CRITICAL INFRASTRUCTURE SUBSECTOR	Election Systems
SUBJECT	Machine-Based Vote Manipulation
COMPONENT SCOPE	Election Management Systems
RISK LEVEL	High
ELECTION RECORDS IMPACTED	Vote Tallies and Results

1 Introduction

Electronic voting systems have several potential vulnerabilities not found with hand counts. If these vulnerabilities were exploited, the election results could be manipulated resulting in certification of fraudulent results. In order to secure our elections from such exploits, significant security rigor is required. If election officials have insufficient expertise or desire to enforce such rigor, serious consideration must be given to whether or not the risk of the security vulnerabilities introduced by electronic voting systems outweighs their perceived benefits.

2 Background

Here are some of the key ways electronic voting systems could be or have been compromised:

2.1 Software Vulnerabilities

2.1.1 Malware infection

Malicious software could potentially be installed on voting machines or election management systems to alter vote counts. This could occur through physical access to machines or remote hacking.[1]

2.1.2 Insecure connections

Some voting systems have modems that connect to cell networks and the internet, creating potential entry points for hackers.[2]

2.2 Hardware Vulnerabilities

2.2.1 Physical tampering

With physical access, an attacker could potentially alter hardware components or install devices such as flash drives to manipulate votes.

2.2.2 Supply chain attacks

Compromised hardware components could be introduced during manufacturing or distribution.[3]

2.3 Data Transmission and Storage Issues

2.3.1 Man-in-the-middle attacks

Vote data could be intercepted and altered as it's transmitted from machines to central tabulators.[2,4]

[1] In Plaintiff Exhibits 10 and 11 in the William Bailey v Antrim County, MI lawsuit, expert Jeffrey Lenberg demonstrated evidence of a vote-shifting algorithm in Antrim County, MI and Barry County, MI. See https://www.depernolaw.com/all-expert-reports.html

[2] See Technical Advisory on Internet Connections at https://electioncrimebureau.com/wp-content/uploads/2024/09/Technical-Advisory-Internet-Connections.pdf

[3] China is a central figure in the supply chain for electronic voting systems as evidenced in Plaintiff Exhibit 5 in the William Bailey v Antrim County, MI lawsuit. See https://www.depernolaw.com/all-expert-reports.html

[4] The Center for Internet Security (CIS) effectively operates as a “trusted” Main-in-the-middle. See Technical Advisory on the CIS at https://electioncrimebureau.com/wp-content/uploads/2024/09/Technical-Advisory-Center-for-Internet-Security.pdf.

2.3.2 Database manipulation

Direct unauthorized access to vote databases could allow changing of tallies.[5]

2.4 Operational Vulnerabilities

2.4.1 Insider threats

Election officials or poll workers with privileged access could potentially manipulate systems or data.

2.4.2 Foreign threats

Advanced Persistent Teams (APTs) sponsored by nation states such as China, Russia, Ukraine, Serbia or Iran could manipulate systems or data.[6]

2.4.3 Configuration errors

Mistakes in setting up machines or software could lead to incorrect vote recording or tallying.[7]

2.5 Denial of Service

2.5.1 Overloading systems

Attacks could aim to crash or slow down voting systems, potentially affecting vote recording or reporting.[8]

2.6 Voter Interface Issues

2.6.1 Vote-flipping

Touchscreen calibration issues or software bugs could cause votes to be recorded for the wrong candidate.[9]

2.6.2 Ballot design flaws

Poor digital ballot designs could lead to voter confusion and unintended selections.

3 Impact

The potential vulnerabilities in electronic voting systems could have several serious impacts if exploited.

[5] Every build of Dominion Voting System Election Management System (EMS) Server examined by cybersecurity professionals includes the installation of SQL Server Management Studio (SSMS). Not only is SSMS not a component of any EAC-certified voting system configuration by Dominion, this software is capable of manipulating election results without detection.

[6] U.S. Cybersecurity experts found evidence of China interference in 2020 election per letter from DNI John Ratcliffe. See https://electioncrimebureau.com/wp-content/uploads/2024/09/491038048-Ratcliffe-Views-on-Intelligence-Community-Election-Security-Analysis.pdf

[7] Mismatches between township and county election configurations were blamed for a 7,060 vote switch from Trump to Biden in 2020 election.

[8] The 2024 Primary Election in Arizona was impacted by a CrowdStrike service outage. See https://thehill.com/homenews/campaign/4788112-rnc-arizona-election-crowdstrike-outage/.

[9] In Northampton County, Pennsylvania, there was a coding error in voting machines during the 2023 election that caused votes to be flipped on a ballot question about retaining state appeals judges. This was due to a programming error by the voting machine company Election Systems & Software (ES&S). See https://whyy.org/articles/pennsylvania-voting-machines-error/

3.1 Vote manipulation

Malicious actors could potentially alter vote counts or change votes, undermining the integrity of election results.[10]

3.2 Voter disenfranchisement

Attacks that disrupt voting systems or spread misinformation could prevent legitimate voters from casting ballots.

3.3 Undermining public trust

The perception of vulnerabilities enhanced by the utter lack of transparency associated with the operation of electronic voting systems can erode confidence in election outcomes and democratic processes.

3.4 Targeted voter suppression

AI and other technologies could be used to disproportionately target certain voter groups with misinformation or suppression efforts.

3.5 Compromised ballot secrecy

Some online voting systems may jeopardize the secret ballot, enabling voter coercion or vote buying.

3.6 Large-scale election failures

Internet and blockchain-based voting introduce risks of undetectable, nation-scale election failures.

3.7 Identity theft risks

Collecting voter information online exposes voters to potential identity theft.

3.8 National security threats

Vote manipulation could result in the overthrow of the United States government thereby posing an existential threat to our sovereignty. Furthermore, for military voters, online voting could potentially reveal sensitive deployment information.

4 Risk Mitigation Strategy

To counter these risks, we recommend the following best practices:

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

- Remove electronic voting systems
- Define and implement hand count procedures

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] In Lake v Fontes, evidence of vote manipulation by a Proportional-Integral-Derivative (PID) controller was introduced. See https://electioncrimebureau.com/wp-content/uploads/2024/03/23-_PetitionForWritOfCertiorari.pdf

- 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

Election officials are obligated to ensure the accuracy and integrity of election records under their jurisdiction. Electronic voting systems introduce significant security vulnerabilities that are often beyond the skill level and resources available to most election officials to address in any reliable or substantive manner. Failure to address such vulnerabilities enables the manipulation of vote tallies and overall election results. In this light, serious consideration should be given as to whether or not the perceived benefits of electronic voting systems are outweighed by the severe risks to our system of government introduced by such systems.