National Institute of Standards and Technology
U.S. Department of Commerce

VVSG 2.0 Security Requirements Overview

Gema Howell
Gema@nist.gov

EAC Public Hearing March 27, 2020

An Expanding Threat Model

Traditional Attacks

- Physically proximate
- Accidental events
- Natural disasters
- Events affecting public confidence and trust

Recent Attacks

- Nation-state
- Phishing of work and personal accounts
- Supporting election systems

"We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the US presidential election to future influence efforts worldwide, including against US allies and their election processes." – Office of the Director of National Intelligence

Innovations Since 2007

Industry

- New technologies
- Research in plain language, UX design, accessibility
- Data interchange standards
- Secure boot and strong process isolation
- Exploit mitigation technologies (e.g., ASLR, DEP)
- Stronger network protocols
- Security frameworks

Voting Systems

- Software Independence
- Risk Limiting Audits
- E2E verifiable cryptographic protocols
- Recognition that security and accessibility/usability must work together

Where to find the Security Requirements?

- The majority of the security requirements fall under Principles 9 through 15
- A few requirements that cover software security are under Principle 2
- Some areas of overlap with other principles

	Principle
9	Auditable
10	Ballot Secrecy
11	Access Control
12	Physical Security
13	Data Protection
14	System Integrity
15	Detection and Monitoring

	Principle
2	High Quality Implementation

Principle 9 – Auditable Overview

The voting system is auditable and enables evidence-based elections.

- 4 Guidelines
- 40 Requirements
- Makes software independence mandatory
- Supports for both paper-based and E2E verifiable systems
- Includes machine support for post-election audits, including support for RLA’s and compliance audits

Principle 10 – Ballot Secrecy Overview

The voting system protects the secrecy of voters' ballot selections.

- 2 Guidelines
- 20 Requirements
- New section that distinguishes ballot secrecy from voter privacy
- No voter information within the voting system and throughout the voting process
- Prevent the ability to associate a voter with their ballot selections

Principle 11 – Access Control Overview

The voting system authenticates administrators, users, devices, and services before granting access to sensitive functions.

- 5 Guidelines
- 26 Requirements
- Significant updates made to strengthen monitoring of access
  - Prevents the ability to disable logging
- Requires multifactor authentication to ensure critical operations are performed by authorized users

Principle 12 – Physical Security Overview

The voting system prevents or detects attempts to tamper with voting system hardware.

- 2 Guidelines
- 14 Requirements
- Mostly unchanged
- Ability to log physical connections/disconnections
- Physical evidence of for unauthorized physical access to a container storing voting system records
- Restricts physical access to voting system ports that accommodate removable media (CD, DVD, Floppy, thumb drives/USB)

Principle 13 – Data Protection Overview

The voting system protects sensitive data from unauthorized access, modification, or deletion.

- 4 Guidelines
- 17 Requirements
- Applies data protection of artifacts and transmitted data (e.g., digitally signed tabulation reports)

Principle 14 – System Integrity Overview

The voting system performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

- 4 Guidelines
- 30 Requirements
- Improves system integrity
  - Risk assessment, including supply chain
  - System hardening, authenticated updates
  - Secure configurations

Principle 15 – Detection and Monitoring Overview

The voting system provides mechanisms to detect anomalous or malicious behavior.

- 4 Guidelines
- 23 Requirements
- Moderately updated, including
  - Additional log types
  - Updatable and configurable detection and monitoring systems

Implications for Remote Ballot Marking

Remote Ballot Marking

- Remote Ballot Marking (RBM) is an election system for voters to mark their ballots outside of a voting center or polling place.

- The VVSG 2.0 requirements **do not apply to remote ballot marking devices and applications**. The requirements **affect only those voting system devices** that **constitute a *voting system***.

- **RBM applications need to comply with accessibility laws such as the the Access Board Information and Communication Technology Standards (Section 508) and Americans with Disabilities Act**.

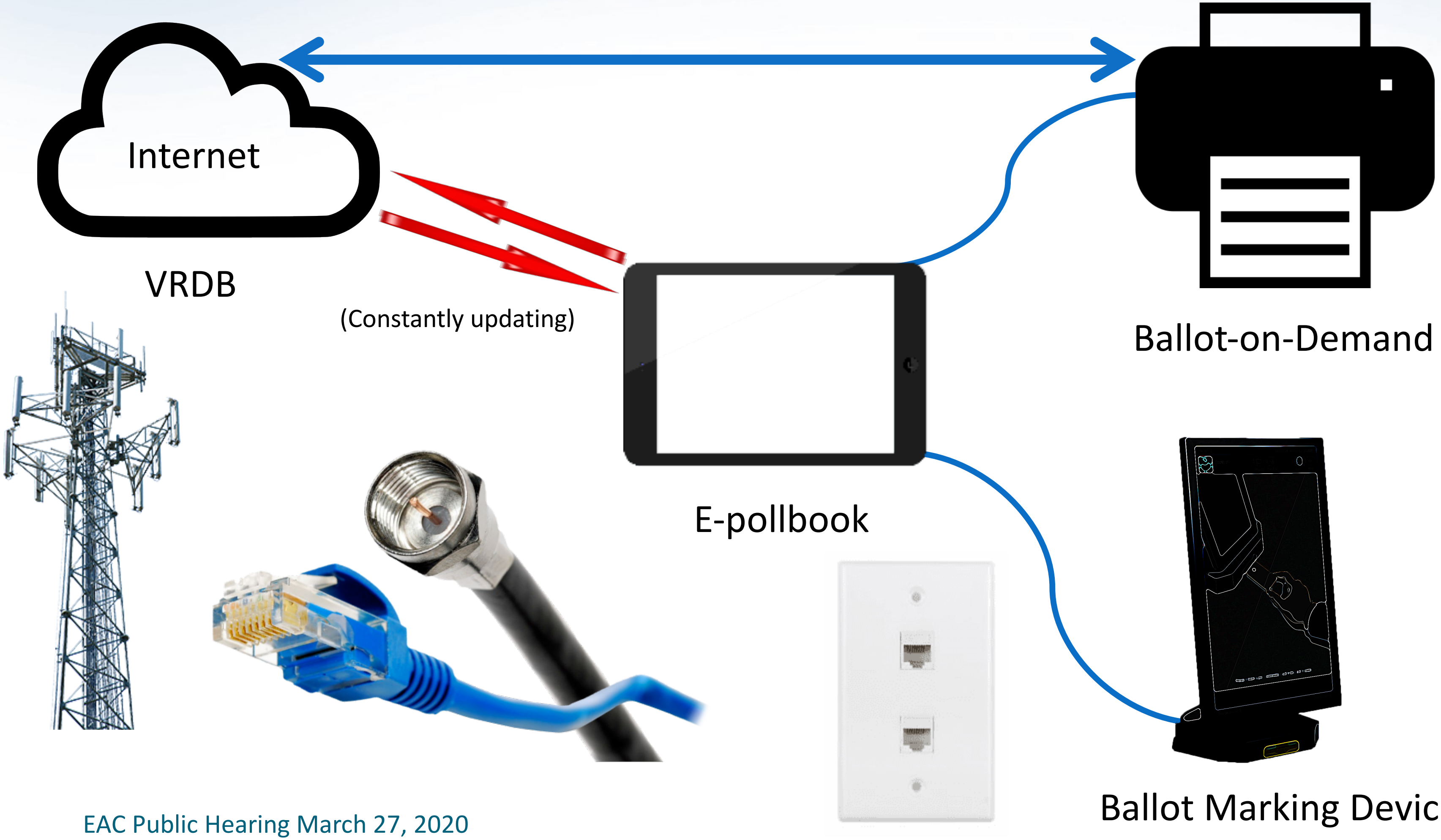
- VVSG 2.0 requirements that address the accessibility and usability for electronic interface of a remote ballot marking software application can serve as an informative resource for developers of these systems.

Implications for Network Connections

External Network Connections

Possible E-pollbooks Network Connections

External Network Communication



Internet

VRDB

(Constantly updating)

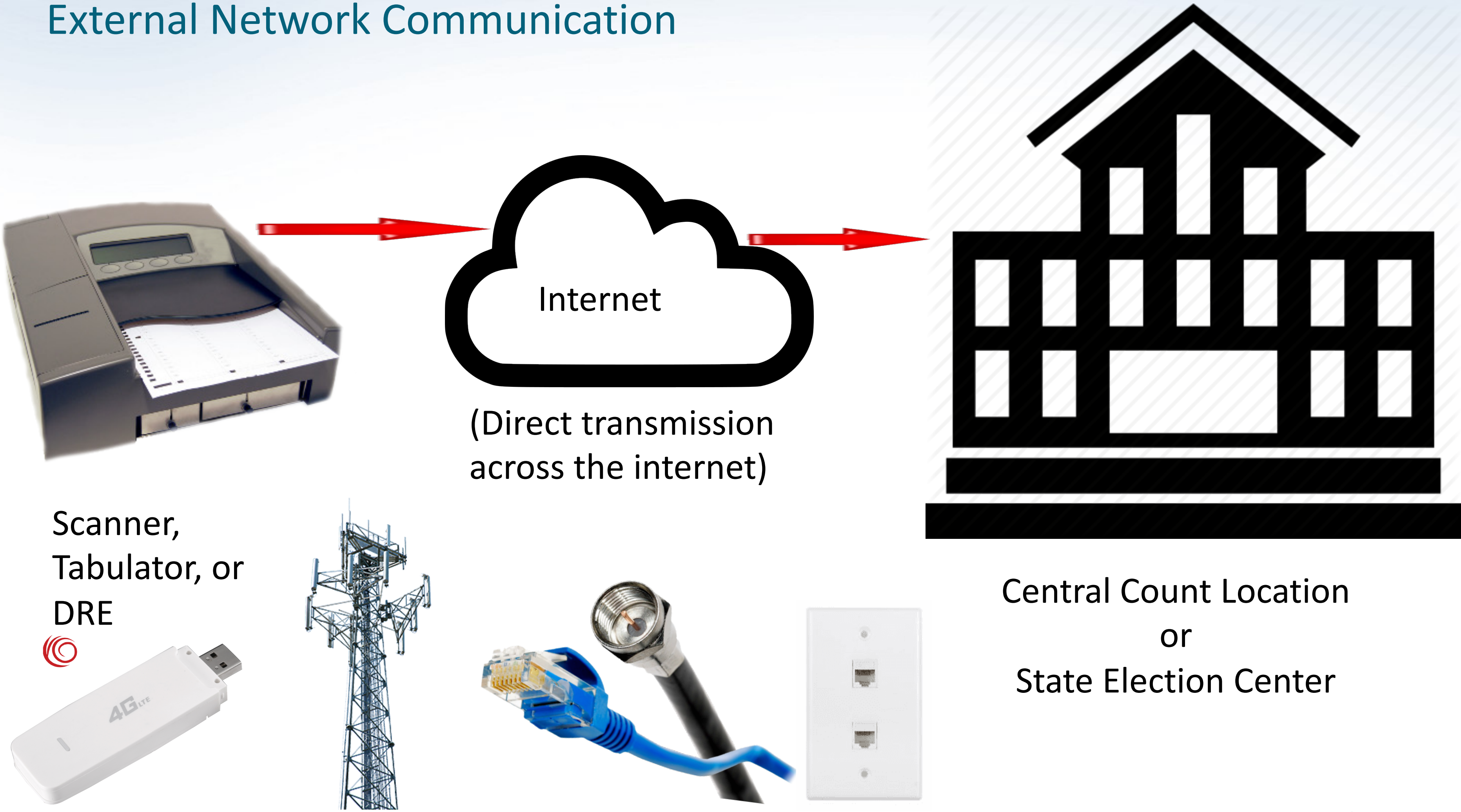
E-pollbook

Ballot-on-Demand

Ballot Marking Device

Possible Electronic Transmission Network Connections

External Network Communication



Internet

(Direct transmission across the internet)

Scanner, Tabulator, or DRE

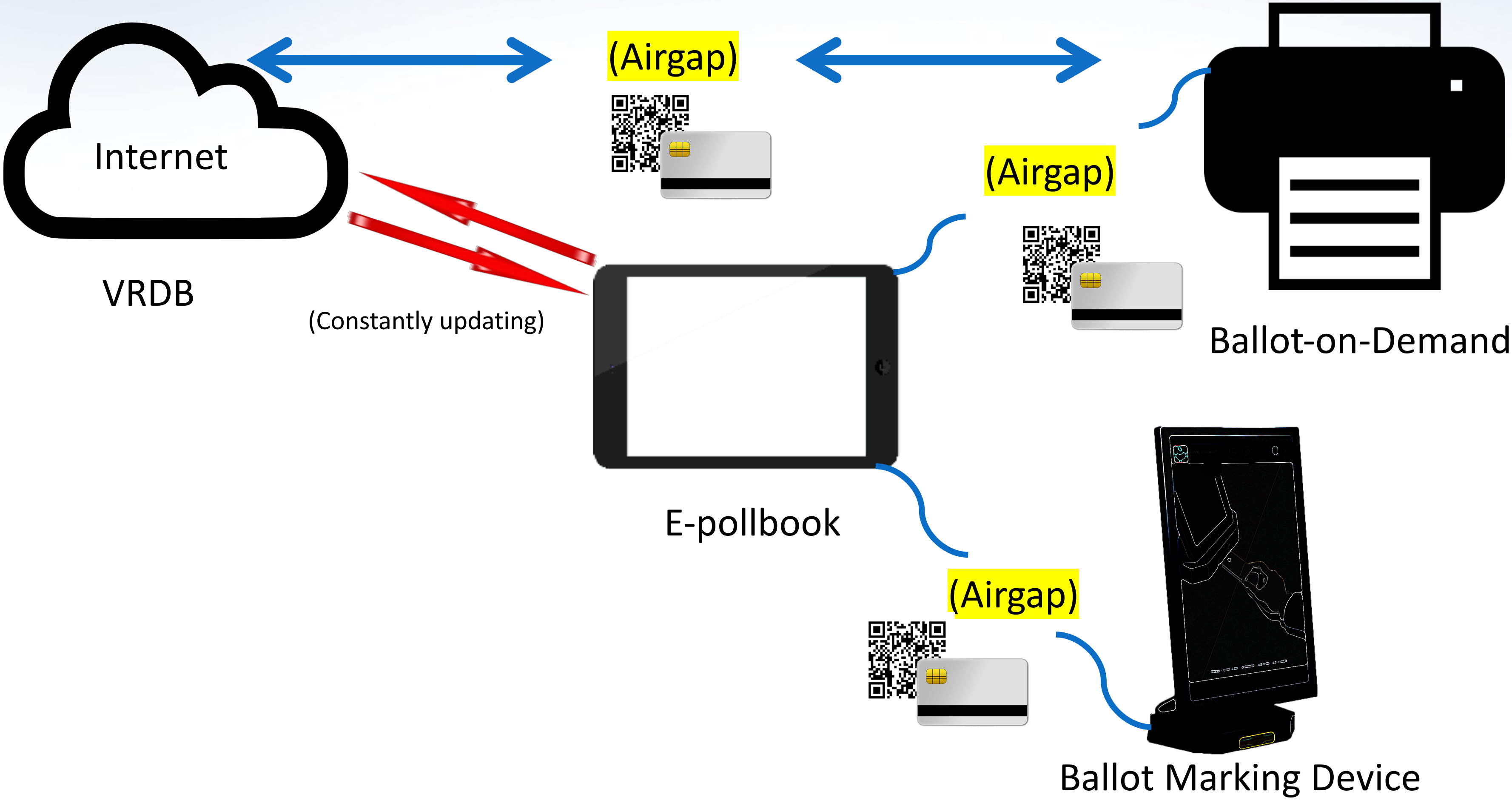
Central Count Location
or
State Election Center

External Network Connections

- The VVSG 2.0 requirements do not permit the voting system to connect to devices or components that create external network connections.
- **Security Concerns:**
  - External network connections provide access to the voting system through the Internet and thus an attack can be orchestrated from anywhere in the world (e.g., Nation State Attacks)
  - Loss of confidentiality and integrity of the voting system and election data through malware injection or eavesdropping
  - The loss of availability to access data or perform election process (e.g., ransomware attack)
- **Related Requirements:**
  - 14.2-E *External Network Restrictions*
  - 15.4-B *Secure Configuration Documentation*

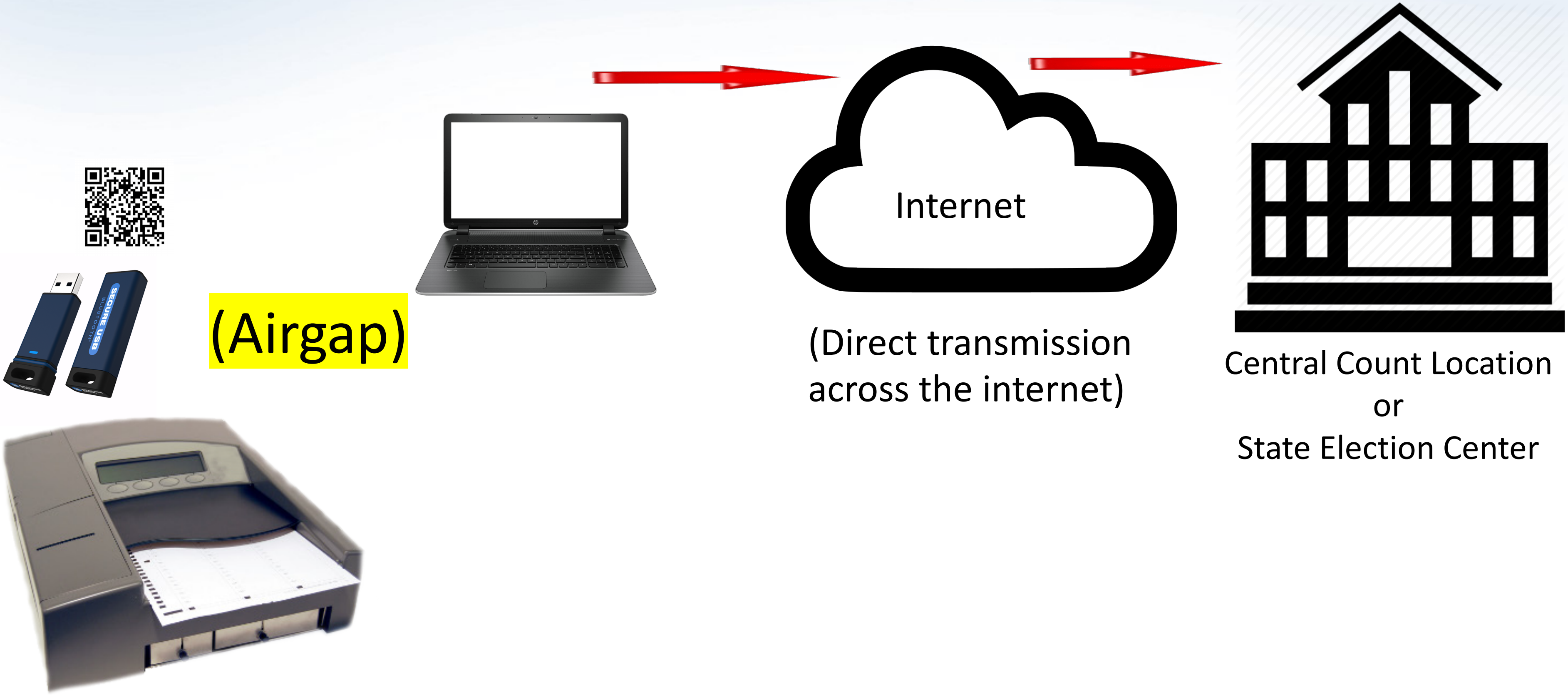
Addressing Concerns: E-pollbooks

External Network Communication



Addressing Concerns: Electronic Transmission of Results

External Network Communication



(Airgap)

Internet

(Direct transmission across the internet)

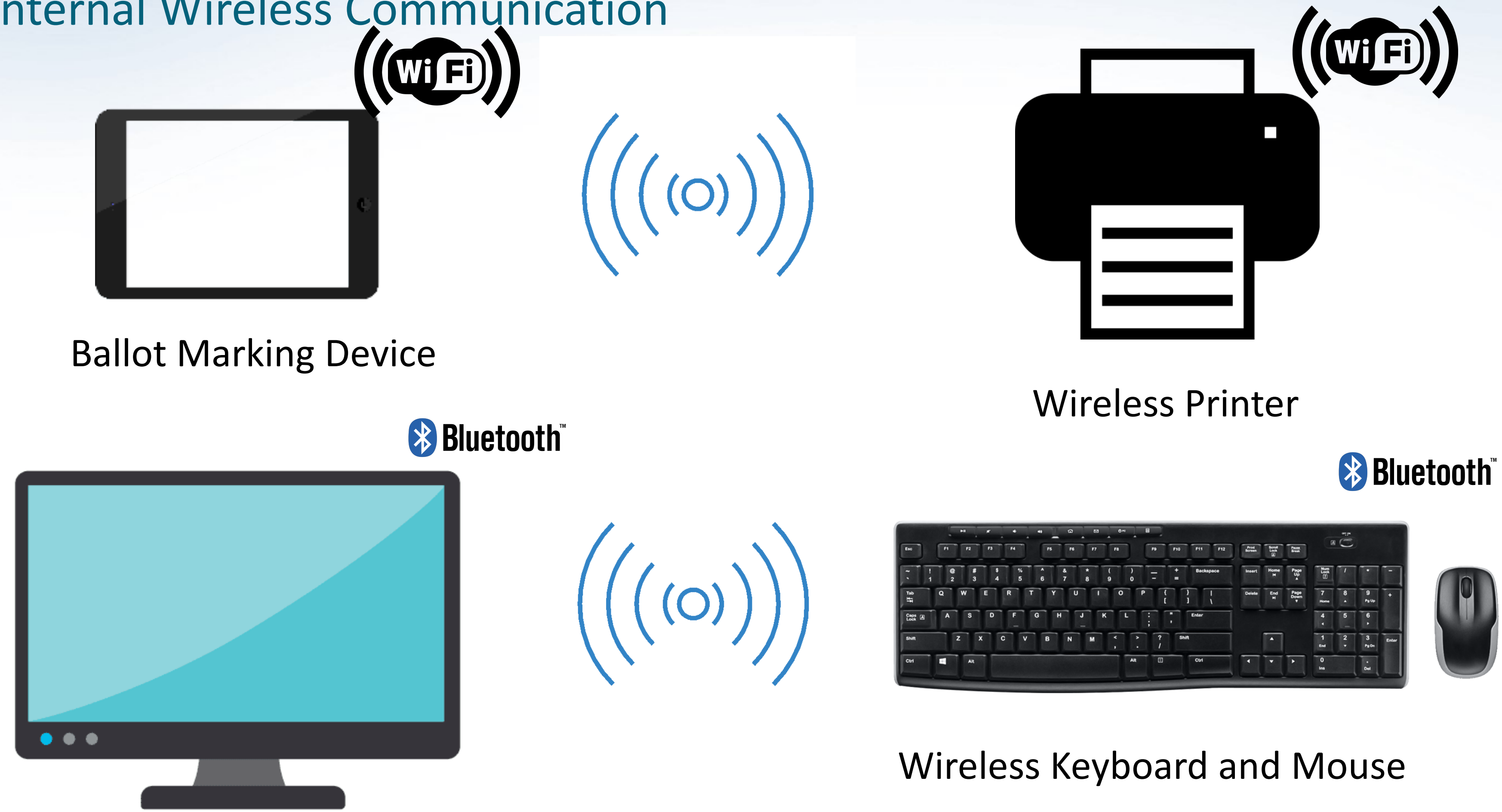
Central Count Location
or
State Election Center

Scanner,
Tabulator, or DRE

Internal
Wireless Connections

Possible Peripheral Device Communications

Internal Wireless Communication



Ballot Marking Device

Wireless Printer

Wireless Keyboard and Mouse

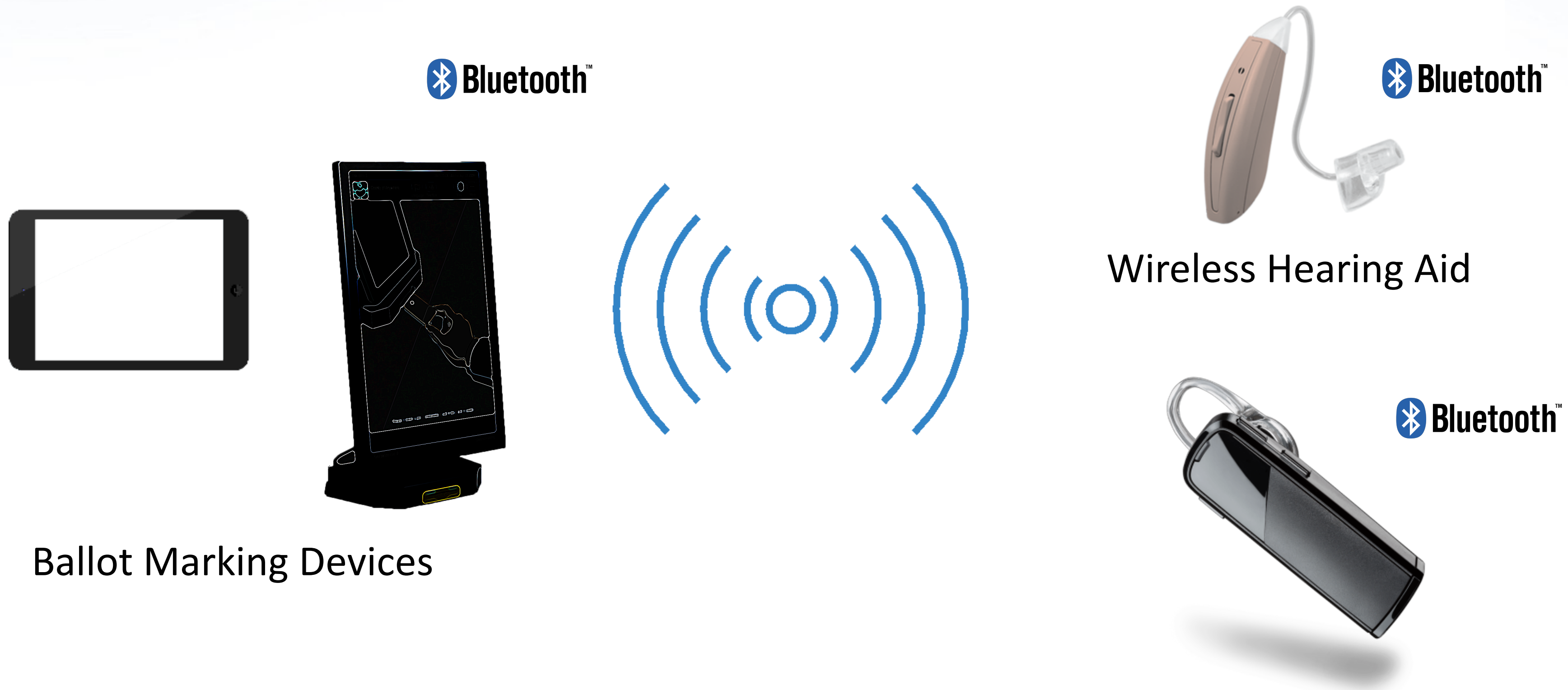
Election Management System

Possible Activation Mechanism Communications

Internal Wireless Communication

Possible Assistive Technology Communications

Internal Wireless Communication



Ballot Marking Devices

Wireless Hearing Aid

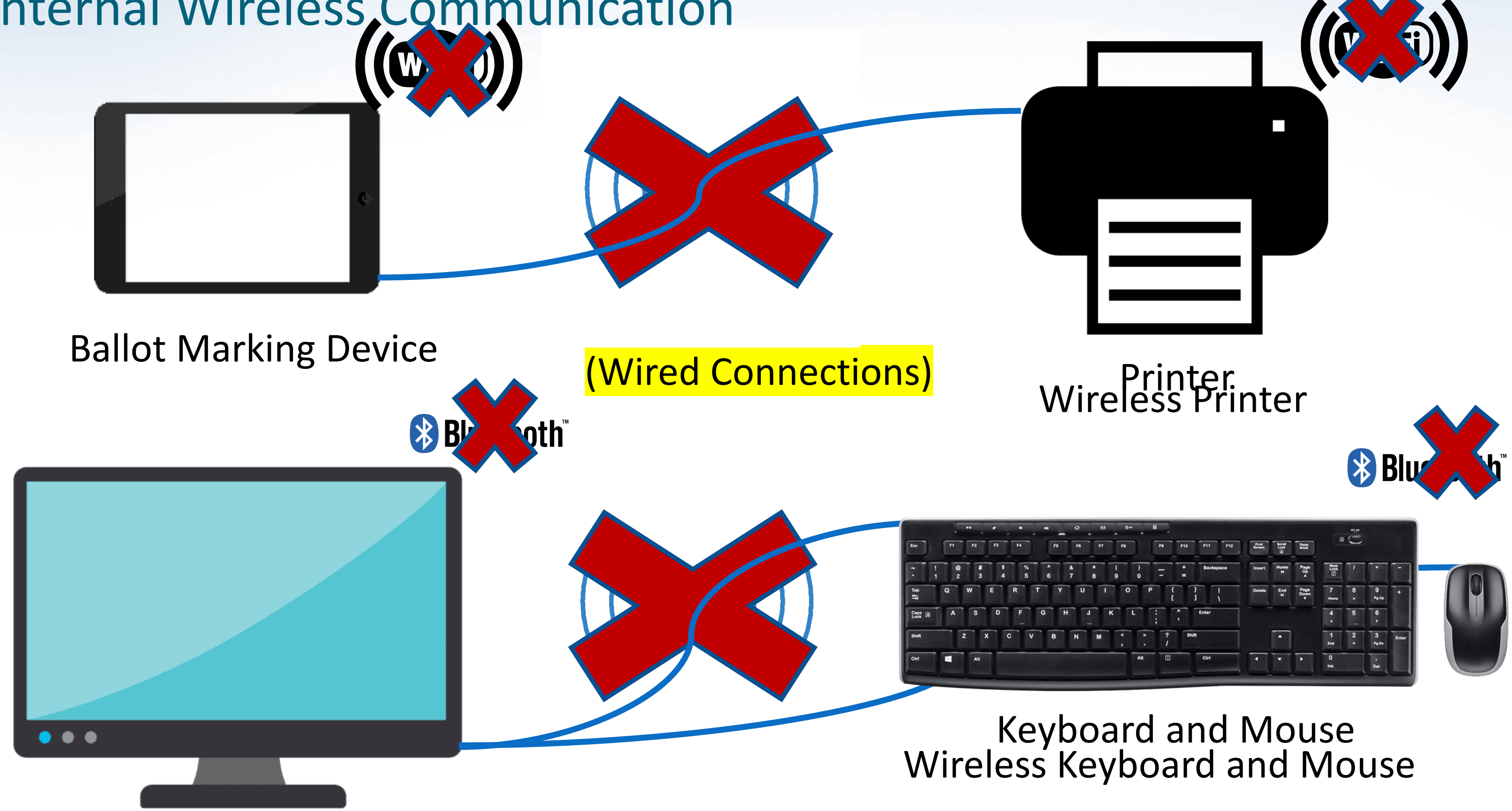
Wireless Headset

Internal Wireless Networks

- The VVSG 2.0 Requirements requires the voting system be incapable of broadcasting a wireless network.
- **Security Concerns:**
  - Provide a wireless entry point for attackers
  - Loss of confidentiality and integrity of the voting system and election data through malware injection or eavesdropping
  - The loss of availability to access data or perform election process.
  - Security configurations for wireless technologies are not equally secure
- **A voter may use their wireless personal assistive technologies (e.g. Bluetooth headset or Bluetooth hearing aid)** by using an adapter to connect to the voting system’s 3.5mm standard headphone jack.
- **Related Requirements:**
  - 14.2-D *Wireless Communication Restrictions*
  - 15.4-C *Documentation for Disabled Wireless*

Addressing Concerns: Peripheral Devices

Internal Wireless Communication



Ballot Marking Device

(Wired Connections)

Printer

Wireless Printer

Keyboard and Mouse

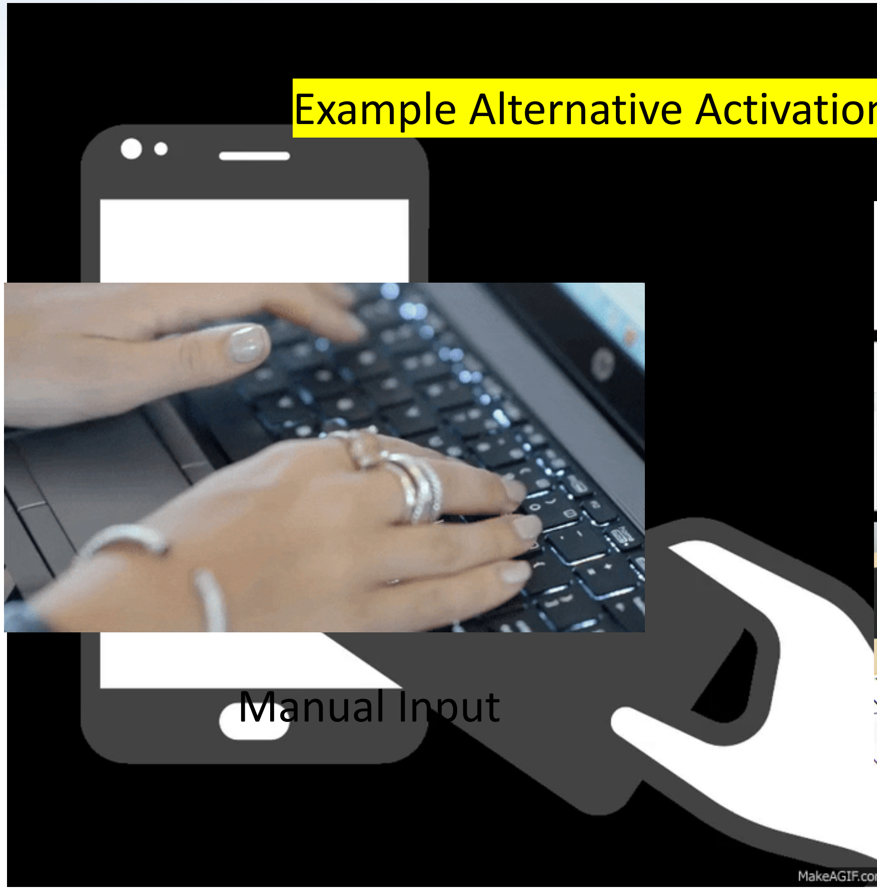
Wireless Keyboard and Mouse

Election Management System

Addressing Concerns: Activation Mechanisms

Internal Wireless Communication

Example Alternative Activation Mechanisms



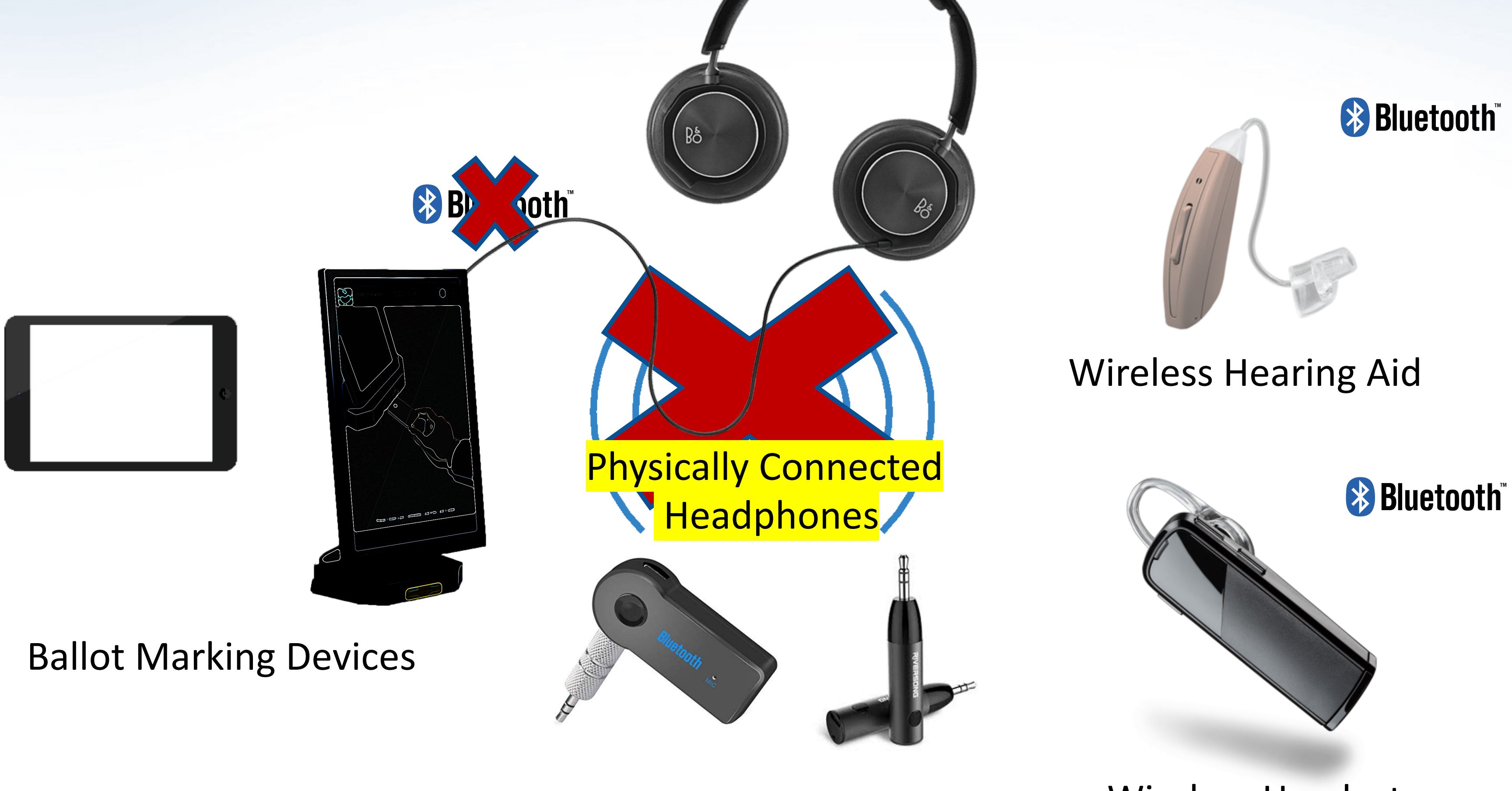
Manual Input

step 3 Choose Logistics Services (Logistics your region supports the following logistics transaction way)
Online orders
Contact their logistics
Without logistics
Company Name
Waybill number
XX快递

Scan a Barcode

Addressing Concerns: Assistive Technology

Internal Wireless Communication



Wireless Hearing Aid

Physically Connected Headphones

Ballot Marking Devices

Wireless Headset

Bluetooth Receiver

Summary

- Revised structure, organized by principle, applies to functions
- Requires security, usability, and incorporates modern practices and latest research
- Meets expectations for voter interaction, system design and development
- Accessible and secure
- Common formats for data and barcode transparency
- Requires evidence trail and records to support audits

Thank You!