Discussion Topic: *Barcodes*

This document highlights the discussion around the use of barcodes by a voting system. There are requirements within the Voluntary Voting System Guidelines (VVSG) 2.0 that are specific to barcodes or encoded information produced by a voting system. Barcodes are noted as an open area for the standard due to concerns around integrity, transparency, auditability, interoperability and ballot secrecy.

**Decision Points**

- What information can be encoded or stored in barcodes?
- Does this topic include similar markings on a ballot (e.g., timing marks or mark-sense)?

**Use Cases**

This section does not cover all use cases of barcodes in elections. These lists are intended to capture the interest in the technology and assist in explaining the concerns.

**Current Use of Barcodes in Elections**

- Store and apply ballot activation information (e.g., ballot style)
- Store voter registration number on ballots submitted through vote-by-mail
- Use stored ballot selections for tabulation
- Store ballot identifier
- Printing/recreating mail-in ballots (Ballot on Demand)
- Apply voter accessibility options
- Capture ballot selections at the polling place
- Store ballot selections prior to entering polling place (e.g., Interactive Sample Ballot Transfer)
- Input CVR data
- Remotely transferring aggregation of unofficial tabulation results

**Potential Future Use of Barcodes in Elections**

- Compare ballot selections in barcode with human-readable text
- Store digital signature to verify the data is from a valid BMD and a checksum to identify any discrepancies
- Protect against coercion by storing a crypto-code that verifies valid ballots vs. faux ballots (Ballot Selfies Coercion)
Store checksum value that notifies of any discrepancies in interpretation of human-readable text

Preserve ballot secrecy by storing encryption data that only provides the necessary information for a ballot comparison audit

In the context of the VSAP system, using the barcode to store E2E Verifiable back-end verification data (e.g., Seed data)

The following sections describe the concerns with using barcodes in the voting system and potential mitigations to 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 3: Transparency, Guideline 3.3 - The public can understand and verify the operations of the voting system throughout the entirety of the election.**
Barcodes lack transparency. They are not human-readable, meaning a voter/election worker is unable to easily read and understand what information is stored in a barcode. Poor or maliciously designed barcodes may allow for unauthorized transmission of data (e.g. data leakage). This data may include, voter identifying information or malicious input to the voting system.

Concern B.  
**Principle 7: Marked, Verified, and Cast as Intended - Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.**
If a voter’s ballot selections are stored in a barcode, the lack of human-readability of that barcode, means the voter may be unable to verify that their ballot selections are accurately captured within the barcode.

Concern C.  
**Principle 9: Auditable, Guideline 9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.**
Barcodes alone are not software independent. In the case of a presentation attack, a vote capture device may display the voter selecting one contest when they are actually selecting another (a.k.a. clickjacking). Malicious/faulty production of a barcode or barcode reader may present inaccurate information to a voter or election worker. For example, a malicious barcode may present the voter with different ballot selections than what will be interpreted by the voting machine. If barcodes are used for tabulation of cast ballots, any modification of a voter’s ballot selections may go undetected and impact the election results. Another concern is how
discrepancies can be detected and how to handle issues of mismatching information.

**Concern D.** 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.

Some barcodes are used to activate the ballot, apply ballot style, and/or apply accessibility options to a vote capture device. This information may come from an e-pollbook. Barcodes generated outside of the polling place can also be used to "remake" a ballot or to generate an electronic ballot with selections. The lack of transparency makes it unclear whether the barcode stores any voter identifying information that can be used to link a voter to their ballot selections. If a barcode does include voter identifying information and that information is stored by the voting system or presented on a "remade" ballot, then it would violate the principle of ballot secrecy.

**D.1. 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.

In the use case where, a voter can store their ballot selections prior to entering polling place (e.g., Interactive Sample Ballot Transfer), a voter may be coerced into filling out their sample ballot in a manner that goes against their own opinion. Voters can use the barcode to present the coercer with proof of their vote selections. Voters may also be offered a reward to vote a specific way and required to provide proof to receive the reward.

**Concern E.** Principle 15: System Integrity - The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

A barcode can store additional data that can be used to inject malicious commands into a voting system. A barcode could potentially input malicious commands that modify data, inject malware, or give unauthorized access to election data. In addition to the modification of election results as mentioned under the auditable principle, the injection of malware may modify system data to force the machine to perform in an unintended manner or not perform at all (e.g., Denial of Service).

**Potential Mitigations**

*Note:* It is not within the scope of the VVSG to require audits, specify what types of audits states should perform, and how states should review their voting system’s services. The below mitigations may be dependent on whether a state requires audits and reviews/analyzes any implementation documentation. This notion and potential mitigations may apply to various other requirements and may apply to other aspects of the voting system beyond barcodes.
Principle 4: Interoperable, Guideline 4.2 - Standard, publicly-available formats for other types of data are used, where available.

Due to the potential lack of transparency, awareness of the contents of a barcode is vital to ensure the barcode only contains the necessary information for its function. This concern would imply the need for a way to verify that the barcode/encoding scheme does not contain any opportunities for data leakage or malicious input. This verification would require documentation that gives insight into the implementation used to encode and decode information in a barcode. This documentation may be used to develop a barcode reader that is able to reproduce a ballot based on the information captured within the barcode. This mitigation requires audits to be performed in every jurisdiction and in every election to ensure the barcodes only contain the necessary information.

Applies to concern(s): A, D, E,

Principle 7: Marked, Verified, and Cast as Intended, Guideline 7.3 - Voters can understand all information as it is presented, including instructions, messages from the system, and error messages.

Including the human readable version of the voter’s ballot selections gives voter’s the opportunity to verify their selections before submitting their ballots.

Applies to concern(s): B

Principle 9: Auditable, Guideline 9.1 - An error or fault in the voting system software or hardware cannot cause an undetectable change in election results.

Inclusion of the human readable selections made by a voter, allows for a way to ensure an error or fault in the reading of a barcode can be detected. This mitigation requires audits to be performed in all jurisdictions for every election using the human readable selections. When election workers/auditors are performing the audit, they will be able to reference and verify the human readable selections to confirm accurate tabulation results.

For the scenario mentioned in Concern D.1, at the polling place, the voter is given the opportunity to review, modify, and confirm their choices before printing their selections. Below are options for handling this review process:

- The voter is provided with a summary of their ballot selections and has the choice of whether to change or confirm their selections.
- The voter individually confirms each selection and is offered the opportunity to make a change before moving to the next selection. This mitigates against any coercion/vote buying that may occur prior to the voter casting their ballot.
- The voter is allowed to cast their ballot without making any selections and without being able to identify this different method of voting.

Applies to concern(s): C, D.1
The following section describes additional thoughts on the potential benefits to using barcodes in the voting system. The potential benefits do not represent a consensus opinion, but rather an aggregation of what was discussed by the cybersecurity working group.

Potential Benefits

*Note:* The following do not imply that barcodes are the only solution to these achieve these benefits. One alternative to barcodes is the use of Optical Character Recognition (OCR).

**Benefit A.** *Principle 6: Voter Privacy - Voters can mark, verify, and cast their ballot privately and independently.*

With barcodes, a voter may be able to automatically apply the necessary accessibility settings without additional assistance from an election worker. Also, a voter may be able to make their ballot selections in the comfort of their home, utilizing their own accessibility tools and storing their selections in a barcode. Then once the voter reaches the polling place, a voter can populate their selections and potentially decrease their time, placing and reviewing their votes.

**Benefit B.** *Principle 7: Marked, Verified, and Cast as Intended - Ballots and vote selections are presented in a perceivable, operable, and understandable way and can be marked, verified, and cast by all voters.*

This principle emphasizes that voting systems should support all voters. To support voters with disabilities, such as lack of sight or low vision, a barcode may be used to review ballot selections. In this instance, a voter may scan their barcode and the voting system would read the voter’s ballot selections. This allows the voter to listen and verify their selections before casting their ballot.

**Benefit C.** *Principle 9: Auditable, Guideline 9.4 - The voting system supports efficient audits.*

Barcodes may be used as a faster way to input election data for processing. Without barcodes, an election worker may have to manually input the data necessary to process a ballot including, ballot style, ballot identifiers, CVR data, etc. This could lead to increased time and effort spent processing ballots.