Ballot and Asset Chain of Custody:

The Foundation for Election Security, Recounts, and Audits

> In addition to cybersecurity, the key to election security, timely election conclusion, and smooth audits and recounts is leveraging technology through systematic ballot and asset tracking, backed by chain of custody visibility, and process management enforcement.

Wireless Data
Systems, Inc.

INTRODUCTION

State chief elections officials, usually secretaries of state or lieutenant governors are responsible for the safeguarding of voter records and ensuring the integrity and security of the overall election process in their state. While much of the day-to-day operational functions are handled by local elections administrators, the state chief elections official ultimately bears the responsibility of public confidence in elections. This perception is not only based on election results, but also the perception of the entire election process.

Much of the discussion around elections security has been focused – and justly so – on cybersecurity. From electronic voting machines to jump drives and even communications, cybercrime is a real threat to democracy. Efforts to address cybercrime hacking is only part of a complete election security program. The program should also include systems and protocols for handling election assets, particularly ballots.

In addition to cybersecurity, the key to **election security**, **timely election conclusion**, and smooth **audits and recounts** is leveraging technology through systematic **ballot and asset tracking**, backed by chain of custody visibility, and **process management enforcement**.

According to the U.S. Election Assistance Commission:
"The most common method for tracking voting system assets in jurisdictions is still a manual comprehensive inventory using a spreadsheet." And: "Automated tools, including processes that integrate IT barcode scanning software that update into a system asset database can allow you to have an accurate, current inventory at all times." (*Managing Election Technology: Ten Things to Know About Managing Aging Voting Systems. EAC. October 2017*)

ELECTION SECURITY THROUGH PHYSICAL SECURITY

Physical assets are potential access points to cybersecurity; therefore, security and protection of these physical elements (voting systems, ballots, memory devices, etc.) remains critical to maintaining a secure, but open election process.

According to The U.S. Elections Assistance Commission (EAC), physical election security refers "to standards, procedures, and actions taken to protect voting systems and related facilities and equipment from natural and environmental hazards, tampering, vandalism, and theft." (*Election Management Guidelines Chapter 3: Physical Security. EAC.*)

A physical security approach should begin with a collective review of each county's current elections procedures and processes. This includes chain-of-custody procedures and inventory control/asset management. Every touch-point should be reviewed to ensure ballots and assets are secured and tracked throughout the entire election cycle.

The review will likely identify potential gaps where chain of custody, oversight, and human error can lead to a security breach. These gaps should be addressed with a combination of physical security tactics (access, cameras, tamper-proof seals, etc.), documented policies and procedures, and an elections-specific system to help manage, control, and provide visibility to every election-critical asset and process.

TIMELY ELECTION CONCLUSION

At the conclusion of an election, ballots should be validated and properly secured. Election equipment must be accounted for, sealed, and returned. If using thumb drives, it is critical these are properly processed to ensure a timely and accurate tabulation. Every county should have a systematic way to know when these assets are returned from voting precincts in real time. A dashboard is an ideal way for elections administrators – and even secretaries of states offices – to track and identify any precincts with issues or delayed results.

Closely managing the supply chain and logistics of voted ballots and tabulation data, will not only encourage public trust, but also ensure an efficient uneventful post-election. This includes initial results tabulation reporting and post-election audits and recounts.

As the US population is expected to grow by 15-20 million by the year 2025, there will be roughly 250,000,000 people of voting age. A constantly growing population increases strain on current elections logistics. Election night and post-election collection of ballots and tabulation data remains the most time-critical and highly watched aspect that will be negatively impacted should a state not invest now in resources and technology to help manage election conclusion

AUDITS AND RECOUNTS

Close elections may require tabulated ballots to be efficiently and accurately recounted. The requirements for accurate election results demand that ballots are in the correct location at the proper time, without questions to their authenticity. If questions arise, it is important to have complete chain of custody history for ballots, tabulators, and all critical assets.

In the 2018 General, Florida was faced with a statewide recount. Miami-Dade, the state's largest county, was able to quickly conduct a timely and successful recount due largely to accurate and accessible data stored by a system that accounted for every ballot, its location, and full chain of custody history.

BALLOT AND ASSET TRACKING

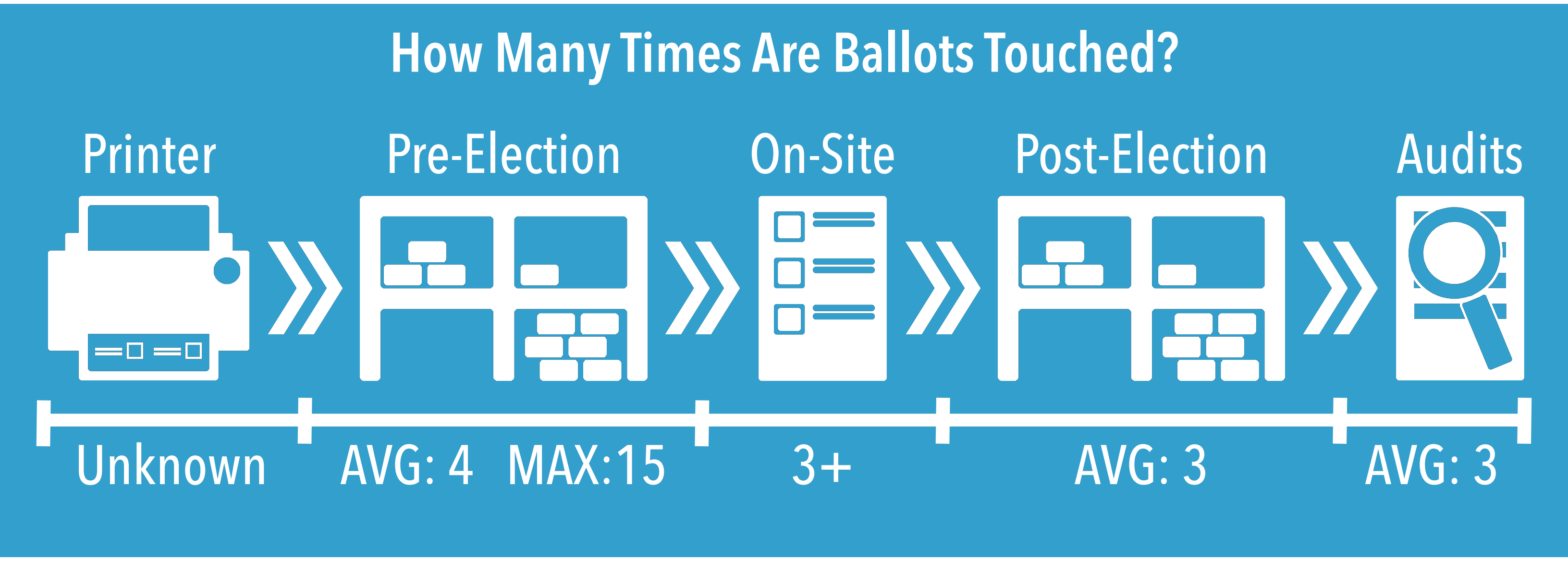
According to the EAC, election officials should maintain an accurate inventory including the following:

- Voting devices (including thumb drives)
- Administrator and ballot activation devices
- Seal envelopes
- Voter registration (poll) lists
- Election result tapes and printouts
- Field supervisor and rover reports
- Poll worker daily logs
- Reconciliation reports
- Audit data
- Voting Equipment Delivery Sheets

This is an extensive list that necessitates the use of technology to manage and store data. For example, consider the average ballot can be handled by over 20 different people through the lifespan from ballot printing through the election and ultimately stored and retrieved for audits.

"It's always good practice to have a procedural system to check who has done what, and when. 'Chain of custody' requirements come into play when there are any movements or actions relating to ballots, poll books, equipment and just about anything else." (*Election Security: A Priority for Everyone. National Conference of State Legislators. July 2017.*)

Every movement should be tracked and logged. The log data must be accessible to help address any issues in a timely fashion.



How Many Times Are Ballots Touched?

Printer	Pre-Election	On-Site	Post-Election	Audits
Unknown	AVG: 4 MAX:15	3+	AVG: 3	AVG: 3

PROCESS MANAGEMENT ENFORCEMENT

Even if every county in your state has implemented the EAC's best-practices, physical elections security will still fail without process management enforcement. Consider the following inherent challenges constantly faced by election departments:

- Ensuring bipartisan, 2-deep teams at every ballot touch-point
- Managing turnover in warehouse, transportation, and other logistical staff
- Recruiting and training poll workers where poll worker population remains skewed toward older Americans

Enforcement of physical security processes requires diligent effort on behalf of the entire election department. The most-effective way to keep everyone on task is to implement a system that will make it easy – even for the newly hired or physically challenged personnel – to follow correct procedures.

An elections-specific system will ensure the appropriate and correct number of individuals complete every process task while maintaining a log of every transaction. If a process is not completed per policy, the system sends notifications so that parties can remedy or mitigate the situation in a timely manner. A properly implemented system can prevent a process failure from becoming a security breach.

Lastly, an elections-specific system will assist with contingency policies as a result of elections disruptions such as voter turnout variances, equipment failures, and even natural disasters. A real-world example is having a voting machine go down at one precinct. This can quickly have a domino effect throughout other precincts if there is no systematic way to repair or replace it on the fly. Every county should have a system in place that would notify, locate, and reroute the appropriate personnel and equipment to mitigate the impact of the unforeseen.

CONCLUSION

Visibility into every aspect of the election cycle is critical to security. Having a comprehensive set of procedures is only the first step of protection. In order to maintain public trust, every procedure must be validated. Every ballot and physical asset movement must be tracked and logged. That data must be available in real-time and readily accessible to address issues and any resulting media or citizen inquiries.

Challenges in knowing the location and integrity of ballots and critical assets at any point in time can be avoided through planning and use of systems designed specifically for election logistics and security. A statewide implementation of such a system can help standardize and enforce processes, save in administrative costs, and most importantly, improve overall elections security.

ABOUT WDS:

Founded in November of 1990, Wireless Data Systems, Inc. (WDS) has over 25 years of experience in successfully designing and implementing complete software and hardware solutions for some of the most well-known corporations in America. Headquartered in Boca Raton, Florida, WDS specializes in software development for mobile, enterprise-wide real-time, data collection and validation. We have extensive experience in supply chain management solutions for critical security-sensitive and time-sensitive inventory and assets.

In 2006, we implemented our first election-specific system for Miami-Dade County in Florida. Over the years, our systems have expanded to an entire software suite centering around ballot, asset, and physical security.

Wireless Data
Systems, Inc.