Principle 10
Ballot Secrecy

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

10.1 - Ballot secrecy is maintained throughout the voting process.

10.1-A – System Use of Voter Information

The voting system must be incapable of accepting, processing, storing, and reporting identifying information about a specific voter.

Applies to: Voting System

Discussion

Examples include first name, last name, address, driver's license and voter registration number. The voting system cannot prevent a voter from self-identifying within write-in fields.

Status:	New
Updated:	Jan 2, 2018
Source:	N/A
Gap notes:	

10.1-B – Physical Secrecy Protection

The voting system must provide physical security mitigations against a ballot being seen by other individuals or technology in the polling place (e.g., privacy screen).

Applies to: Voting System

Discussion

A polling place may use a variety of methods to prevent shoulder surfing attacks (e.g., a voting booth, A blackout curtain, or a protective screen).

Status:	New
Updated:	Jan 2, 2018
Source:	N/A
Gap notes:	Physical Security

Comment [FJM(1]: Open comment: 10.1-A would preclude many remote electronic ballot delivery systems from being included as a part of the voting system. These systems may authenticate voters with username and password, which often has first name, last name, and email within the same system.

Deleted: and

Comment [FJM(2]: Open comment: We have a comment that this is out of scope for security and belongs in voter privacy.

10.1-C – Secrecy of Audibly Read Ballot Selections

During the voting session, the audio interface of the voting system must only be audible within a one foot radius of the voter.

Applies to: Voting System

Discussion
Voters who are hard of hearing but need to use an audio interface may also need to increase the volume of the audio. Such situations require headphones with low sound leakage.

Status:	New
Updated:	Jan. 2, 2018
Source:	2007 3.2.3.1-A.2
Gap notes:	Voter Privacy

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-A – Direct Voter Associations

The voting system must not create or store direct associations between a voter's identity and their ballot.

Applies to: Voting System

Discussion
A direct voter association would be the voting system storing that John Smith voted for George Washington. Other examples of a direct association would include tying ballot selections to a social security number (SSN), voter identification number, or driver's license number. This is not an exhaustive list of direct voter association examples.

Status:	New
Updated:	Jan 2, 2018
Source:	N/A
Gap notes:	

10.2-A.1 – Confidentiality Protection of Cast Votes

The voting system must not encrypt CVRs and ballot images that have been cast.

Applies to: Voting System

Discussion
To be anonymous, cast ballots lack any association to a voter. Cast ballots, including their digital analogues, make up a key portion of a voting system's audit trail. It is of utmost importance that the

audit trail be available to election officials to be used within an audit. The management of cryptographic keys and passwords provides an opportunity to be unable to retrieve this information.

Status:	New
Updated:	Jan. 2, 2018
Source:	N/A
Gap notes:	Data Protection

10.2-A.2 – Cast Vote Signatures

The voting system must digitally sign CVRs and ballot images.

Applies to: Voting System

Discussion

Digitally signing CVRs and ballot images provides integrity protection to ensure that these digital voter records unmodified. Digital signatures are also useful in ensuring the identity of the entity signing the records. Cryptographic hashes solely provide integrity protection and are insufficient for this use case.

Status:	New
Updated:	Jan. 18, 2018
Source:	N/A
Gap notes:	Data Protection

The requirements within 10.2-B apply to voting systems that provide the capability for using indirect voter associations. Although many jurisdictions may choose for the voting system to assist in handling them, other jurisdictions may choose to handle the use of these associations procedurally.

10.2-B – Indirect Voter Associations

The voting system may use Indirect associations for situations when a voter needs to fill out a ballot before their eligibility is deteremined.

Applies to: Voting 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, death of a voter, etc. The act of casting the ballot permanently strips it of an identifier. The most common example of indirect association would be a randomly generated number. 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.

Status: New
Updated: Jan 2, 2018
Source: N/A
Gap notes:

10.2-B.1 – System-wide Support of Indirect Associations

All voting system components that capture ballot selections from a voter must be able to support indirect associations.

Applies to: Voting System

Discussion

Ensuring that all voting systems can support indirect associations helps to prevent a single machine from being designated as the "provisional" or "accessible" machine.

Status: New
Updated: Jan 18, 2018
Source: N/A
Gap notes:

10.2-B.2 – Pollworker Selection of Indirect Associations

The option for using an indirect association must be selected at the beginning of each new voting session.

Applies to: Voting System

Discussion

Status: New
Updated: Jan 18, 2018
Source: N/A
Gap notes:

10.2-B.3 – Isolated Storage Location

Ballots that are not cast, and contain an indirect association, must be stored in separate storage locations from cast ballots.

Applies to: Voting System

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.

Status: New
Updated: Jan 2, 2018
Source: N/A
Gap notes:

10.2-B.4 – Confidentiality for Indirect Associations

Ballots that are not cast, and contain an indirect association, must be encrypted.

Applies to: Voting System

Discussion

Status: New
Updated: Jan 2, 2018
Source: N/A
Gap notes: Data Protection

10.2-C – Identifiers Used for Audits

Identifiers used for tying a CVR and ballot images to physical paper ballots must be distinct from identifiers used for indirect associations.

Applies to: Voting System

Discussion

For the purpose of these requirements, associations between physical ballots and CVRs are not considered direct or indirect identifiers.

Status: New
Updated: Jan 18, 2018
Source: N/A
Gap notes:

10.2-D – Prohibition on Voter Record Order Information

The voting system SHALL NOT contain data or metadata associated with the CVR and ballot image files which can be used to determine the order in which votes are cast..

Applies to: Voting System

Discussion

Status: New
Updated: Jan. 2, 2018
Source: N/A
Gap notes:

10.2-E – Identifying Information in Voter Record File Names

CVR and ballot image names must not include any information identifying a voter.

Applies to: Voting System

Discussion

This helps to ensure that information that could accidently be used to reference a voter is not used within a file name.

Status: New
Updated: Jan. 2, 2018
Source: N/A
Gap notes:

10.2-F – Non-Memorable Identifiers & Associations

Unique identifiers and associations must not be displayed in a way that is easily memorable by the voter.

Applies to: Voting System

Discussion

Unique identifiers on the paper record are displayed or formatted in such a way that they are not memorable to voters, such as by obscuring them in other characters.

Status: New
Updated: Jan. 2, 2018
Source: N/A
Gap notes: 9.4 Efficiency

10.2-G – Voter Record Metadata

Comment [FJM(3]: Open comment: Need serious discussion to evaluate.

CVR and ballot image metadata must be encrypted.

Applies to: Voting System

Discussion

Status: New
Updated: Jan. 2, 2018

Source: N/A
Gap notes:

10.2-H – Aggregation & Ordering

Aggregated and final totals must not contain voter specific information, and must not be able to recreate the order in which the ballots were cast.

Applies to: Voting System

Discussion

Status: New
Updated: Jan. 2, 2018
Source: N/A
Gap notes:

10.2-I – Least Privilege Access to Store

The directory or storage location of CVRs, ballot images, and ballot selections on the voting system must be subject to the principle of least privilege.

Applies to: Voting System

Discussion

Status: New
Updated: Jan. 2, 2018
Source: N/A
Gap notes: Access Control

10.2-I.1 – Limited Access

Permissions to access the directory or storage location for CVRs, ballot images, and ballot selections must be assigned to as few entities as possible.

Applies to: Voting System

Discussion
Entities include people and applications / processes running on the voting system.

Status: New
Updated: Jan. 2, 2018
Source: N/A
Gap notes: Access Control

10.2-I.2 – Authorized Access

Permissions to access the directory or storage location for CVRs, ballot images, and ballot selections must be validated and explicitly authorized before access is given.

Applies to: Voting System

Discussion

Modern operating systems often have sufficient mechanisms in place to accomplish this, but these security capabilities must be configured and enforced.

Status:	New
Updated:	Jan. 2, 2018
Source:	N/A
Gap notes:	Access Control

10.2-I.3 – Digital Voter Record Access Log

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

Applies to: Voting 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.

Status:	New
Updated:	Jan. 2, 2018
Source:	N/A
Gap notes:	Access Control, Auditing

10.2-J – Voter Information within Receipts

Voting systems providing a receipt must not contain voter information.

Applies to: Voting System

Discussion

Status:	Updated
Updated:	Jan. 2, 2018
Source:	N/A
Gap notes:	

10.2-K – Logging of Ballot Selections

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

Applies to: Voting System

Discussion

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

Status:	Updated
Updated:	Jan. 2, 2018
Source:	N/A
Gap notes:	

10.2-L – Activation Device Records

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.

Applies to: Voting System

Discussion

The activation device must not create or retain any information that could be used for the purposes of identifying a voter's ballot, or the time at which the voter arrived at the polls, or the specific vote-capture device used by the voter.

Status:	Updated
Updated:	Jan. 2, 2018
Source:	N/A
Gap notes:	

10.2-M – Warnings

The voting system must issue all warnings in a way that preserves the confidentiality of the ballot.

Applies to: Voting System

Discussion

HAVA 301 (a)(1)(C) mandates that the voting system must notify the voter of an attempted overvote

in a way that preserves the privacy of the voter and the confidentiality of the ballot. This requirement generalizes that mandate.

Status: Updated
Updated: Jan. 2, 2018
Source: N/A
Gap notes:

10.2-N – Error Notifications

The voting system must obscure any evidence of the voter's ballot selections when an error is presented onscreen.

Applies to: Voting System

Discussion

Status: New
Updated: Jan 2, 2018
Source: N/A
Gap notes:

The requirement 10.2-K applies to voting system using End-to-End Cryptographic Protocols.

10.2-O – Ballot Secrecy for Receipts

The voting system must not issue a receipt to the voter that would provide proof to another of how the voter voted.

Applies to: Voting System

Discussion
This requirement primarily applies to

Status: Updated
Updated: Jan. 2, 2018
Source: 2007 Vol 1: 3.2.3.1-A.4
Gap notes:

Comment [FJM(4]: Open Comment: What kind of error? It might be useful to display the voter's selections onscreen if the error is regarding second chance voting. If the error is defined as unexpected behavior of the system, then I agree.