Discussion of Indirect Voter Association

This document highlights the cybersecurity working group discussion around the indirect identifiers by a voting system. Indirect identifiers are noted as an open area due to concerns around indirect voter associations and ballot secrecy. This document will list the current and potential use cases of indirect identifiers, identify the threat concerns, and discuss current VVSG 2.0 related requirements.

Overview
Decision Points
• Are Indirect voter associations necessary for certain voting systems?

Use Cases
Future Uses

| E2E verifiable paperless system handling conditional ballots |

Primary Concern(s) of using
Violation of Ballot Secrecy - Any association (direct or indirect) can be used to link a voter to their 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.
Indirect Voter Association Analysis
This section steps through a list of indirect voter association uses cases that are relevant to scope of the VVSG requirements. Each use case is followed by concerns, suggested mitigations and related requirements.

E2E Verifiable Paperless System Handling Conditional Ballots
Conditional ballots are completed and submitted by a voter for review of voter eligibility. Ballots that are completed and submitted through an electronic system (e.g., E2E paperless system), may require an indirect identifier to locate and remove the ballot if a voter is found ineligible. There are three common scenarios for conditional ballots:

1. **Provisionals** - If a voter is unable to confirm their identity at the polling place, the voter is allowed to complete and submit a ballot for eligibility review.
2. **Absentee/Military Voting** – Ballots may be submitted in advance due to a voter’s schedule or other unavoidable circumstances.
3. **Change of Eligibility** – A ballot must be removed from the official count due to a change in a voter’s eligibility status (e.g., death or relocation).

Concerns

**Ballot Secrecy Violation**
If the indirect voter associations are stored on the voting system. Due to their nature, the indirect voter associations may allow an attacker to extract the indirect voter associations and use them to correlate a voter with their ballot selections.

**Coercion and Vote Buying**
A coerced voter may be able to provide proof of how they voted using an indirect voter association.

**Eligibility Tampering**
Because indirect voter associations are used to confirm eligibility, if an attacker has access to the IVA database, they may be able to maliciously modify the eligibility of ballots.

Mitigations

**Ensure Unlinkability of Ballots – External Storage**
Ensure that the voting system does not receive any voter information that can be used to link a voter to their ballot selections. This may done by storing the indirect voter associations in a database that is separate from the voting system.
Related Requirements

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

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

Interoperability Guideline 4.2
Standard, publicly-available formats for other types of data are used, where available.

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.

10.2-E – Identifying information in voter record file names
CVR and ballot image names must not include any information identifying a voter.

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

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.

10.2-J – Voting information with receipts
Receipts produced by a voting system must not contain voter information.

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.

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.

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: E2E voting system architectures