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

VVSG 2.0
Network Considerations

Gema Howell
Security Engineer
Co-Chair of the VVSG Election Cybersecurity Working Group

December 18, 2019

Agenda

- Methodology
- Vendor Discussions
- External Network Connections
  - Use Cases
  - Technology Overview
  - Concerns
  - Requirements Addressing Concerns
- Internal Wireless Communications
  - Use Cases
  - Technology Overview
  - Concerns
  - Requirements Addressing Concerns

Methodology

- **Contact vendors** per the request of the TGDC
- Identify the **use cases** for devices that connect to external public networks (i.e., the Internet) and use internal wireless communications
- Understand the **technology** used by these devices to create external/internal connections
- Review **concerns** and **potential threats** to the voting system
- Provide **recommendations** to address concerns
- Review relevant **VVSG 2.0 requirements**

Vendor Discussion Overview

- Spoke with vendors
  - *3 voting systems vendors*
  - *2 e-pollbook vendors*
- Shared NIST's initial research findings and current VVSG requirements
- Discussed use cases and any concerns about the impact of the VVSG requirements
- Some states request built-in cellular modem ability to transmit election results
  - (Have ***not*** confirmed this with States)

External Network Connections

Use Cases

External Network Communication

NIST reviewed the use of external network connections in voting systems and the implications of VVSG 2.0 for the following two use cases:

- E-pollbooks that activate the ballot
- Transmission of election results

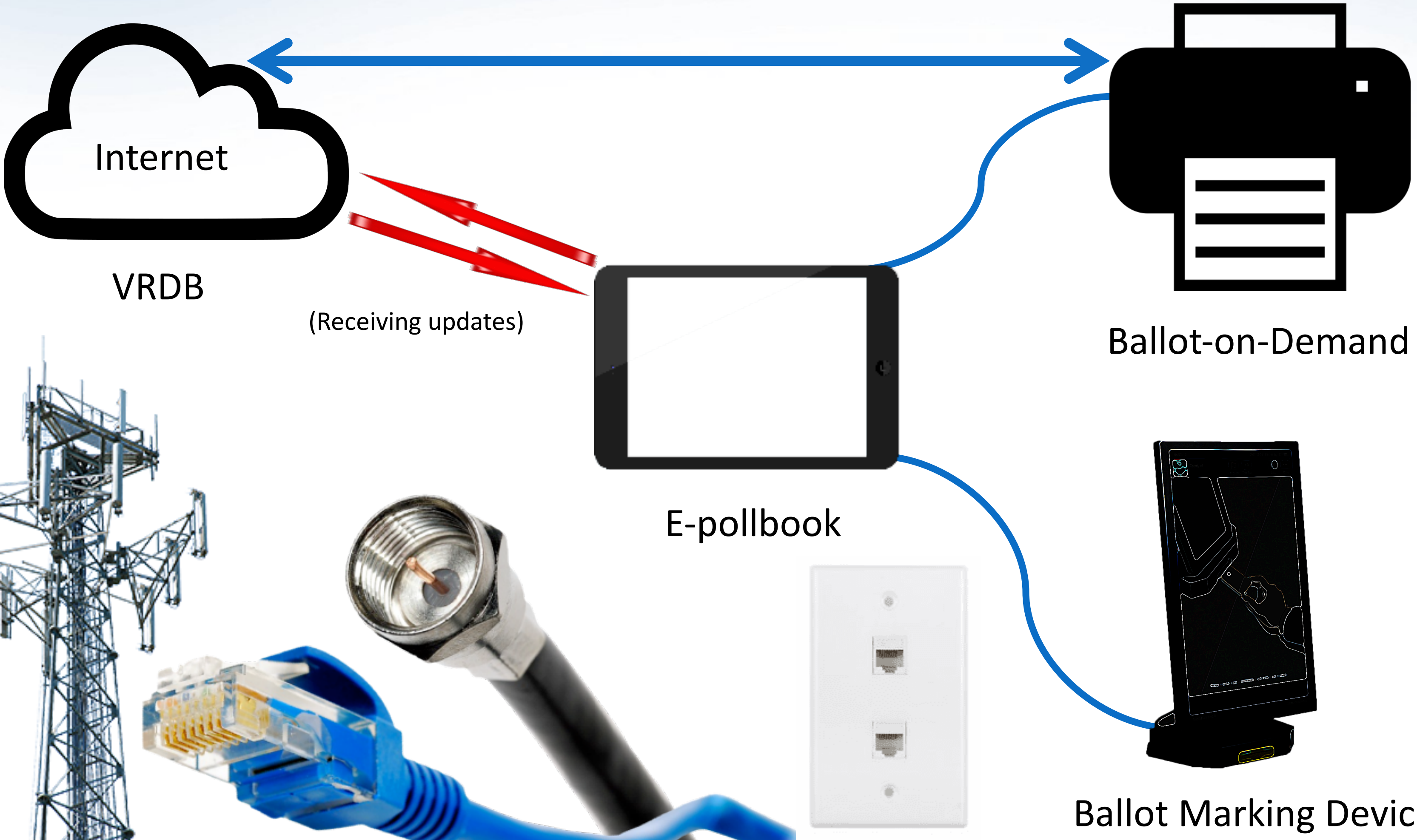
Use Case: E-pollbooks

External Network Communication

- E-pollbooks are digitized voter registry devices used to check-in voters and provide them with the correct ballot (ballot activation).
- These e-pollbooks connect to external networks to receive updates from voter registration databases (VRDB) that are commonly hosted on the Internet.
- Ballot-on Demand (BoD) devices print out a voter’s ballot with appropriate ballot style. These devices may be integrated with a networked e-pollbook and/or voter registration database.
- Ballot marking devices may be connected to e-pollbooks to activate a voter’s ballot.

Possible E-pollbooks Network Connections

External Network Communication



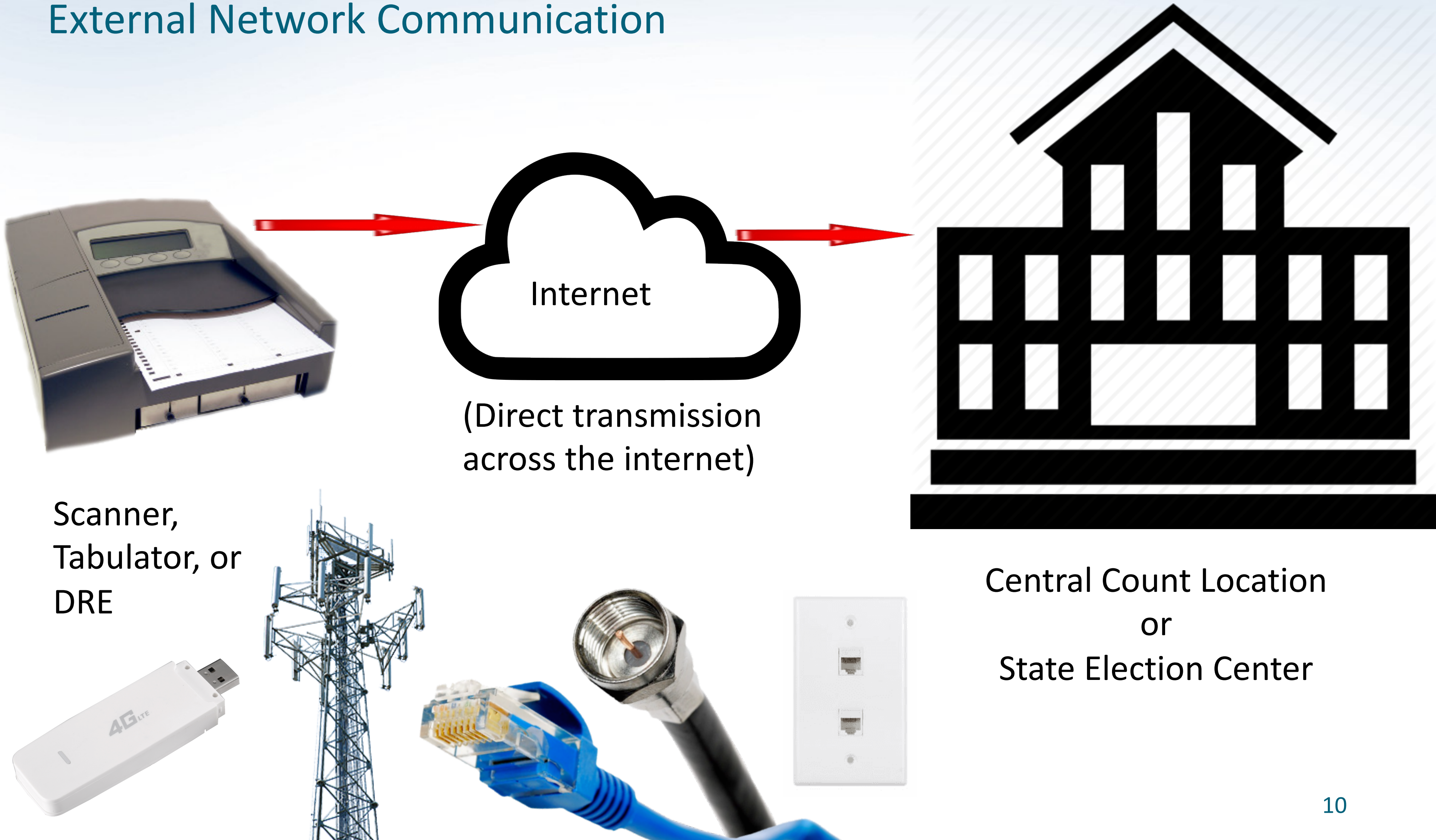
Use Cases: Transmit Election Results

External Network Communication

- Once polls close, a polling place/precinct aggregates and sends election results to the jurisdictions central count location or State election center.
- Historically, electronic transmission has occurred by placing a DRE or an optical scanner in tabulator mode, aggregating results, and then transmitting over a cellular, cable, or dial-up modem.
- The results may also be sent by physical transport (i.e., sneaker-net) of a memory device/printed report.

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

Technology Overview

External Network Communication

- To perform these use cases, the following technology is often used:
  - Cellular Networks (e.g., USB Modem)
    - Once booted begins trying to connect to a cellular network and send data over the internet
    - Connection maintained while powered on
    - Hardware/Software are COTS and not subject to source code review/software analysis by VSTL
  - Cable Modems (e.g., Comcast or Verizon Modem)
    - Wired connections (e.g., fiber or coaxial cable)
    - Always on connections exposed to many devices and users on the internet
  - Dial-up Modems
    - Originally fixed analog systems, but today may be digital and traverse many different networks, including the internet.

Concerns/Potential Threats

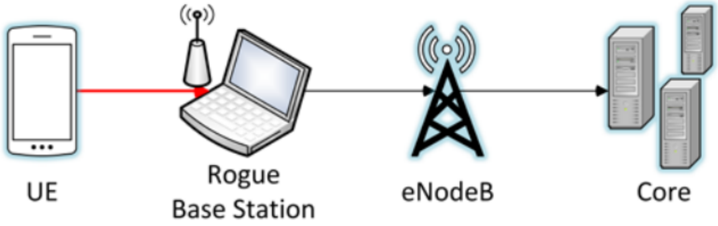
External Network Communication

- The physical connection between devices communicating over the internet and the voting system.
- This connection provides an entry way for remote attackers including Nation-state attackers.
- Loss of confidentiality and integrity of the voting system and election data through malware injection or eavesdropping.
- Loss of availability to access data or perform election process (e.g., ransomware attack).

Attack Example: Rogue Base Station

External Network Communication

- Rogue base stations impersonate cellular networks.
- A voting system with a cellular modem may attempt to connect to a rogue base station that is broadcasting at higher power levels than other cell towers.
- If the connection is successful, an attacker may be able to inject malware, modify files (e.g., tabulation results), or delete files (e.g., ballot records).



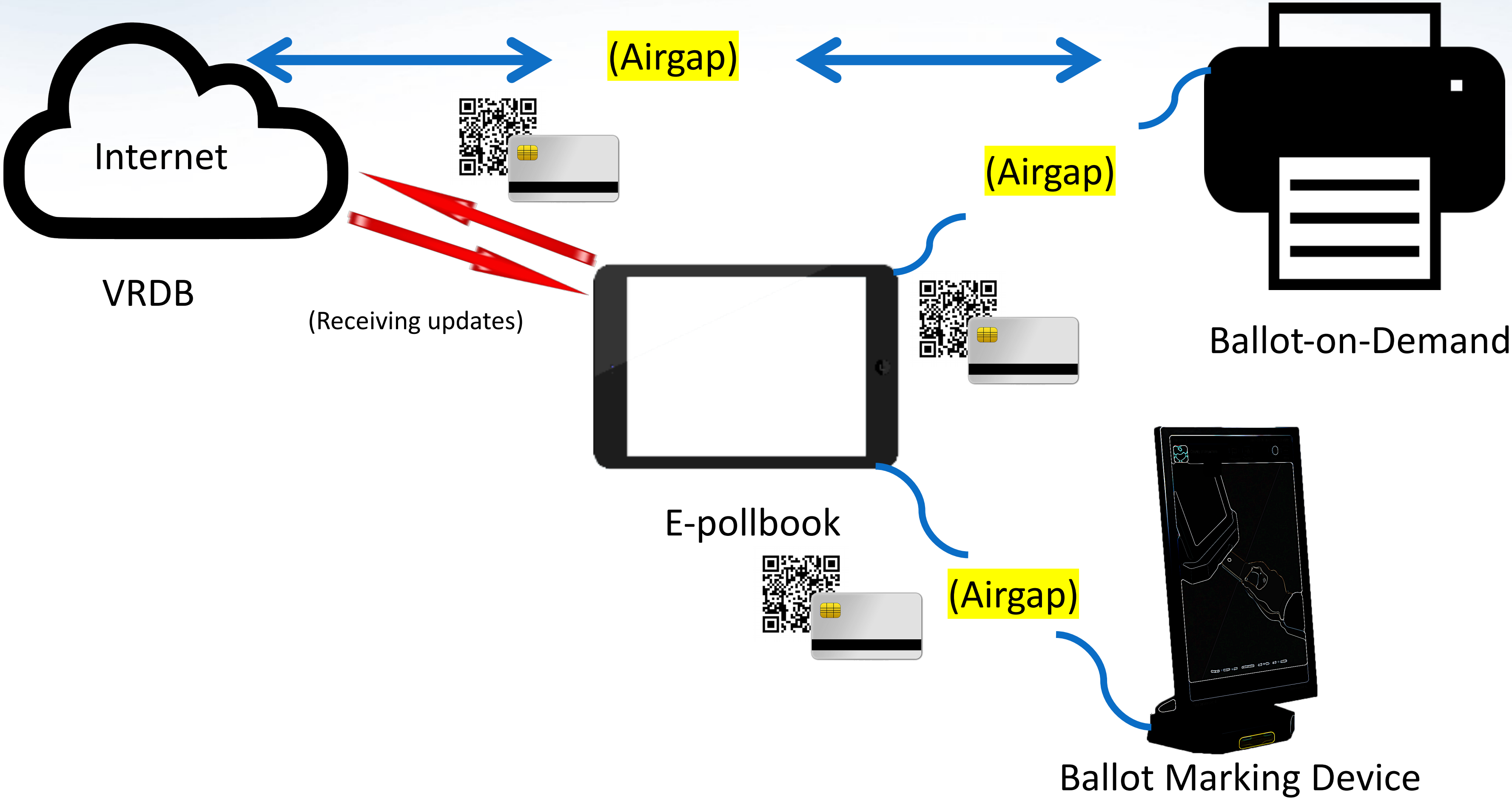
Addressing Concerns

External Network Communication

- Devices may be connected to external networks as long as they are physically isolated from the voting system.
- This can be described as an ***airgap.***
- Alternatives:
  - E-pollbooks produces a physical token to activate the ballot on a device that is on a separate network.
  - The devices used for transmitting results over an external network (i.e., the Internet) must not be on the same network as the voting system.

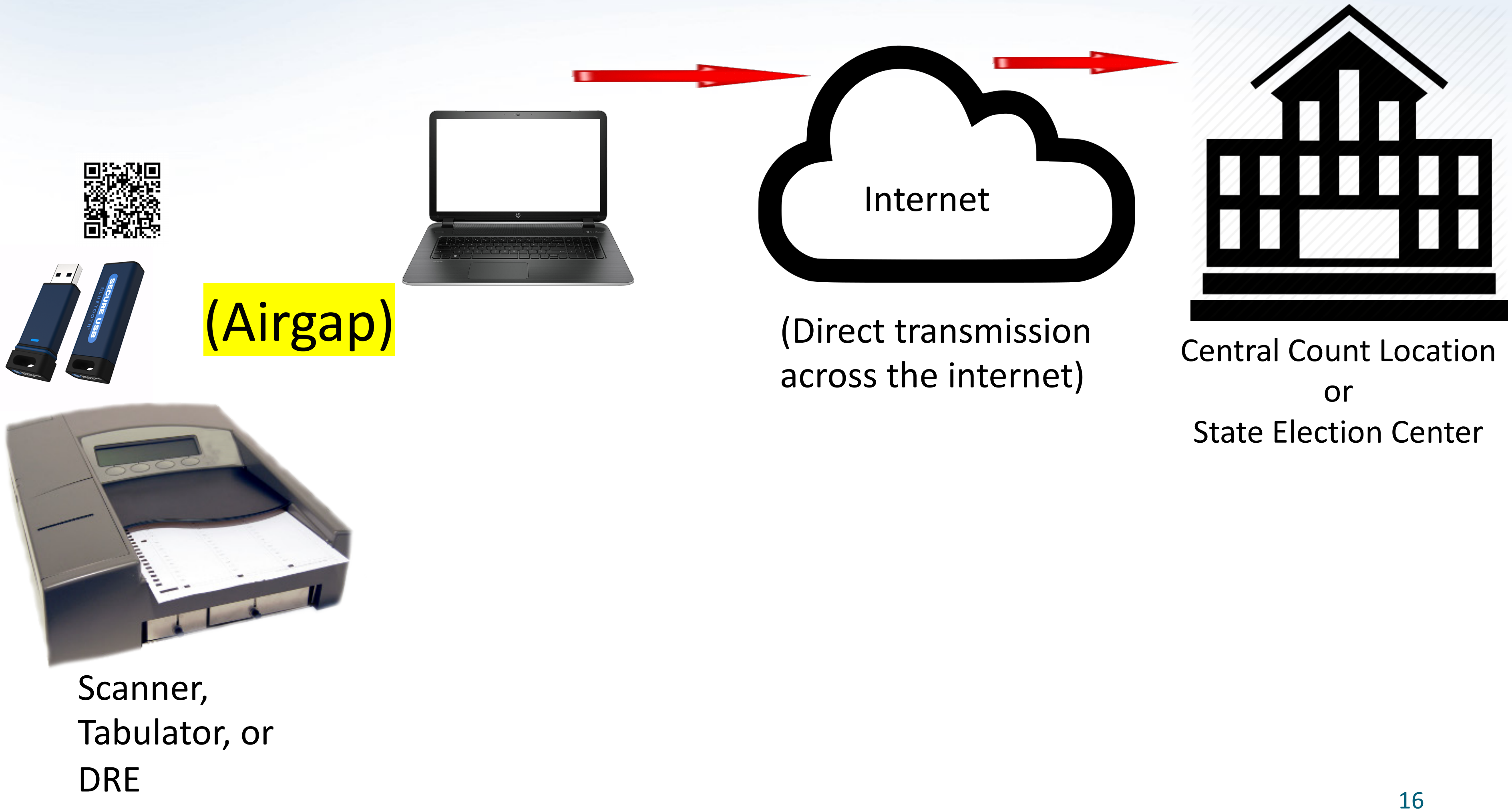
Addressing Concerns: E-pollbooks

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

VVSG 2.0 Requirements

External Network Communication

- **14.2-E – External Network Restrictions**

A voting system must not be capable of…

1. establishing a connection to an external network
2. connecting to any device that is capable of establishing a connection to an external network.

- **15.4-B – Secure configuration documentation**

The voting system documentation must list security relevant configurations and be accompanied by network security best practices.

Internal Wireless Communications

Use Cases

Internal Wireless Communication

NIST reviewed the use of internal wireless communication in voting systems and the implications of VVSG 2.0 for the following three use cases:

- Peripheral Input/output Devices
- Activation Mechanism
- Assistive Technology

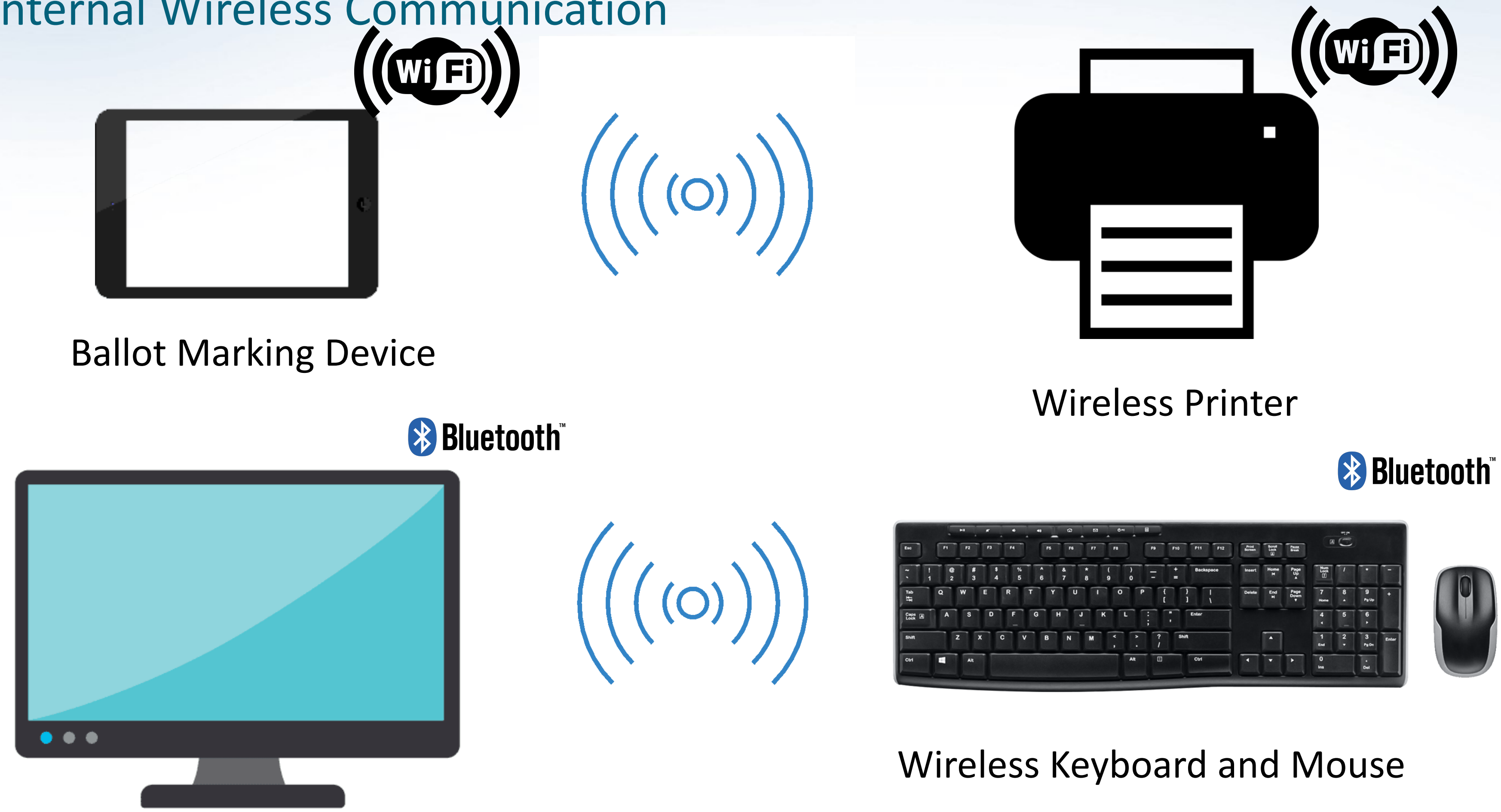
Use Cases: Peripheral Devices

Internal Wireless Communication

- Peripheral Input/output Devices communicate with the voting system using wireless technology
- Once paired with a voting system then can be used to input data (e.g. wireless keyboard) or output data (e.g., wireless printer).
- These peripheral devices may be provided by a voting system vendor or brought into the polling place by an election worker.
- These peripheral devices often use Wi-Fi or Bluetooth wireless technology.

Possible Peripheral Device Communications

Internal Wireless Communication



Ballot Marking Device

Wireless Printer

Wireless Keyboard and Mouse

Election Management System

Use Cases: Activation Mechanism

Internal Wireless Communication

- To activate a voter’s ballot, the voting system needs the activation information from an e-pollbook.
- This activation information may be stored on an activation card.
- The activation card may communicate with a ballot marking device via wireless technology to activate a voter’s ballot.
- Near-field communication (NFC) is the wireless technology may be used in the activation cards.

Possible Activation Mechanism Communications

Internal Wireless Communication

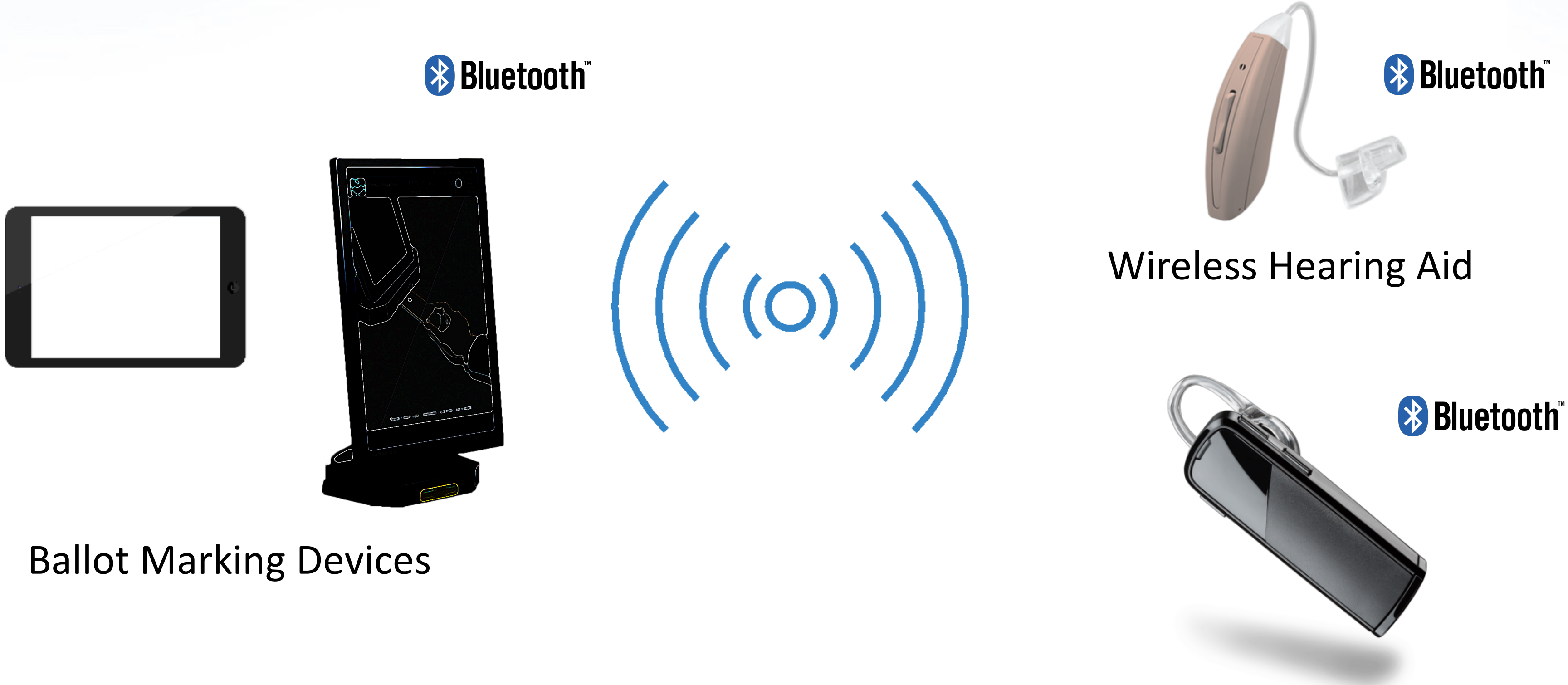
Use Cases: Assistive Technology

Internal Wireless Communication

- Voting systems must allow voters to use their personal assistive technologies.
- These personal assistive technologies may use wireless technologies to interact with the voting system.
- There is a growing trend towards using wireless technologies, such as a Bluetooth headset or hearing aid.

Possible Assistive Technology Communications

Internal Wireless Communication



Ballot Marking Devices

Wireless Hearing Aid

Wireless Headset

Technology Overview

External Network Communication

- To perform these use cases, the following technology is often used:
  - Wi-Fi
    - Used in wireless local area networks (WLANS), which are a group of devices wirelessly connected to a network that is restricted to a limited geographical area
  - Bluetooth
    - Short range, low power, wireless communication protocol that creates small wireless networks known as personal area networks (PANs)
  - Near-field communication (NFC)
    - Of the wireless technology discussed here, NFC has the shortest range of wireless communication, which is typically less than 4 inches.

Concerns/Potential Threats

Internal Wireless Communication

- Devices using wireless over-the-air (OTA) communication signals that are vulnerable to interception.
- Wireless OTA communication creates a point of entry for attackers within close range.
- Internal wireless communications have concerns similar to external network connections, at a shorter range:
    - Loss of confidentiality and integrity of the voting system and election data
    - Loss of availability to perform election functions and access election data
    - Loss of ballot secrecy if voter's ballot activation card is compromised
    - Lack of technical expertise required to securely configure wireless technologies

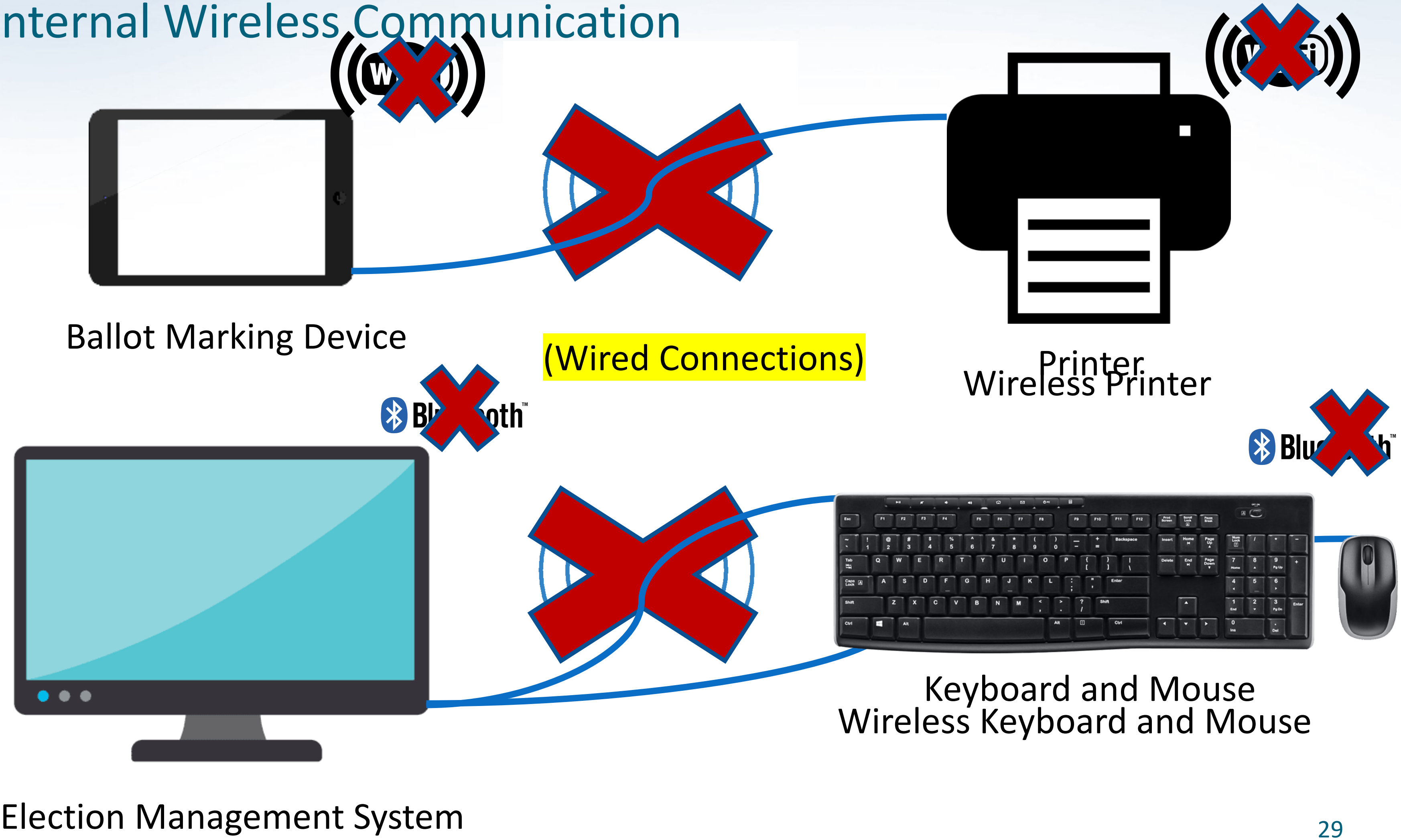
Addressing Concerns

Internal Wireless Communication

- Physical wired connection only
- Limit the attack surface by disabling wireless communication capability
- This does not preclude the use of voter's personal assistive technologies within the polling place.
  - A voter may use a Bluetooth headset by attaching an adapter to the voting system's 3.5 mm headphone jack.

Addressing Concerns: Peripheral Devices

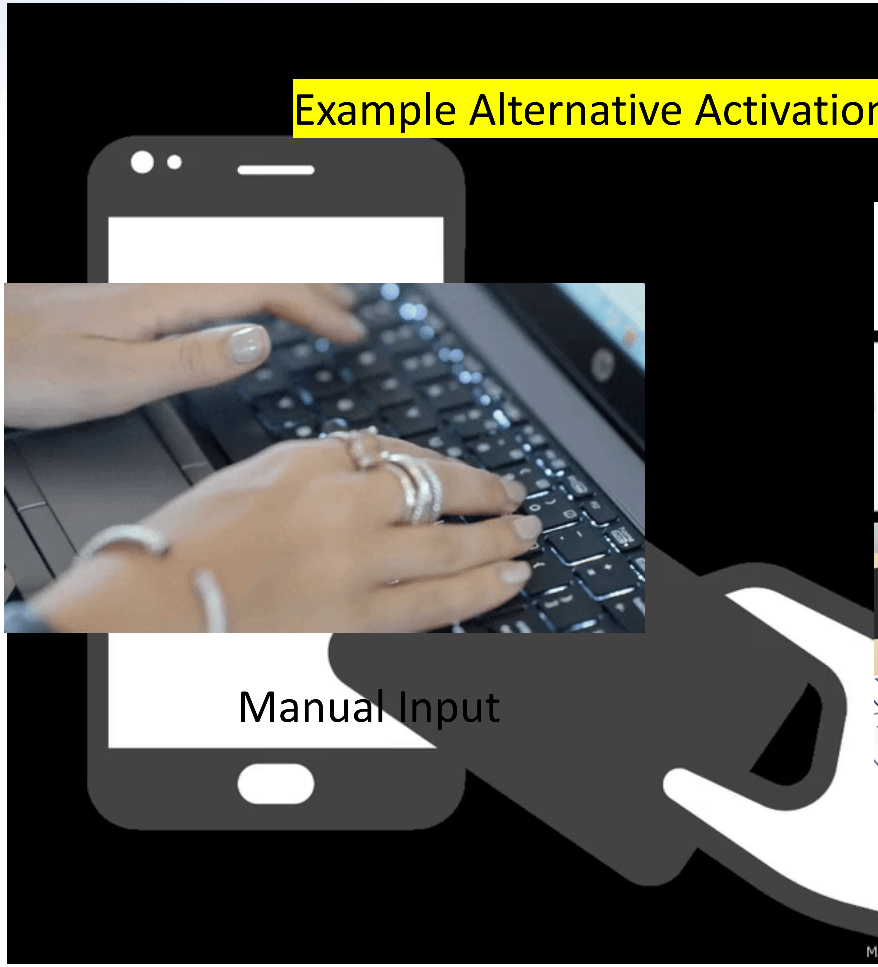
Internal Wireless Communication



Addressing Concerns: Activation Mechanisms

Internal Wireless Communication

Example Alternative Activation Mechanisms



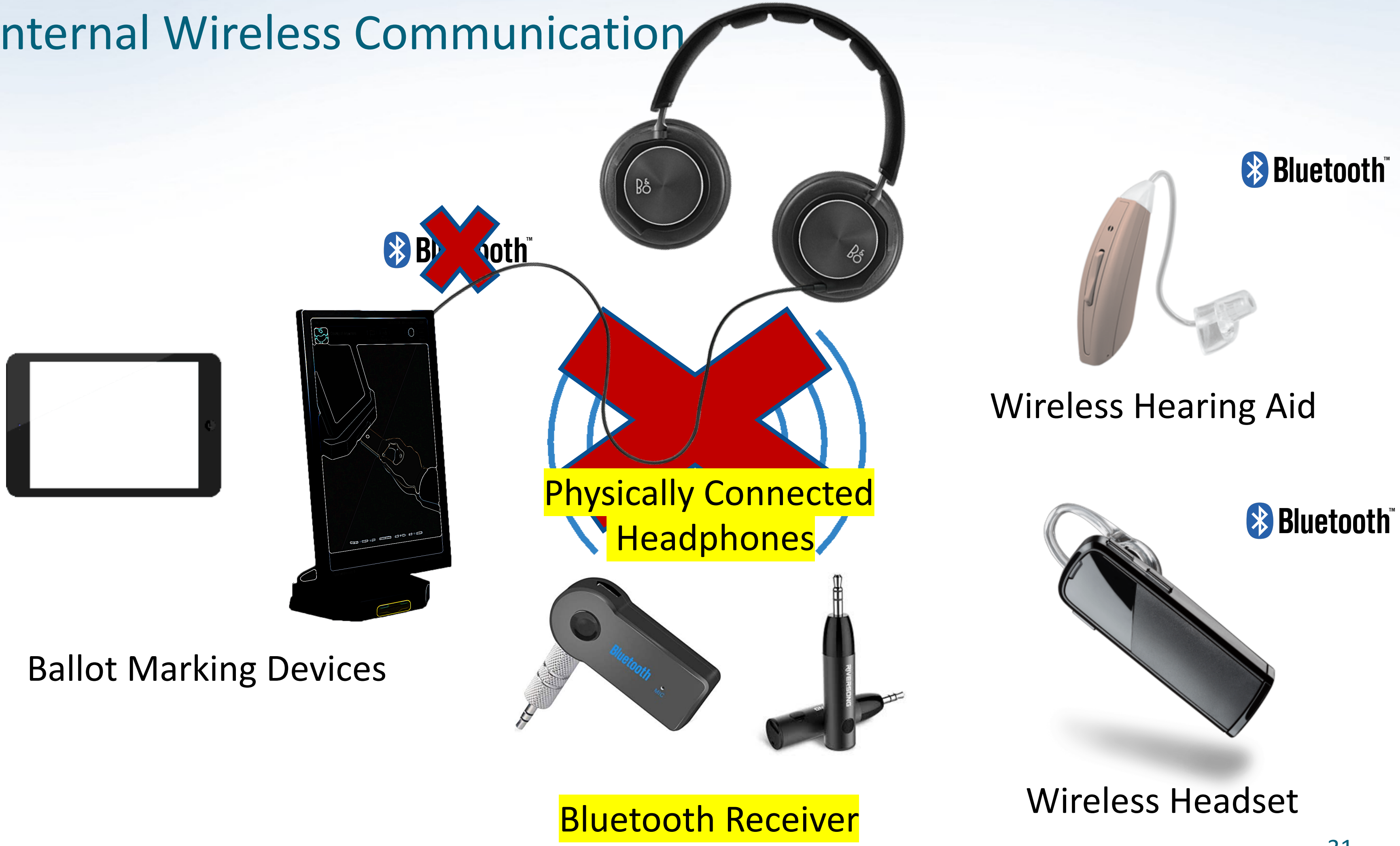
Manual Input

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



Ballot Marking Devices

Physically Connected Headphones

Bluetooth Receiver

Wireless Hearing Aid

Wireless Headset

VVSG 2.0 Requirements

Internal Wireless Communication

- **14.2-D – Wireless Communication Restrictions**

Voting systems must not be capable of establishing wireless connections.

- **15.4-B.1 – Disable wireless secure configuration documentation**

The voting system documentation must list security relevant configurations and other necessary information for disabling the use of wireless technology within the voting system.