Discussion Topic: *Indirect Voter Association (IVA)*

This document highlights the cybersecurity working group discussion around the indirect voter associations (IVAs) by a voting system. IVAs are noted as an open area due to concerns around ballot secrecy. This document will list the potential use cases for IVAs, identify the threat concerns, and discuss current VVSG 2.0 related principles, guidelines, and/or requirements.

**Decision Points**
- Are indirect voter associations necessary for certain voting systems?

**Use Cases**
Through discussion with the working group, one potential use case for IVAs was identified and is listed below.

**Potential Future Use of IVAs**
- Paperless system handling conditional ballots (e.g., provisional ballots)
  
  *Note:* The current draft VVSG 2.0 requirements states that a voting system must be software independent.

The following sections describe the general concerns with using IVAs in the voting system and potential mitigations to address those concerns. The concerns and mitigations are illustrated through reference to the VVSG Principles and Guidelines. The concerns and mitigations do not represent a consensus opinion, but rather an aggregation of what was discussed by the cybersecurity working group.

**General Concerns**

**Concern A.**  
*Principle 10: Ballot Secrecy, Guideline 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.*

If a voter submits a provisional ballot via a paperless system, the voting system will need a way to process the conditional ballot. This would require to the voting system to store an IVA to remove a voter’s ballot if they are found ineligible. This IVA could be used to link a voter with their ballot selections and violating ballot secrecy.

IVAs may also be problematic if a coerced voter is able to use an IVA to prove to their coercer/vote buyer how they voted during an election.
Concern B. Principle 9: Auditable, Guideline 9.3 - Voting system records are resilient in the presence of intentional forms of tampering and accidental errors.

IVAs stored in a voting system may be used to identify all eligible and ineligible voters. An attacker with access to this IVA database, may be able to maliciously modify the eligibility of ballots and falsely discard the ballots of eligible voters or include the ballots of ineligible voters.

Potential Mitigations

Principle 10: Ballot Secrecy, Guideline 10.1 - Ballot secrecy is maintained throughout the voting process.

To apply ballot secrecy, one potential mitigation is the submission of provisional ballots through the use of a paper ballot and the implementation of an external process. This external process is one way of ensuring that no IVAs are stored within the voting system. This external process is not described within the VVSG requirements because it does not utilize the physical voting system and is administered by the local jurisdictions.

Applies to concern(s): A

Principle 13: Data Protection, Guideline 13.1 - The voting system prevents unauthorized access to or manipulation of configuration data, cast vote records, transmitted data, or audit records.

Similar to the external paper process for handling provisional ballots, IVAs may be stored in a database that is physically separate from the voting system. Once that separate system confirms a ballot is eligible for submission, that ballot is disassociated from its IVA and added to the final tabulation.

Applies to concern(s): B