CRITICAL INFRASTRUCTURE SUBSECTOR	Election Systems
SUBJECT	Tabulation Method Comparison
COMPONENT SCOPE	Tabulators
RISK LEVEL	Elevated
ELECTION RECORDS IMPACTED	Voter Registration Data, Poll Worker Data, Vote Tallies and Results

1 Introduction

Vote tabulation methods have changed over the years. In recent years, the use of electronic voting systems to tabulate vote totals has gained prominence. Electronic voting systems introduces unique risks to the conduct of elections. Cyberattacks, power outages, and malicious insider threats due to the inability of the general public to monitor the vote tally process are all unique to the tabulation of votes using electronic voting systems. In exchange for accepting these new risks, the general public is told that the use of electronic voting systems is necessary to provide faster results at less cost. This technical advisory will examine whether or not the perceived benefits outweigh the risks.

2 Background

2.1 Hand Counts

Hand counting of paper ballots was the original and primary method of vote tallying in American elections from the country's founding through much of the 19th century. The use of standardized paper ballots printed by the government and counted by hand began in 1789, shortly after the establishment of the United States.

A major innovation came in 1858 with the introduction of the Australian ballot system, which was first adopted in Massachusetts in 1888. This system used government-printed ballots that were distributed at polling places and required voters to mark and return them immediately, enhancing security and standardization.

Without introducing any of the incremental risks posed by electronic voting systems, the cost of hand counts all across the country has been estimated to be on the order of $62M per year.[1]

Using the method promoted by Cause of America, 50-100 ballots per hour can be counted depending upon the number of measures on each ballot.[2]

If hand counts are performed with video surveillance that shows clear pictures of each ballot, there is no longer any need for expensive recounts. Unlike machine-based counts, the tabulation operations are fully transparent for all to see.

2.2 Analog Voting Machines

The first mechanical lever voting machine was patented in 1889 and first used in Lockport, New York in 1892. By 1930, lever machines were used in almost every major U.S. city. This marked the beginning of a shift away from hand counting in many areas.

In 1898, lever voting machines cost $550 each, which is equivalent to about $11,600 in today's dollars[3]. These machines were described as being "built like bank vaults" and weighing about as much.

[1] Source: Calculations used calculator posted at https://causeofamerica.org/Post/hand-counting-simplified
[2] Source: Handcounting.com/eManual
[3] Source: https://www.smithsonianmag.com/smithsonian-institution/pulling-lever-tallied-vote-98774074/

Another approach to analog voting machines is punch card voting machines as featured in the "dangling chad" election of 2000. The Votomatic punch card system, introduced in 1965, sold for $185 per machine (equivalent to about $1,547 today)[4]. This was considered much more affordable than lever machines, allowing jurisdictions to place more voting machines in each polling place.

The high cost of lever voting machines (over $11,000 in today's dollars) was one factor that led to their eventual replacement with more affordable technologies like punch card and optical scan systems. The expense of moving, storing, and maintaining lever machines also made them increasingly unpopular with budget-conscious officials.

2.3 Electronic Voting Systems

The functional components of a modern electronic voting system as defined by the Cybersecurity Infrastructure Security Agency (CISA) in their July 2020 Critical Infrastructure Security and Resiliency Note that pertain to the counting of votes are defined in Figure 1.

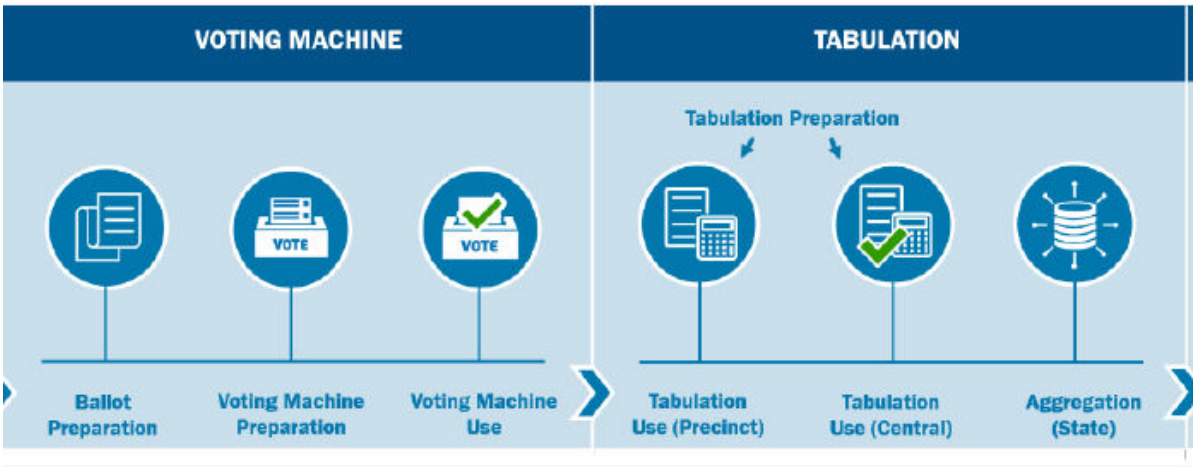

Figure 1 Election System Functional Ecosystem (Critical Infrastructure Security and Resilience Note Page 2)

In this report, CISA went on to address the confidentiality consequences, integrity consequences, and availability consequences of risks unique to electronic voting systems (See Figure 2). These consequences were significant as highlighted by the ability to change the results of vote tabulation or prevent the tabulation of votes altogether.

[4] Source: https://www.csg.org/2023/11/08/election-technology-through-the-years/

ELECTION COMPONENT	CONFIDENTIALITY CONSEQUENCE	INTEGRITY CONSEQUENCE	AVAILABILITY CONSEQUENCE
Voting Machine Preparation	Change Voting Machine Functionality to Expose Voter Choices	Change Voting Machine Functionality (Presentation of Ballot/Recording of Choices)	Prevent Voting Machine Functionality
Tabulation Preparation	Change Tabulation Machine Functionality to Expose Results	Change Tabulation Machine Functionality	Prevent Tabulation Machine Functionality
Voting Machine Use	Expose Voter Choices	Change Voting Machine Functionality	Prevent Voting Machine Functionality
Tabulation (Precinct)	Expose Tabulation Results Before Intended	Change Results of Vote Tabulation	Prevent Vote Tabulation
Tabulation (Central)	Expose Tabulation Results Before Intended (Aggregation)	Change Results of Vote Tabulation (Aggregation)	Prevent Vote Tabulation (Aggregation)
Aggregation (State)	Expose Aggregation Results Before Intended	Change Results of Vote Aggregation	Prevent Vote Aggregation

Figure 2 Electronic Voting System Risk Consequences

In an attempt to mitigate some of these risks, the Federal government has created the Election Assistance Commission (EAC) and Election Integrity Information Sharing Analysis Center (EI-ISAC) at an annual cost of $103M and $43M respectively.

The Federal government, however, does not conduct our elections. States and local units of government do. The annual expenditures by state, county and local government across the United States are more difficult to compile, but we do have some rudimentary data. As of 2019, Dominion held a 37.3% market share[5] and roughly $107M in sales in the lead up to the 2020 election. Based upon these figures, the total state and local government cost for electronic voting systems in the United States at roughly $287M for the 2020 election. This yields a total cost of ~$433M for the 2020 election not including the cost of various support contracts provided by companies such as Runbeck and Election Source who are typically hired by government officials to configure these complex systems prior to elections.

3 Impact

3.1 Confidentiality

On March 1, 2022, Former Wisconsin Supreme Court Justice Michael Gableman release an investigative report on the "apparatus and procedures of the Wisconsin election system" known as "The Gableman Report"[6]. The Gableman Report indicates that Michael Spitzer Rubenstein of the National Vote at Home Institute (NVAHI) appears to have had extensive and potentially improper

[5] Source: https://about.bgov.com/news/voting-machine-firms-add-lobbyists-amid-election-hacker-concerns/
[6] Source: https://electioncrimebureau.com/wp-content/uploads/2024/10/Special-Counsel-Gableman-Report.pdf

access to election records and processes in Green Bay, Wisconsin during the 2020 election. Specifically:

- He had access to absentee ballot data and requested detailed information on returned and outstanding ballots by ward.
- He was given access to set up wireless networks at the central count location, including a hidden network without a password.
- He had unrestricted access to the central count area on election day.
- He was involved in transporting ballots to central count on election day.
- He appeared to be making decisions about which ballots would be counted, noting in an email that some ballots were delayed arriving but would likely be counted because no one had challenged them when they came in late.
- He was given access to develop procedures and instructions for central count workers.
- He was involved in assigning poll workers and inspectors to locations.
- He requested and may have received access to WisVote voter data that is not typically shared with outside groups.

The report suggests this level of access and involvement by an outside consultant to confidential information was improper and potentially unlawful under Wisconsin election laws. While Rubenstein was brought in as part of a grant program, the report argues he and other outside groups were given privileged access that went beyond what should have been allowed for non-government employees in administering the election.

Breaches of confidential information regarding elections does not need to be accomplished by compromising electronic voting systems directly. Any system connected to the same network used by voting systems potentially has access to this data as well. Such was the case with Poll Chief Software developed by Konnech. On October 4, 2022, Eugene Yu, the CEO of Konnech Corporation, was arrested on suspicion of theft of personal identifying information (PII) of election poll workers. The company was responsible for managing software used in Los Angeles County for election poll worker management[7].

According to the Los Angeles County District Attorney's Office, Konnech was contracted to securely maintain the data of poll workers and ensure that only United States citizens and permanent residents had access to it. However, investigators found that contrary to the contract terms, this information was allegedly stored on servers in the People's Republic of China[8].

3.2 Integrity

Elections in Williamson County, Tennessee were affected by an anomaly in Dominion voting systems during a local election on October 26, 2021[9]. This anomaly resulted in valid ballots being incorrectly sorted into a provisional ballot category. The issue was detected by poll officials, who noticed that the number of votes cast in half the precincts did not match the number of ballots received.

During the 2020 election in Antrim County, MI, initial results indicated that the perennial Republican County was won instead by Joe Biden. Upon further investigation by election officials, it was determined that there was a 7,060 vote flip from Donald Trump to Joe Biden between the initial and final certified results. The error was attributed by the MI Secretary of State to “user

[7] Source: https://da.lacounty.gov/media/news/head-election-worker-management-company-arrested-connection-theft-personal-data
[8] Source: https://www.theregister.com/2022/10/05/konnech_election_software_china/
[9] Source: https://www.eac.gov/news/2022/04/01/eac-issues-report-tennessee-voting-system-anomaly

error"[10] however court exhibits provided during the subsequent Bailey v Antrim County lawsuit revealed evidence of a vote shifting algorithm not only on Antrim County, MI but also in Barry County, MI[11].

During the 2022 primary election in DeKalb County, GA, Board of Commissioners candidate Michelle Long Spears was initially reported to have received only 2 votes in the entire district, including zero votes in her own precinct. It was later discovered that Spears had been shortchanged 3,792 votes due to a technical error in the voting system[12]. Instead of losing the contest, it was revealed via hand count that Spears had in fact won the contest.

3.3 Availability

During the 2022 election, 60 out of the 223 voting locations in Maricopa County, AZ reported machine outages that prevented voters from casting ballots during the election[13].

On February 14, 2024, a group of Mercer County, NJ residents filed a 360 page complaint with compelling evidence of systemic failures in Dominion Voting Systems machines that stripped them of fundamental voting rights.[14]

A global Microsoft-based computer outage crippled electronic voting systems in Arizona's two largest counties during the February 2024 election.[15]

During the August 2022 primary election in Michigan, 65 out of 83 counties reported modem issues that delayed the reporting of results.[16]

4 Risk Mitigation Strategy

If state law permits the removal of electronic voting systems, election officials should:

- Remove electronic voting systems
- Define and implement hand count procedures (See Cause of America Hand Count Guide for reference)
- Maintain local voter rolls on equipment that is not connected to the internet

If state law mandates the use of electronic voting systems, election officials should:

- Define a disaster recovery plan that features a plan for hand counts if needed (See Cause of America Hand Count Guide for reference)
- Implement strong access controls and authentication for election databases
- Conduct regular security audits to detect vulnerabilities
- Follow NIST guidelines for protecting sensitive election data

---

[10] Source: https://www.michigan.gov/-/media/Project/Websites/sos/30lawens/Antrim_Fact_Check.pdf?rev=7a929e4d262e4532bbe574a3b82ddbcf

[11] Source: https://www.depernolaw.com/all-expert-reports.html

[12] Source: https://www.nytimes.com/2022/06/06/us/politics/michelle-long-spears-georgia.html

[13] Source: https://www.nbcnews.com/politics/2022-election/vote-machine-glitch-roils-arizonas-maricopa-county-fuels-false-stateme-rcna56261

[14] Source: https://www.thegatewaypundit.com/2024/02/exclusive-mercer-county-nj-residents-file-lawsuit-against/

[15] Source: https://www.votebeat.org/arizona/2024/07/19/microsoft-windows-crowdstrike-outage-arizona-primary-early-voting-disruption/

[16] Source: https://www.wxyz.com/news/democracy-2022/election-results-delayed-65-michigan-counties-reporting-modem-issues

- Use paper records: Ensure the electronic voting system creates a voter-verified paper audit trail (VVPAT) or paper ballot for every vote cast. This provides a physical backup that can be used to audit and verify the electronic results
- Conduct post-election audits: Perform risk-limiting audits after the election, manually comparing a statistically significant sample of paper records to the electronic tallies to confirm accuracy
- Implement strong access controls: Use multi-factor authentication, enforce the principle of least privilege, and carefully manage user accounts and passwords for anyone accessing the voting systems
- Air gap systems: Keep voting and tabulation systems completely disconnected from the internet or other external networks
- Use dedicated hardware: Have dedicated servers and workstations used only for election-related tasks, not general computing
- Secure physical access: Implement strict physical security controls for voting equipment, including locks, tamper-evident seals, and chain of custody procedures
- Perform pre-election testing: Conduct thorough logic and accuracy testing of all voting equipment before use
- Use trusted builds: Ensure voting system software comes from a trusted, verified source
- Maintain backups: Regularly backup election data and store securely offsite
- Train staff: Provide cybersecurity awareness training to election officials and workers
- Have an incident response plan: Develop and practice cybersecurity incident response procedures
- Work with partners: Collaborate with federal, state and local cybersecurity partners like CISA for support and best practices

5 Conclusion

The use of electronic voting systems to conduct elections introduces significant election integrity risks in exchange for the false promise of speed and efficiency. Hand counts can provide the same vote tally function without the risks and for significantly less cost.