ballot is cast. Any ballot images from a scanner of hand-marked paper ballots or BMD-printed ballots must secure the images as soon as possible using hash values and trusted cryptographic signatures of groups of hash values to allow for detection of any future changes of those images and enable audits of the chain of custody of the paper ballots. The voting system must be able to show any selected ballot images from a batch, for checking immediately after scanning a batch.

Cryptographic signatures of images may be time stamped if that will not reveal the time or order of voting. It's important to enable quality control audits of image accuracy immediately after images are created and hashed, by selecting a random sample and comparing images to paper ballots.

Discussion

Voter-facing scanners and other vote-capture devices produce the paper records or other tamper evident electronic records. These records can be useful artifacts for post-election audits.

Applies to: Voter-facing scanners and electronic ballot markers

9.1.3 – Voter verification

9.1.3-A – Records for voter verification

The voting system must provide individual voters the opportunity to verify that the ballot, whether a hand-marked paper ballot or a BMD-printed ballot, reflects their selections before casting it.~~ that the voting system correctly interpreted their ballot selections.~~

It is the ballot that the voter must be able to verify, not how the voting system interpreted that ballot. Generally, scanners do not allow the voter to verify how the ballot was interpreted. Showing the voter the interpretation would be a huge change and could affect privacy and throughput.

Discussion

- ~~Voter-facing scanners and other vote-capture devices can be used to meet this requirement.~~ An electronic ballot marker can print a voter's ballot selections to review before casting. An E2E verifiable system can print a receipt that allows a voter to verify their selections are tabulated and captured correctly. *Principle 7: Marked, Verified, and Cast as Intended* includes more requirements for voter verification.

Applies to:	Voter-facing scanners and electronic ballot markers
Related requirements:	7.3-G – Full ballot selections review

9.1.5 – Paper records

9.1.5-C – Paper record intelligibility

The recorded ballot selections must be presented in a human-readable format that is understandable by the voter.

The voting system must be evaluated for usability by voters both in terms of the rate at which voters thoroughly review their ballots and in terms of how successful they are in discovering any discrepancies between the ballot and their intended selections.

Discussion

The requirement ensures that a human-readable version of the data is also printed whenever a barcode is used to encode ballot selections.

The intelligibility of the paper record affects both the rate at which voters review their ballots and the rate at which voters discover any discrepancies between the ballot and their intended selections.

See suggested 7.3-II. A voting system with an electronic interface must inform the voter that the paper hand-marked or BMD-printed ballot is the official record of their vote and that the voter should check the ballot before casting it.

Applies to:	Paper-based system architectures

9.1.5-G – Preserving software independence

After a voter verifies their selections on a voted ballot and submits the ballot for casting, a paper-based voting system must not be capable of making an undetectable change to the paper record.

Discussion

After a voter verifies and submits their ballot, a voting system may print on paper ballot to apply a unique identifier that is later used for auditing purposes. To preserve software independence the voting system should not be able to print over or within the ballot selection area because that would cause an undetectable change to the election outcome. Instead the voting system should only be physically able to print outside of the bounds of the ballot selection area and may also create further distinction by printing in a different font style or color.

This printing process should be preserved regardless of software or hardware updates.

Black and blue are the most common colors used by voters. If machines use other colors, it will usually be possible to distinguish between voter & machine marks on original paper ballots, even when machines malfunction and drip ink unexpectedly.

Related requirements: 9.1.1-A – Software independent

9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

9.3-B – Chain-of-custody support for a voting system

Images (and any associated hashes and digital signatures) are available to help protect the chain of custody of the paper ballots and of the images themselves.

9.4 - The voting system supports efficient audits.

9.4-A – Risk-limiting audit

A paper-based voting system must produce paper records that allow election officials to conduct a risk-limiting audit.

Discussion

Voting systems contain information which enables election officials to conduct risk-limiting audits. For example, batch subtotal reporting by the voting system, may make the process of ballot sampling more efficient.

An evidence-based election requires convenient access to ballot sheets, ballot sheet images, ~~and~~ cast vote records, and hashes or digital signatures of images and CVRs for efficient and trustworthy public tabulation audits. Vendors should demonstrate how an election system provides all the information necessary for an independent Risk-Limiting Audit (RLA) (both single ballot-level comparison audits and batch comparison audits).

Some example features/paper records that may be produced to support risk-limiting audits include the following:

- the ability to associate electronic cast vote records (CVRs) with corresponding paper records while also preserving ballot secrecy;

- the ability to export of CVRs in an open and interoperable format;
- the ability to create a ballot manifest that allows users to identify the physical location of ballots (e.g., scanner name or number, batch number, and ballot sequence number); and
- supporting multi-sheet ballots, including association of each sheet with its corresponding CVR.

9.4-B – Random numbers supporting audit processes

Voting systems that generate or rely on random or pseudo-random numbers for auditing purposes must document the method used to obtain the numbers, how the sequence of random numbers cannot be associated with the order in which ballot sheets were read, and how the random numbers are used within the voting system.

Discussion

Various systems used to implement software independence require random numbers, whether for ballot selection for audits.

This documentation should specify:

- how random numbers are generated, and
- what any random numbers are used for.

One common use for random numbers is to create unique identifiers associated with ballots to assist in supporting audits.

The method for generating the pseudo-random numbers should meet the requirement *10.2.2-E Randomly generated identifiers.*

For additional information, see *NIST SP 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators [NIST15a].*

Related requirements: 9.4-C – Unique ballot identifiers
10.2.2-E – Randomly generated identifiers

9.4-C – Unique ballot identifiers

The voting system must enable election auditors to easily and uniquely address individual ballot~~s~~ sheets using a unique identifier. Such ballot identifiers must not allow the voter to be matched up to the ballot, ballot image, or cast vote record.

Discussion

This capability is needed to support ballot comparison RLAs. Although the voting system has this capability, this does not require jurisdictions to use this feature if it conflicts with state laws. In order to conduct a ballot comparison risk-limiting audit, paper ballot records must either be stored in the order in which they were scanned or contain a unique ballot identifier. A unique ballot identifier is a unique ID that provides information about the device it was scanned on and the batch in which it is stored. One example of a unique ballot identifier is: scanner ID, batch ID, and ballot card number. The unique ballot identifier must not tie a ballot to an individual voter

Principle 10
Ballot Secrecy

Principle 10 Ballot Secrecy

The voting system protects the secrecy of voters' ballot selections.

10.2 - The voting system does not contain nor produce records, notifications, information about the voter, or other election artifacts that can be used to associate the voter's identity with the voter's intent, choices, or selections.

10.2.1 – Voter associations

10.2.1-B – Indirect voter associations

No systems may use indirect voter association. ~~Indirect voter associations must only be used to associate a voter with their encrypted ballot selections.~~

Discussion

~~Certain channels of voting require indirect associations so that ineligible ballots can be removed before the ballot is read and counted. Some reasons include signature mismatch or death of a voter. The most common example of indirect association would be a randomly generated number. Best practice would ensure that indirect voter associations are only available to authorized election personnel.~~

Indirect voter associations jeopardize ballot secrecy. Eligibility mismatches must be determined prior to including ballots in the tabulation. Votes legitimately cast by a voter during the allowable voting period should not be able to be retrieved even if the voter dies; the danger to the integrity of an election by degrading ballot secrecy far outweighs any questionable and small advantage.

Signature mismatches and death of voters do not specifically relate to Cryptographic E2E systems.

~~This requirement only applies to paperless voting systems that also meet the requirements under *Guideline 9.1*, which states that the voting system must be software independent. During the writing of these requirements, cryptographic E2E verifiable voting systems are a potential paperless and software independent system that could be applicable for this requirement.~~

~~Applies to: Cryptographic E2E verifiable voting system architectures~~

10.2.1-C – Recallable Ballots

Ballots may never be recallable.

The desire of a tiny number of jurisdictions which wish to require recallable ballots should not be used to allow highly dangerous capabilities in the voting machines used by the rest of the country.

Discussion

A recallable capability alone could reduce the confidence of voters and be used by some to spread distrust of voting systems. It also could open up the voting system to insider attack and vote buying and selling schemes. There is never a need to have an electronic provisional ballot. A hand-marked provisional paper ballot or BMD-printed provisional ballot can be used in a voter-facing system.

~~Use of indirect voter associations~~

~~The voting system must only use indirect voter associations when the option is selected at the beginning of a voting session for situations when a voter needs to fill out a ballot before their eligibility is determined~~.

There is never a need to have an electronic provisional ballot. A hand-marked paper ballot or BMD-printed ballot can be used in a voter-facing system.

~~**Discussion**~~

~~Certain channels of voting require indirect associations so that ballots can be removed before casting for a variety of reasons including signature mismatch or death of a voter. These types of ballots are often considered provisional or recallable ballots.~~

~~Applies to: Cryptographic E2E verifiable voting system~~

~~10.2.1-D – Isolated storage location~~

~~Ballots that are not cast and contain an indirect association must be separated from cast ballots.~~

~~**Discussion**~~

~~Ballots that contain an indirect association are not considered cast. Cast ballots and ballots having their eligibility considered need to be kept separate from each other. Although not the only way of meeting this requirement, one example would be storing cast ballots in a different directory from ballots not yet cast.~~

There is never a need to have an electronic provisional ballot. A handmarked paper ballot or BMD-printed ballot can be used in a voter-facing system.

~~Applies to: Cryptographic E2E verifiable voting architectures~~

~~10.2.1-E – Removal of indirect voter associations~~

~~The voting system must be capable of removing the indirect voter association between a ballot and a voter once that voter is determined to be eligible.~~

~~**Discussion**~~

~~Provisional or recallable ballots may require indirect associations so that ballots can be removed before casting. After a voter's eligibility is determined the indirect voter association can be removed and the ballot can be added to a collection of cast ballots. In the case of electronic E2E systems, whatever data record provides this association must be removed from the system.~~

~~Ballots with indirect associations are not considered cast until the association is removed. Best practice would ensure that indirect voter associations are only available to authorized election personnel.~~

~~Applies to: Cryptographic E2E verifiable voting architectures~~

~~10.2.1-F – Confidentiality for ballots with indirect voter associations~~

~~The voting system must only be capable of decrypting a ballot after any indirect voter association to it has been removed.~~

~~**Discussion**~~

~~Encryption of the ballot preserves the confidentiality of the voter's ballot selections while the ballot is tied to an indirect association to the voter. The indirect voter association is not encrypted with the ballot.~~

~~The voting system must not be capable of decrypting a ballot that still has an indirect association to a voter. A possible approach to implement this is by requiring that a decryption key (or set of keys) be entered to decrypt ballots but disallowing input until after all indirect associations have been removed. If the key is present on the system at the same time as indirect associations, it may be possible for malicious software to decrypt ballots and associate selections with voters.~~

~~Applies to: Cryptographic E2E verifiable voting architectures~~

10.2.2 – Identification in vote records

10.2.2-B – No voter record order information

A voter-facing voting system must not collect or contain data or metadata ~~associated with the~~ such as data in CVR and ballot image files that can be used to determine the order in which ~~ballots votes are cast~~ voters cast ballots.

Discussion

No data or metadata is allowed whether in CVRs and ballot images or elsewhere if that metadata can be used to associate a voter with a record of voter intent. Otherwise, metadata can be useful for verification. For instance, date of creation of record in the voter-facing device might reveal the order of voting. Most other metadata won't be a problem.

10.2.3 – Access to cast vote records (CVR)

10.2.3-B – Digital voter record access log

The voting system must log all access to the directory or storage location for CVRs, ballot images, and ballot selections in addition to logging access to all actions occurring within the system.

Discussion

This ensures that any person, process, or other entity reading, writing, or performing other actions to the electronic audit trail is properly logged.

This requirement applies ~~does not apply~~ when the CVR, ballot images, and ballot selections are stored on removable media and removed from the vote-capture device. Logging data allows detection if anyone is peeking at results before the election is closed.

Related requirements: 11.1-A – Logging activities and resource access

10.2.4 – Voter information in other devices and artifacts

10.2.4-B – Logging of ballot selections

Logs and other portions of the audit trail must not contain individual or aggregate ballot selections.

Discussion

The voting system needs to be constructed so that the security of the system does not rely upon the secrecy of the event logs. It will be considered routine for event logs to be made available to election officials, and ~~possibly even~~ to the public~~, if election officials so desire~~, if permitted by law. The system will be designed to permit the election officials to access event logs without fear of negative consequences to the security and integrity of the election. For example, cryptographic secret keys or passwords will not be logged in event log records.

10.2.4-C – Activation device records

Ballot activation devices must not create or retain information that can be used to identify a voter's ballot, including the order and time at which a voter uses the voting system. The ballot activation device must not be able to transport voter selections from the BMD back to the e-pollbook.

Discussion

Information such as the time the voter arrived at the polls or the specific vote-capture device used by the voter may be used to link a voter with their specific ballot and violates the principle of ballot secrecy. Also, there is a risk that information from the BMD can be transported back to the e-pollbook.

Ballot Activation Device should be in the glossary.

Principle 11
Access Control

11.3 - The voting system supports strong, configurable authentication mechanisms to verify the identities of authorized users and includes multi-factor authentication mechanisms for critical operations.

11.3.1 – Access control mechanisms

11.3.1-B – Multi-factor authentication for critical operations

At a minimum, the voting system must be capable of using multi-factor authentication to verify a user has authorized access to perform critical operations, including:

1. runtime software updates to the certified voting system;
2. aggregation and tabulation;
3. enabling network functions;
4. changing device states, including opening and closing the polls;
5. deleting or modifying the CVRs and ballot images; and
6. modifying authentication mechanisms.

Discussion

NIST SP 800-63-3, Digital Identity Guidelines [NIST17c] provides additional information useful in meeting this requirement. *NIST SP 800-63-3* defines multi-factor authentication (MFA) as follows:

“An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors.

The three authentication factors are something you know, something you have, and something you are.

Multi-factor authenticators include, but are not limited to the following:

- Username & password
- Smartcard (for example, voter access card)
- iButton
- Biometric authentication (for example, fingerprint)

Multi-factor authenticators can be tested for usability to ensure an appropriate balance of security, usability, and functionality. A significant impact to usability may require revision of the multi-factor authenticator implementation.

Related requirements: 8.4-A – Usability testing with election workers

11.3.1-D Multi-person authentication for particularly critical functions

Critical functions should allow extra protection by enabling election offices to require two or more persons, presumably bi-partisan, to authenticate actions. Such protection would be similar to having two keys controlled by different people to open a safe.

Principle 12
Physical Security

Principle 13
Data Protection

Principle 13 Data Protection

The voting system protects data from unauthorized access, modification, or deletion.

The requirements for *Principle 13* include ensuring that the voting system prevents unauthorized access to or manipulation of data and records and that the source and integrity of electronic tabulation reports are verifiable. It details cryptographic standards and ensures that the system protects sensitive data that is transmitted over all networks.

The sections in ***Guideline 13.1*** **include**:

1 – Configuration file which deals with the requirement that the system allow only authenticated system administrators to access and modify voting device configuration files. In addition, the election management system (EMS) will uniquely authenticate individuals associated with the role of system administrator before they can access and modify EMS configuration files. Network appliances will uniquely authenticate individuals before allowing them to access and modify configuration files. Configuration files contain important settings, including security settings, and altering them could impact the overall system

2 – Elections records deals with the need for the vote-capture and tabulation system and the EMS to protect the integrity of the cast vote records (CVRs) and ballot images when they are stored in the voting device. These protections should prevent undetectable changes to CVRs and ballot images.

13.2 – Source and integrity of election records covers the requirement that CVRs and ballot images be digitally signed both when stored and before being transmitted. The EMS needs to be able to cryptographically certify all electronic voting records. Digital signatures of collections of hashes are a form of integrity protection that can also help trace the source of any updates or alterations to election records. The timing and content of the digital signature for the collection of hashes must ensure that votes cannot be linked to a voter.

13.3 – Cryptographic algorithms deals with the requirements that cryptographic functionality be implemented in a cryptographic module validated against *Federal Information Processing Standard (FIPS) 140 [NIST01]*. In addition, cryptographic functions specific to E2E cryptographic voting protocols must adhere to requirements set by the EAC and are omitted from FIPS 140-2 validation. Devices using cryptography need to employ NIST approved algorithms, and the key used with Message Authentication Codes needs to have a specific security strength. Voting system documentation describes how key management is to be performed by election officials.

13.4 – Protecting sensitive data transmission deals with the requirement that data be transmitted by a mutually authenticated connection. Voting systems transmitting data need to cryptographically protect the confidentiality and integrity of data sent over a network. A voting system receiving data will adhere to requirements on verifying and logging data received and presenting any verification errors immediately.

13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

13.1.1 – Configuration file

13.1.2 – Election records

13.1.2-A – Integrity protection for election records

The voting system must ~~integrity~~ either detect or prevent modification of CVRs and ballot images ~~when they are stored~~ anywhere within the voting system.

Any CVRs and ballot images should be cryptographically hashed as soon as possible, and then secured using a digital signature of a collection of cryptographic hashes. The images should be exported in the same format that they were in when originally hashed, collected and signed, so hashes of the exported images match the earlier ones.

.

Discussion

Applying access control can help prevent any unauthorized modifications to CVRs and ballot images.

Applying integrity protection ensures that any unauthorized modifications to CVRs and ballot images can be detected.

For example, ballot images can be integrity protected using a private key maintained in a Hardware Security Module and a cryptographic hash ~~signature~~ of the image collection along with a digital signature of a collection of hashes. The timing and content of the digital signature for the collection of hashes must ensure that votes cannot be linked to a voter.

Related requirements:	13.2-A – Signing stored election records 13.2-B – Verification of election records 1.1.5-I – Ballot Image Hashes, Digital Signatures and Exports

13.2 – The source and integrity of electronic tabulation reports are verifiable.

13.2-A – Signing stored election records

Cast vote records and ballot images must be cryptographically hashed ~~digitally~~ when created ~~stored~~ and, if modified during election processing, again cryptographically hashed before being transmitted or otherwise exported. Collections of hashes must be exported along with a digital signature for each collection. The timing and content of the digital signature for the collection of hashes must ensure that votes cannot be linked to a voter.

Discussion

Digital signatures address the threat that the records might be tampered with when stored or transmitted. Cryptographic hashes do not sufficiently mitigate this threat, as election records could be altered and then re-hashed. Digital signatures also allow verification of the source of any collections of created or modified records. Additional information can be found in *FIPS 186-4 Digital Signature Standard [NIST13c].*

13.2-B – Verification of election records

A voting system must:

1. cryptographically verify the integrity and authenticity of all election data received;
2. immediately log any verification error of received election results;
3. immediately present on-screen any verification errors; and
4. not tabulate or aggregate any data that fails verification.
5. Not include information that provides order of voting for voter-facing systems.

Discussion

This process of verifying election data and results is a defense in depth measure against accidental errors or a malicious incident regarding modified or false election records. For example, checking the cryptographic integrity of received election results prevents modified election results from being maliciously modified and reported on election night.

Principle 14
System Integrity

14.1 - The voting system uses multiple layers of controls to provide resiliency against security failures or vulnerabilities.

14.2 - The voting system limits its attack surface by avoiding unnecessary code, data paths, connectivity, and physical ports, and by using other technical controls.

14.2-A – Non-essential networking interfaces

14.2-B – Network status indicator

14.2-C – Wireless communication restrictions

Voting systems must ~~not~~ be disabled from ~~capable of~~ establishing wireless connections as provided in this section.

Wireless should not be allowed at all. Preventing wireless through software alone is not sufficient. There have been cases where a model without wireless capabilities was purchased and later updated to a model with wireless all through software changes. Wireless must be prevented by permanently disabling any wireless capability in the hardware. If wireless hardware were present, the system could be hacked to provide wireless access to data or to modify the voting system software.

Discussion

Wireless connections can expand the attack surface of the voting system by opening it up to overthe-air attacks. Over-the-air access can allow for adversaries to attack remotely without physical access to the voting system. By disallowing wireless capabilities in the voting system, this limits the attack surface and restricts any network connections to be hardwired. Examples of how wireless can be disabled may include the following:

- ~~a system configuration process that disables wireless networking devices,~~
- ~~disconnecting/unplugging wireless device antennas, or~~
- removing wireless hardware within the voting system.

~~This requirement does not prohibit wireless hardware within the voting system so long as the hardware cannot be used e.g. no wireless drivers present.~~

This requirement applies solely to voting systems that are within the scope of the VVSG. It is not a prohibition on wireless technology within election systems overall. This requirement does not impact or restrict the use of assistive technology (AT) within the polling place. Voters with wireless AT may have to use an adapter that leverages the 3.5 mm headphone jack.

Related requirements:	8.1-E – Standard audio connectors 15.4-C – Documentation for disabled wireless

14.2-D – Wireless network status indicator

If a voting system has network functionality, the voting system application must visually show an indicator within the management interface to confirm that wireless networking functionality is disabled.

If there is no wireless hardware, this indicator would be unnecessary.

Discussion

Note that this is in addition to the networking identifier.

Wireless is a significant avenue for system compromise. This indicator ensures that wireless functionality is not enabled by accident.

14.3 - The voting system maintains and verifies the integrity of software, firmware, and other critical components.

14.3-A – Supply chain risk management strategy

14.3-B – Criticality analysis

14.3-C – Bill of materials

The voting system's documentation must include the hardware and software information for all ~~the critical~~ components defined in the *14.3-B* and at minimum list the following information for each component:

1. component name;
2. manufacturer;
3. model or version; and
4. applicable platform for software (e.g., Windows or Linux).

Even non-critical components can later be discovered to be non-trustworthy.

Discussion

This requirement will use the critical components defined in the critical analysis of *14.3-B – Criticality analysis*. At minimum the bill of materials for critical components are required, but this does not restrict the voting system vendor from listing the bill of materials for other components.

This is a common practice when providing a hardware bill of materials. It is not as common to produce a bill of materials for software and as standards/best practices are developed, they should be considered for inclusion in the software bill of materials.

For more information about the risks of third-party components and developing software bills of materials, see *"Managing Security Risks Inherent in the Use of Third-party Components" [SAFECode19]* and resources from the *National Telecommunications and Information Administration about Software Bills of Materials [NTIA19].*

Principle 15 Detection and Monitoring

Appendix A Glossary of Terms

adjudication

Process of resolving flagged **cast ballots** to reflect **voter intent**. Common reasons for flagging include:

- write-ins,
- **overvotes**,
- marginal **machine-readable mark**,
- having no **contest selections** marked on the entire **ballot**, or
- the ballot being unreadable by a scanner,
- voter intent that is not machine-readable.

ballot image

Archival digital two-dimensional image (e.g. JPEG, PDF, etc.) optically captured from one or more sides of a paper ballot cast by an individual voter.

ballot sheet

A sheet of paper that is part of a voter's ballot. A ballot may consist of several sheets of paper, each containing one or two ballot sides with selections.

ballot side

A side of a ballot sheet that is part of a voter's ballot with selections.

cast vote record

Archival tabulatable **record** of a set of some or all **contest selections** produced by a single **voter** as interpreted by the **voting system**.

Synonyms: CVR

E.g., A CVR can consist of the votes of a voter on one or two sides of the same ballot sheet, yet multi-sheet ballots would require separate CVRs.

compliance audit

A compliance audit is a comprehensive review of an organization's adherence to governing documents or processes. For instance, a compliance audit of a paper ballot system assesses the trustworthiness of the paper trail. It includes but is not limited to ballot accounting, eligibility compliance, physical chain-of-custody, evaluation of compliance with election processes.

~~Misfeed~~ misfeed rate

Ratio of the misfeed total to the total **ballot** volume.

N-of-M voting

Vote variation in which the **voter** is entitled to allocate a fixed number of **votes** (N) over a list of M **contest options** or **write-in options**, with the constraint that at most 1 vote may be allocated to a given contest option. This usually occurs when multiple **seats** are concurrently being filled in a governing body such as a city council or school board where **candidates** contend for at-large seats. The voter is not obliged to allocate all N votes. 1-of-M is N-of-M voting where N = 1.

non-manual mode

An interaction mode that uses ~~use~~ assistive technology, for example, a sip-and-puff switch, to allow voters with no use of their hands to operate the voting system.

paper ballot side

The face of a ~~**paper**~~ **ballot sheet**. A **paper ballot** may have two sides per sheet and one or more sheets per ballot.

Synonyms: ballot side

Note that we have suggested a definition for ballot sheet.

ranked choice voting

A **vote variation**:

- Ranked Choice Voting (RCV) is a voting method which allows each **voter** to rank **contest options** in order of the voter's preference,
- RCV is a counting method in which **votes** are **counted** in rounds using a series of runoff tabulations to defeat contest options with the fewest votes and transfer votes for each defeated contest option to a lower-ranked contest option on each ballot, and,
- Instant Runoff Voting (IRV) is a counting method which elects a winner with a majority of final-round votes in a single-winner **contest** and
- Single Transferable Vote (STV) is a counting method which provides proportional representation in multi-winner contests.
- Sequential At-Large IRV is a multi-winner counting method which uses successive IRV passes and does not result in proportional representation.

Synonyms: ~~IRV,~~ RCV~~, instant run-off voting ranked order~~

> *A vote variation has two parts: the way that a voter marks a ballot and the tabulation method. RCV uses the same ballot for many different possible tabulation methods.*

Confusion arises because non-RCV methods, such as Borda Count or Buckin Voting or Microsoft 365's Ranking Form, also use a ranked-order ballot, but very different tabulation.

recallable ballot

Recorded ballot that can be individually retrieved and included or excluded from further processing.

Recallable ballots should never be allowed, but the term is used so it should be in the glossary.

See 10.2.1-C.

straight-party voting

Mechanism that allows **voters** to **cast** a single **vote** to select all **candidates** on the **ballot** affiliated with ~~from~~ a single **political party**.

secret key cryptography

Encryption system that uses the same key for encryption and **decryption**. Access to this ~~This~~ key must be limited to authorized users~~kept secret~~.

test ~~Test~~ plan

Document created prior to testing that outlines the scope and nature of testing, items to be **tested**, test approach, resources needed to perform testing, test tasks, risks, and schedule.

vote-capture device

Component of a voting system that captures and/or counts voter selections from paper or electronic ballots. Vote-capture devices may or may not be directly voter-facing; voter-facing vote-capture devices include ballot marking devices and voter-facing scanners, while non-voter facing vote-capture devices include batch-fed scanners used in central count facilities.

Electronic ballot is not defined and either should be defined or should not be used.

voter-facing scanner

An electronic **voting device** that:

- accepts hand-marked or BMD-produced **paper ballots** one sheet at a time;
- is usually used for **in-person voting**;
- permits **election workers** to open and close the **polls**;

- scans a **ballot** and rejects it if either unreadable or un-processable;
- detects, interprets and validates **contest selections**;
- notifies the **voter** of voting exceptions (such as **undervotes** or **overvotes**) or unreadable marks;
- stores accepted ballots in a secure container; and
- ~~sorts or otherwise marks ballots or **ballot images** that need subsequent human review; and~~
- **tabulates** and **reports** **contest** results after polls are closed.

This unit was previously referred to as a **precinct count** optical scanner or

PCOS.

Synonyms: PCOS, precinct-count optical scanner

—----------end of SAWG comments, May 2023—------------------