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 – Preventing the Mixing of Voter Information

The voting system SHALL be incapable of accepting, processing, storing, and reporting, identifying information about a specific voter, such as first name, last name, address, and any unique identifiers used outside the voting system.

Applies to: Voting System

Discussion

Voter information in this context includes first name, last name, address, drivers license number, and any other identifier used external from the voting system. For instance, voter registration information shall never be intermixed with the voting system.

Status: New
Updated: Jan 2, 2018
Source:
Gap notes:

10.1-B – Physical Secrecy Protection

The voting system SHALL 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:
Gap notes:
10.1-C – Ballot Secrecy Inferences
No inference of a voter’s ballot selections SHALL be possible that reveals a voter’s identity or how they voted.

Apply to: Voting System

Discussion
For instance, if multiple data sources from the voting system are combined, is it not possible to determine an individual voter’s ballot.

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated:</td>
<td>Jan. 2, 2018</td>
</tr>
<tr>
<td>Source:</td>
<td></td>
</tr>
<tr>
<td>Gap notes:</td>
<td>Voter Privacy</td>
</tr>
</tbody>
</table>

10.1-D – Secrecy of Audibly Read Ballot Selections
During the voting session, the audio interface of the voting system SHALL be audible only to the voter.

Apply 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.

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated:</td>
<td>Jan. 2, 2018</td>
</tr>
<tr>
<td>Source:</td>
<td>2007 3.2.3.1-A.2</td>
</tr>
<tr>
<td>Gap notes:</td>
<td>Voter Privacy</td>
</tr>
</tbody>
</table>
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 SHALL not create or store direct associations between a voter’s identity and their ballot.

Applies to: Voting System

Discussion
Definition of “direct voter association” included here. Should include name, SSN, voter identification number, DL number

Status: New
Updated: Jan 2, 2018
Source:
Gap notes:

10.2-A.1 – Protecting Cast Votes
The voting system SHALL not encrypt CVRs and ballot images that have been cast.

Applies to: Voting System

Discussion
This ensures they are part of the audit trail. Integrity protection for this information is addressed within the Data Protection guidelines.

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

10.2-B – Indirect Voter Associations
The voting system SHALL only use Indirect associations for early, absentee, and provisional voting modes.

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. Example of an indirect association include
10.2-B.1 – Separate Storage Location
Ballots that are not cast, and contain an indirect association, SHALL be stored separately from cast ballots.

Applies to: Voting System

10.2-B.2 – Confidentiality for Indirect Associations
Ballots that are not cast, and contain an indirect association, SHALL contain confidentiality protection.

Applies to: Voting System

10.2-C – Voter Record File Name Randomization
CVR and ballot image file names SHALL be randomly generated.

Applies to: Voting System
10.2-D – Identifying Information in Voter Record File Names
CVR and ballot image names SHALL not include any information identifying a voter.

Applies to: Voting System

Discussion

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

10.2-E – Non-Memorable Identifiers & Associations
Unique identifiers and associations SHALL 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:
Gap notes: audit efficiency?

10.2-F – Storage Randomization
CVRs and ballot images SHALL be stored in a random manner to prevent a loss of ballot secrecy.

Applies to: Voting System

Discussion

Status: New
Updated: Jan. 2, 2018
Source:
Gap notes:
10.2-G – Voter Record Metadata
CVR and ballot image metadata SHALL be confidentiality protected.

Applies to: Voting System

Discussion

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated:</td>
<td>Jan. 2, 2018</td>
</tr>
<tr>
<td>Source:</td>
<td></td>
</tr>
<tr>
<td>Gap notes:</td>
<td></td>
</tr>
</tbody>
</table>

10.2-H – Aggregation & Ordering
Aggregated and final totals SHALL not contain voter specific information, and should not be able to recreate the order in which the ballots were cast.

Applies to: Voting System

Discussion

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated:</td>
<td>Jan. 2, 2018</td>
</tr>
<tr>
<td>Source:</td>
<td></td>
</tr>
<tr>
<td>Gap notes:</td>
<td></td>
</tr>
</tbody>
</table>

10.2-I – Least Privilege Access to Store
The directory or storage location of CVRs, ballot images, and ballot selections on the voting system SHALL be subject to the principle of least privilege.

Applies to: Voting System

Discussion

<table>
<thead>
<tr>
<th>Status:</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated:</td>
<td>Jan. 2, 2018</td>
</tr>
<tr>
<td>Source:</td>
<td></td>
</tr>
<tr>
<td>Gap notes:</td>
<td>Access Control</td>
</tr>
</tbody>
</table>

10.2-I.1 – Limited Access
Permissions to access the directory or storage location for CVRs, ballot images, and ballot selections SHALL be assigned to as few entities as possible.
10.2-I.2 – Authorized Access
Permissions to access the directory or storage location for CVRs, ballot images, and ballot selections SHALL be validated and explicitly authorized before access is given.

10.2-I.3 – Access Log
The voting system SHALL log all access to, and actions occurring within, the directory or storage location for CVRs, ballot images, and ballot selections.

10.2-J – Ballot Secrecy for Receipts
The voting system SHALL NOT issue a receipt to the voter that would provide proof to another of how the voter voted.
10.2-K – Voter Information within Receipts
Voting systems that provide a receipt SHALL NOT contain voter information.

Applies to: Voting System

10.2-L – Logging of Ballot Selections
Logs and other portions of the audit trail SHALL 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.
10.2-M – Activation Device Records

Activation devices SHALL 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:
Gap notes:

10.2-N – Warnings

The voting system SHALL 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:
Gap notes:

10.2-O – Error Notifications

The voting system SHALL 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:
Gap notes: <text>