Deleted: 4/6/18

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, with the exception of blank ballot distribution and online ballot marking systems.

Deleted: U
Deleted: V
Deleted: I
Deleted: .

Applies to: Voting device

Deleted: 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.

Deleted: S
Deleted: P
Deleted: (for example e.g., privacy screen)

Applies to: Voting System

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

Deleted: (e.g.
Deleted: A
Deleted: a

Status:	New
Updated:	Jan 2, 2018
Source:	N/A
Gap notes:	Physical security, Voter privacy

Deleted: S
Deleted: /
Deleted: P
Deleted:

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 and 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, 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:	

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.

Deleted: A

Deleted: R

Deleted: B

Deleted: S

Deleted:

Deleted: but

Deleted: P

Deleted:

Deleted: V

Deleted: A

Deleted: S

Deleted: (SSN)

Deleted: 10.2-A.1 – Confidentiality pProtection of cCast vVotes¶
The voting system must not encrypt cast vote records (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 prevent the be unable to retrieval of e this information. ¶
Status: →New¶
Updated:→ Jan. 2, 2018¶
Source: →N/A¶
Gap notes:→Data Protection ¶
10.2-A.2 – Cast vVote sSignatures ¶
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 are 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¶

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 determined.

Applies to: E2E voting system architectures

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. 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.2 –Election worker selection of indirect associations

When the use of an indirect associations is needed, an election worker must select the option for using an indirect association at the beginning of each new voting session.

Applies to: E2E voting system architectures

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: E2E voting system architectures

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

Deleted: V

Deleted: A

Deleted: e

Deleted: Voting System

Deleted: ,

Deleted: , etc

Deleted: 10.2-B.1 – System-wide sSupport of iIndirect aAssociations ¶
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:→ ¶

Deleted: Poll

Deleted: S

Deleted: I

Deleted: A

Deleted: The

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

Deleted: Voting System

Deleted: ¶

Deleted: S

Deleted: L

Deleted: ,

Deleted: Voting System

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 association

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

Applies to: E2E voting system architectures

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: Auditability

10.2-D – Prohibition on voter record order information

The voting system must 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

Deleted: I
Deleted: A
Deleted: iations
Deleted: Voting System
Deleted: U
Deleted: A
Deleted: S
Deleted:
Deleted: V
Deleted: R
Deleted: O
Deleted: I
Deleted: SHALL NOT
Deleted: .
Deleted: S

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 and associations

Unique identifiers and associations must not be displayed in a way that is easily remembered 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 easily remembered by 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-H – Aggregation and 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

Deleted: I
Deleted: V
Deleted: R
Deleted: F
Deleted: N
Deleted: S
Deleted: M
Deleted: I
Deleted: &
Deleted: A
Deleted: memorable
Deleted: S
Deleted: memorable to
Deleted: 10.2-G – Voter rRecord Mmetadata¶
CVR and ballot image metadata must be encrypted. ¶
Applies to: Voting System¶
Discussion
¶
Status: →New¶
Updated:→Jan. 2, 2018¶
Source: →N/A ¶
Gap notes:→¶
Deleted: &
Deleted: O
Deleted: S

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

NIST SP 800-12 defines "least privilege" as "The security objective of granting users only those accesses they need to perform their official duties." [800-12]

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

10.2-I.1 – Limited access

Permission 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 or 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

Deleted: P
Deleted: A
Deleted: S
Deleted: S
Deleted: JL: Consider explaining "least privilege" here.
Formatted: Font: Not Bold
Formatted: Font: Not Bold
Formatted: Tab stops: 4.03", Left
Formatted: Highlight
Deleted: A
Deleted: s
Deleted: S
Deleted: /
Deleted: A
Deleted:
Deleted: S

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

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

Receipts produced by a voting system 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 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. The system must be designed to permit

Deleted: V
Deleted: R
Deleted: A
Deleted: L
Deleted: and actions occurring within,
Deleted: .
Deleted: S
Deleted: I
Deleted: R
Deleted: Voting systems providing a
Deleted: r
Deleted: S
Deleted: B
Deleted: S
Deleted: S
Deleted: should
Deleted: ,

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 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 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:

Deleted: do so

Deleted: ¶

Formatted: Indent: Left: 0.5", Hanging: 1.5"

Deleted: D

Deleted: R

Deleted: S

Deleted: at which

Deleted: S

10.2-N – Error notifications

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

Applies to: Voting system

Discussion

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

The requirement 10.2-O 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, E2E voting system architectures

Discussion

This requirement primarily applies to

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

Deleted: N

Deleted: S

Deleted: S

Deleted: R

Deleted: S

Deleted: System using

Deleted: Cryptgraphic Protocols