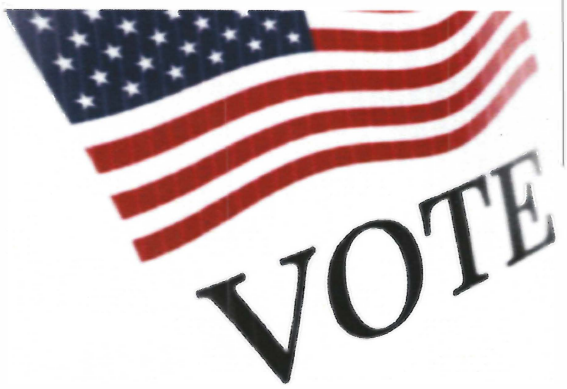
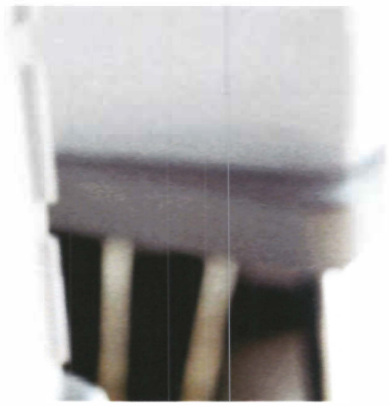
Recognizing and Addressing Threats to Statewide Voter Registration Databases

July, 2026





EXECUTIVE SUMMARY

Recently declassified records revealed that China breached multiple state voter registration systems prior to the 2020 election. Unfortunately, this is not a new phenomenon. Unclassified reports from the last decade reveal that Statewide Voter Registration Databases (VRDB) are attractive targets for foreign adversaries.[1] Hackers have attempted to breach voter registration systems in all 50 states, with confirmed successes in at least 20 states. However, experts have routinely minimized the significance of successful voter registration breaches and the exposure of sensitive personal data used for voter verification. This failure to identify and accurately describe the potential threats makes U.S. elections less secure.

State and local election officials must prioritize enhanced defenses to protect voter registration databases, and to limit the ways that compromised data can be exploited. Steps should be taken to prevent bad actors from using stolen data to successfully obtain absentee ballots, alter voter registration information, or add and delete registrants. Implementing and maintaining safeguards is essential to protecting the electoral process and sustaining public confidence in elections.

It is imperative to be realistic about the threats posed by foreign adversaries to our critical systems, including election infrastructure. Accurately assessing and communicating the potential for serious consequences is fundamental to effective preparedness and risk management. While candid acknowledgment of these threats may cause concern, it enables critical infrastructure owners to make informed decisions about security measures and mitigation strategies, thereby reducing vulnerability to worst case scenarios. Ignoring or minimizing risks undermines the ability to implement robust controls and leaves critical systems exposed. Transparent recognition of the threat landscape is essential for developing resilient defenses and ensuring the integrity and security of our election systems.

This product provides an unclassified overview of the threats to statewide voter registration databases from both foreign and domestic actors. It relies on reporting from the intelligence community, law enforcement, and state election officials. This report is intended to inform state and local election officials of the associated threats and the need to implement recommended mitigating controls.

HISTORY OF VOTER REGISTRATION SYSTEM BREACHES

Below are examples of unclassified reports of breaches of voter registration databases in the last ten years.

- Russian government cyber actors attempted to identify and exploit SQL database vulnerabilities in webservers and databases. The FBI reported that they lacked insight into the extent to which the attempts were successful. However, in at least two separate instances, Russian actors accessed voter registration files from a US county website.[2] (June 2016)

- The District Attorney in Riverside County, California revealed that a bad actor used the state's voter registration website to change the party affiliation of a large number of registered voters. The individual made the changes by leveraging access to voters' personal information (name, date of birth, driver's license, or Social Security number) to make the change without the voters' knowledge or consent.[3] (July 2016)

- Russian actors hacked the website of a state board of elections and stole information related to approximately 500,000 voters, including names, addresses, partial social security numbers, dates of birth, and driver's license numbers.[4] (July 2016)

- Russian actors hacked into the computers of a U.S. vendor that supplied software used to verify voter registration information.[5] (August 2016)

- DHS and FBI confirmed that Russian actors conducted election system reconnaissance to identify vulnerable databases, usernames, and passwords in webpages of state and local governments and probed voter registration database in **all 50 states.** They could not confirm how many of the probes resulted in successful breaches.[6] In January 2017, WH officials reported that the federal assessment was that networks in at least seven states were compromised.[7] (2016)

- Arizona experienced a breach and the Illinois State Board of Elections announced that attackers gained access to voter registration data, including names, addresses, birth dates, and partial Social Security numbers.[8] (2016)

- Kennesaw State University, which was responsible for supporting Georgia's voter registration database, was found to expose nearly 7 million voter records including driver's license and Social Security numbers of registered voters. The data may have been exposed for as long as seven months.[9] (March 2017)

- Chinese state-sponsored cyber actors aggressively targeted U.S. critical infrastructure to steal sensitive data and personally identifiable information (PII).[10] (August 2021)

- CISA and the FBI reported that members of the Iranian Republic Guard Corp attempted to exploit websites to obtain voter registration data. They confirm that the actor successfully obtained voter registration data in at least one state. They could not determine if the attempts were successful in the other 11 states targeted.[11] (September 2020)

- Pro-Russian hacktivists claimed to have conducted a Distributed Denial of Service (DDoS) attack that resulted in temporarily restricted access to a public-facing US state election office website. [12] (2022)

- Suspected Chinese cyber actors scanned both election-related and non-election state government websites. Other suspected PRC cyber actors also collected publicly available U.S. voter information.[13] (2022)

- New Hampshire election officials discovered that a vendor selected to replace the state's aging voter registration database had offshored part of the project. The software had been configured to connect to servers in Russia, and a programmer had hard-coded the Ukrainian national anthem into the database. The issues were corrected prior to deployment.[14] (2023)

State and local election officials must prioritize enhanced defenses to protect voter registration databases and to limit the ways that compromised data can be exploited. Implementing and maintaining safeguards to prevent bad actors from using stolen data to successfully obtain absentee ballots, alter voter registration information, or add and delete registrants are essential for protection of the electoral process.

While the potential impact of voter registration database breaches is often minimized, these exploitations could have serious consequences for the administration of elections. The impact of the breaches is not limited to "undermining confidence" or "spreading false claims" but the data itself could be used months or years after the breach to alter voter registration information or request absentee ballots. **The real threat is what can be done with the stolen data.**

POTENTIAL AVENUES FOR EXPLOITATION

WHY IT MATTERS

OBTAINING ABSENTEE BALLOTS

In nearly every election jurisdiction, the information required to apply for and receive an absentee ballot is stored in the voter registration database. A breach can allow bad actors to access public information such as name, date of birth, and address but also sensitive information like driver's license numbers, full or partial social security numbers, and voter signatures on file. That information could enable bad actors to request absentee ballots at scale for low-propensity voters. Data obtained in a breach from 2021, for example, could be used to request a ballot for an election in 2028 because the data does not get stale.

ALTERING VOTER REGISTRATION INFORMATION OR DELETING REGISTRANTS

A malicious actor could use data from a breach to alter voter registration records to change addresses and therefore their polling place or change party affiliation to impede voting in an election. Perpetrated at scale, this type of exploitation could disenfranchise a significant number of voters, and if carefully distributed, such an attack might go unnoticed even if the scope was significant. This type of malicious alteration of voter data could be done over time using data obtained from a breach to log into official online state systems that enable voters to update their voter registration after passing identity checks using personal data like date of birth, portions of social security numbers, or driver's license number. Deletion of voter registration files could cause disruptions in the administration of elections if done at scale or, if executed in a distributed manner.

PREPAREDNESS IS THE BEST DEFENSE

DEVELOP A PLAN

Preparedness, built on a realistic threat assessment, is the foundation of effective election security measures. With a sober acknowledgment of the threat, state and local election officials can take steps to enhance the security of voter registration databases and absentee and mail ballots.

BACK UP DATABASE FILES REGULARLY

A commitment to good cybersecurity and best practices is critical to protecting voter registration data. States should schedule frequent, routine back-ups of the voter registration database files and store them securely offline. States should also test the ability to revert to back-up during an incident.

For jurisdictions that utilize electronic pollbooks, producing paper pollbooks as back-ups will limit the potential for disruptions on Election Day.

ENGAGE YOUR PLAN

If you detect unauthorized access to your voter registration database, immediately implement your security incident response plan. It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, you should take steps to maintain your organization's essential functions according to your election resiliency and continuity plan.

PREPARE FOR POTENTIAL CYBERSECURITY INCIDENTS

Network infrastructure and internet-facing applications, including voter registration databases, underpin and enable a variety of functions in the conduct of elections. These may include election infrastructure networks that store, host, or process voter registration information, as well as public-facing election websites that support functions like polling place lookup. Local election officials have the power to prevent most security incidents using basic security measures. Take steps now so that even if an incident occurs, critical election operations can continue.

Protect and Respond: Phishing Attempts Targeting Your Email

- Enable Multifactor Authentication on all accounts.
  - Ensure each account has its own unique credentials and do not allow credential sharing.
  - Apply the principle of least privilege by separating admin accounts and user accounts.
  - Ensure everyone changes their default passwords and require strong passwords for all accounts.
- Enable Domain-based Message Authentication Reporting and Conformance for all email accounts to make it easier for email senders and receivers to determine whether an email legitimately originated from the identified sender and provides the user with instructions for handling the email if it is fraudulent.
- Implement flagging external emails to alert users to use due care when opening.
- Train staff so they know to only use their official email accounts, which often include enhanced security features, for official business.
- Train staff to spot and report phishing or other suspicious emails.
  - Malicious actors are improving their techniques all the time, so training should be provided at regular intervals to educate staff about the latest tactics and how to respond to suspicious communications. Regularly review common signs of phishing so staff are familiar with what to look out for and how to report.

Protect and Respond: Distributed Denial of Service Targeting Your Websites

- Review existing contracts and coordinate with both website service providers and internet service providers before an incident occurs.
- Identify what additional Distributed Denial of Service (DDoS) mitigation and redundancy measures are available. Most major service providers have protections available, which may be offered at no cost for basic services, or at additional cost for advanced services.
- Ensure you know who to contact in the event of an incident.

- Share information about important election dates and locations, requesting that ample troubleshooting is available during key periods, and ensuring mutual awareness of any planned maintenance that could impact election operations.
- Ensure network traffic monitoring and analysis is enabled via a firewall or intrusion detection system and that the logs are being reviewed.
- Have an alternate plan for information dissemination in case your website does go down. Make sure to test that plan.

Protect and Respond: Ransomware Targeting Your Network

- While not binding on non-Federal entities, CISA's Binding Operational Directives are indicative of best practices and network owners should consider following them.
- Develop a patch management plan that makes reducing the significant risk of known exploited vulnerabilities a top priority for remediation and requires critical vulnerabilities to be re-mediated within 15 calendar days of initial detection.
- Implement and enforce network segmentation. Proper network segmentation is an effective security mechanism to prevent an intruder from propagating exploits or moving laterally within an internal network. This includes not transferring election results on the business network.
- Implement endpoint detection and response software on endpoint devices to monitor for malicious traffic. Verify alerts are being created and response processes are followed.
- If not already being used, government entities should use .gov domains.
- Implement Malicious Domain Blocking and Reporting (MDBR) across your network devices to prevent IT systems from connecting to harmful web domains. MDBR can block the vast majority of ransomware infections just by preventing the initial outreach to a ransomware delivery domain.
- Develop and maintain incident response plans that specifically detail how to operate mission-critical processes in the event of a cybersecurity incident.
- Test your incident response plans with all key players who would be involved in implementing the response.
- Maintain backups that allow you to recover data at a minimum of up to 30 days prior.
    - Encrypt backup files and ensure credentials for accessing the backups are not stored in the targeted environment. Ransomware actors often hunt for and collect credentials stored in the targeted environment and use those credentials to attempt to access backup solutions; they also use publicly available exploits to target unpatched backup solutions.
    - Ensure backups are maintained offline, as most ransomware actors attempt to find and subsequently delete or encrypt accessible backups to make restoration impossible unless the ransom is paid.
    - Test the availability and integrity of backups in a disaster recovery scenario.

DATA BREACHES GENERALLY

Over the last decade, millions of Americans have had their personally identifiable information (PII) leaked in data breaches that are not related to voter registration but compromise election security, nonetheless. Cybercriminals have gained access to databases belonging to financial institutions, healthcare providers, and other government agencies, obtaining PII including Social Security numbers, addresses, full names, dates of birth, and driver's license numbers. In many cases, this information is sold on the dark web, where it is easily accessible to malicious actors. Because much of this same data is used to verify voter eligibility, maintain voter rolls, and verify identity for absentee ballot requests, large-scale PII exposure of data held by private companies has implications not only for privacy and financial fraud, but also for the integrity of U.S. elections.

- In July 2017, a credit reporting firm discovered a data breach that affected a potential 143 million United States citizens, almost half of the population. The breach reportedly began in May 2017 and was announced nearly four months later. By exploiting an unpatched vulnerability in web application software, cyber attackers were able to steal an unprecedented amount of PII including Social Security numbers, dates of birth, home addresses, driver's license numbers, and full names.
- On February 10, 2020, the Department of Justice (DOJ) indicted four members of China's People's Liberation Army on counts of economic espionage, wire fraud and computer fraud. In a statement following the indictment, Attorney General William Barr said the hack fits "a disturbing and unacceptable pattern of state-sponsored computer intrusions and thefts by China and its citizens that have targeted personally identifiable information, trade secrets, and other confidential information."
- In April 2024, a background check firm that stored troves of records including full names, current and past addresses, Social Security numbers, dates of birth, and telephone numbers suffered a colossal data breach of 2.9 billion records containing PII of 170 million individuals. The information was reportedly found on the Dark Web being offered for $3.5 million.
- One of the largest supplemental insurance providers in the United States suffered a data breach in June 2025 that affected 22.65 million individuals. Information accessed by hackers included PII such as Social Security numbers, dates of birth, driver's license numbers and full names. Hackers gained access to the provider's systems via social engineering tactics e.g. phishing, whaling, and impersonation.
- A report from the University of Oxford found that Russia and China ranked first and third, respectively, as nations that pose the highest threat level of cybercrime. Moreover, the PII available to these adversaries is not limited to that accessed through their own cyber operations but can be readily purchased or accessed on the dark web.

The cases mentioned above involve breaches that contained the information typically needed for voter registration and absentee ballot applications. The threat this exposed data poses to the integrity of U.S. elections is significant and ongoing, underscoring the need to recognize and mitigate the direct risk it poses to critical election infrastructure.

CONCLUSION

Voter registration databases are the foundation of our voting system. State and local election officials must prioritize system security and implement safeguards to prevent the exploitation of data that may have already been exposed. Adopting modern security enhancements such as smart network monitoring and multi-factor authentication can limit the risks of fraud and election disruptions. The Department of Homeland Security is charged with protecting the nation's critical infrastructure, including election infrastructure, and all state election officials are encouraged to collaborate with DHS on this important mission.

For more information about election security and resources to protect elections, visit the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Toolkit and Resources to Protect Elections page: https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections

REFERENCES

[1] https://www.justice.gov/archives/sco/file/1080281/dl?inline

[2] https://www.justice.gov/archives/sco/file/1080281/dl?inline

[3] RIVERSIDE COUNTY: District attorney claims voters' party affiliations purposely changed without consent - Press Enterprise ±

https://www.justice.gov/archives/sco/file/1080281/dl?inline

[5] https://www.justice.gov/archives/sco/file/1080281/dl?inline

[6] https://www.intelligence.senate.gov/2020/08/18/publications-report-select-committee-intelligence-unitedstates-senate-russian-active-measures/

[7] U.S. intel: Russia compromised seven states prior to 2016 election

[8] Voter Databases in Arizona and Illinois Breached, FBI Says

[9] GEORGIA VOTING HACK: FBI investigating alleged breach of Georgia elections center at Kennesaw State University - WSB-TV Channel 2 - Atlanta

[10] https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/1/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF

[11] https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-304a

[12] Key Findings and Recommendations: Foreign Interference Related to the 2022 US Federal Elections | Homeland Security

[13] https://www.dhs.gov/sites/default/files/2023-12/1_b_%20Memo%20DOJ%20and%20DHS%20Approved_508c.pdf

[14] Hacking Blind Spot: States Struggle to Vet Coders of Election Software - HSToday

ELECTION REPORT

EXECUTIVE SUMMARY

From around 2019 to 2024, the Cybersecurity and Infrastructure Security Agency (CISA) conducted a set of technical and operational activities to evaluate the security of certain U.S. election systems. These activities, all carried out upon the request of system owners and operators, included direct examination of election-related software: penetration testing of state, local, tribal, and territorial (SLTT) networks; and incident response operations for intrusions into elections systems. Through these activities, CISA developed a strong understanding of the vulnerabilities that, at the time of testing, affected select election-related software products and network environments evaluated by CISA. In every software product or election-related network in which CISA identified a vulnerability, CISA notified the owner or operator of the vulnerable product or network and encouraged them to mitigate the vulnerability.

CISA's findings highlight the reality that election-related software, like all complex software, contains vulnerabilities that require timely remediation. While past partnerships with election vendors enabled early identification of security weaknesses prior to product release, structural constraints in the certification ecosystem significantly limit vendors' abilities to patch systems quickly. For example, some government election systems certification regimes require that no patches be applied for months before an election. These limitations, combined with inconsistent vulnerability disclosure practices, result in election systems being deployed with known and unpatched security issues.

Beyond software quality, CISA's assessments repeatedly show that the IT networks operated by SLTT election offices lack cybersecurity hygiene. Many election vendor threat models assume strong network segmentation and isolation of election systems. However, in practice, election infrastructure is often accessible from general enterprise networks, creating opportunities for lateral movement by adversaries who compromise email systems, user workstations, or other information technology (IT) assets. Weak identity management, limited logging, and insufficient segmentation exacerbate the risk that a cyber threat actor could access or disrupt mission critical election IT components.

Overall, the security of U.S. elections is shaped by the interaction of three major factors: (1) software vulnerability management constrained by outdated certification regimes; (2) inconsistent transparency from election system vendors on vulnerabilities and patch status; and (3) the cybersecurity immaturity of many SLTT networks responsible for hosting election systems. Addressing these challenges requires coordinated action across technical, policy, and regulatory domains. This report provides detailed analysis and proposes targeted recommendations to strengthen election infrastructure security and enhance public trust in the resilience of the nation's elections infrastructure.

Introduction

From around 2019 to 2024, CISA evaluated the security posture of election entities through multiple, mutually reinforcing technical activities. These included, upon the request of relevant entities, direct source code and binary analysis of election software, protocol and interface assessments, penetration testing and red team operations against SLTT networks, and response operations for cybersecurity incidents affecting those same partners. Together, these activities provided CISA with a multilayered view of vulnerabilities across the software supply chain, deployment environments, operational workflows, and adversary targeting trends. In every case that CISA identified a vulnerability in a software product or election-related network, CISA notified the owner or operator of the vulnerable product or network and encouraged them to mitigate the vulnerability.

CISA correlated vulnerability data; adversary tactics, techniques, and procedures (TTPs); threat intelligence; configuration weaknesses; logging gaps; and systemic architectural issues across numerous assessments of SLTT entities. The agency's analysis helped identify security regressions (in which modifications to software result in the re-emergence of previously resolved issues), recurring ineffective or harmful attempts at solutions, and conditions that enabled adversaries to exfiltrate sensitive data, modify election artifacts, or degrade system availability.

The intent of this report is to draw from CISA's assessments in the 2019-2025 timeframe to present an assessment of the security of U.S. election systems—covering not just voting and registration specific software components, but also the broader enterprise environments in which they operate, to include things like email accounts and other office IT assets. The document concludes with recommendations designed to help policymakers and technical leaders meaningfully reduce systemic risk and strengthen public confidence.

Election Software Security

Direct Software Examination (Static and Dynamic Analysis)

From 2019 through 2024, CISA partnered with Idaho National Laboratory (INL) on the Critical Product Evaluation program to conduct direct technical assessments of election software, in many cases prior to the public release of such software. These assessments occurred only upon the request of the relevant software vendor and included:

- Automated and manual static source code review;
- Binary fuzzing of parsers, media handling components, and data import modules;
- Cryptographic implementation analysis (e.g., misuse of PRNGs, poor key handling);
- Interface security testing, including authentication, authorization, and API boundary validation;
- Supply chain dependency reviews, including third-party libraries, OS packages, and firmware where applicable; and
- Dynamic analysis in hardened and adversarial runtime environments.

While vendors generally viewed the program as valuable, the model created disincentives for transparent, industry standard vulnerability disclosure. Vendors benefited from private remediation prior to market release, but the downstream ecosystem—SLTT administrators, risk managers, and external researchers—did not receive clear vulnerability histories or patch transparency. The program was therefore retired in 2024 based on stakeholder feedback, and final reporting concluded in 2025.

CISA's analysis of the Critical Product Evaluation reports confirms that election software, like any complex system, contains a spectrum of vulnerabilities, including input validation bugs, insecure deserialization, insufficient logging, race conditions leading to unpredictable results, insecure crypto primitives, and privilege escalation paths. Many vulnerabilities were remediated quickly by vendors before release. However, CISA did not independently validate whether production builds deployed in SLTT environments incorporated all fixes.

Constraints on Security Updates

SLTT election officials face difficulties in applying security updates to election software in a timely manner. Most SLTT officials have minimal IT budgets and cybersecurity staff. In addition to resource constraints, some election systems are only deployed for limited periods of time in the immediate period surrounding an election. Others are deployed for longer periods but are "locked down" to prevent any changes during the months or weeks leading up to election day. In some cases, these lockdown periods are mandated by state law. Those state laws may also require that SLTT entities only deploy election software that has been certified by the Election Assistance Commission (EAC), which may also delay the application of security updates if an update postdates EAC certification. These jurisdictional differences present a fragmented certification ecosystem to election software vendors.

The following technical risks predictably arise from this complex environment:

- Vendors often cannot ship security fixes outside narrow certification cycles without jeopardizing eligibility for upcoming elections.
- Third-party components embedded in election systems (operating systems [OS], device drivers, middleware, cryptographic libraries) cannot be patched at normal modern software cadence.
- Legacy OS baselines and unsupported runtime components accumulate unpatched vulnerabilities.
- The absence of secure auto-update mechanisms prevents rapid response to zero-day threats.

In practice, these constraints produce environments where known, documented vulnerabilities persist for months or years on production election systems, increasing exposure to opportunistic and targeted threats. The election vendors' reluctance to publicly disclose vulnerabilities in certified products further limits SLTT operators' ability to make informed risk decisions, perform compensating control analysis, or adjust architectural segmentation.

National policymakers should encourage harmonization of rules applicable to patch management and certification of election systems. Such harmonization would allow SLTT election officials greater flexibility in installing security updates in a timely manner and would present a less fragmented environment for election system vendors.

Election Systems in SLTT Operating Environments

SLTT Network Security Posture

Election software is deployed into SLTT managed networks that frequently lack the defensive maturity assumed in vendor threat models. Across numerous penetration tests and red team engagements, CISA observed recurring structural weaknesses in SLTT-managed networks:

- Flat or minimally segmented networks, allowing lateral movement from standard enterprise zones (email servers, line-of-business applications) into election related environments.
- Weak identity and access management, including poor enforcement of multi-factor authentication, shared credentials, and inadequate service account hygiene.
- Lack of endpoint hardening, including outdated OS versions, insufficient event logging, and unmonitored administrative interfaces.
- Legacy remote access and file transfer pathways that remain reachable from segments that should be isolated.
- Insufficient monitoring of network traffic, preventing detection of adversary activity.[1]

In multiple cases, CISA assessors gained full network control within hours or days, demonstrating that many SLTT partners remain soft targets incapable of stopping even moderately skilled adversaries.

Most states have moved away from paperless electronic voting machines, because these systems don't provide a physical record or give voters a way to ensure their selections were recorded accurately. The replacement paper-voting systems also contain vulnerable components; in 2020, ImageCast X Ballot Marking Devices printed voters' completed ballots on paper but encoded their selections in a barcode that voters had no way to verify. A researcher showed that hackers could change the votes encoded in the barcode, without even having physical access to the machines.[2] The Office of the Director of National Intelligence (ODNI) additionally commissioned a forensic examination of Dominion Voting Systems devices used in Puerto Rico's 2024 election.[3] While CISA did review the report, the agency did not have access to those devices and was unable to perform an examination.

---

1 Cybersecurity and Infrastructure Security Agency (CISA). *Cyber Risk Summary: Election Infrastructure (EI) Subsector, October 2022–September 2023*. Published February 2024.

2 J. Alex Halderman, *Security Analysis of Georgia's ImageCast X Ballot Marking Devices: Expert Report Submitted on Behalf of Plaintiffs Donna Curling, et al., Curling v. Raffensperger, Civil Action No. 1:17-CV-2989-AT, U.S. District Court for the Northern District of Georgia, Atlanta Division*, with assistance from Drew Springall, July 1, 2021.

3 Dominion Voting Systems Democracy Suite Preliminary Vulnerability Assessment, Mojave Research for the ODNI, September 25, 2025.

Segmentation Failures Against Vendor Threat Models

Election vendor threat models typically assume that there is strong network segmentation between election systems—such as voter registration databases, electronic pollbooks, election management systems/tabulation systems, and central scanning infrastructure—from general enterprise IT environments. However, CISA assessments from 2019-2024 repeatedly showed:

- Election systems were reachable from enterprise hosts due to shared authentication domains, legacy VLAN configurations, or "temporary" exceptions that become permanent;
- Inadequate firewall rule hygiene, with over-broad allow rules and insufficient egress controls;
- Election infrastructure that is co-located on general purpose virtualization clusters that also host public facing workloads; and
- Overreliance on "airgap" assumptions that do not reflect actual connectivity (e.g., vendor support tunnels, unmonitored remote management tools, or indirect network paths).

These misalignments between theoretical and actual deployment models create exploitable pathways for adversaries capable of moving from commodity phishing based initial access to high value election assets.

The Importance of Transparency

American citizens have a right to know when the infrastructure that runs elections has been compromised, and what happened as part of the incident. By openly acknowledging incidents and describing mitigation steps, vendors and localities can show that they are proactively defending critical infrastructure rather than obscuring vulnerabilities. This transparency encourages continuous improvement, drives investment in stronger defenses, and reinforces that protecting elections is a collective national priority.

Clear and consistent disclosure strengthens accountability across the institutions responsible for safeguarding election systems. Even the perception of secrecy around cybersecurity incidents can erode trust faster than the incidents themselves. Communicating early, often, and honestly—while still protecting sensitive operational details—helps ensure that Americans maintain faith in the integrity of their elections and the resilience of the systems that support them.

Mitigation Measures

CISA recommends that SLTT election officials take the following mitigation measures:

1. Harmonize relevant patch management and certification rules for voting systems and associated IT infrastructure to allow cybersecurity changes to be made in real-time, without impacting certification.
2. Adhere to CISA's Best Practices for Securing Election Systems, at https://www.cisa.gov/news-events/news/best-practices-securing-election-systems.
3. Use human-readable paper ballots.

4. Conduct post-election manual audits of paper ballots to confirm that voting systems function as intended and to identify errors prior to certification of results.
5. Encourage election software providers to:
    a. Assign Common Vulnerabilities and Exposure (CVE) numbers for vulnerabilities in their software;
    b. Provide notice to customers if elections software source code is leaked or stolen;
    c. Report cybersecurity incidents to relevant authorities; and
    d. Include a software bill of materials (SBOM) with all products.
6. Ensure clear, consistent, and transparent documentation of all security incidents and remediation processes.

Conclusion

CISA's findings highlight that U.S. election systems are subject to the same security concerns as most other software systems: they are subject to outdated and fragmented certification regimes, insufficient vulnerability transparency, and persistent cybersecurity gaps in SLTT operating environments. These issues are not attributable to any single entity but are the result of complex interdependencies between vendors, certifiers, policymakers, and resource constrained SLTT partners.

Strengthening election-system security requires coordinated action across the entire ecosystem. SLTT election offices need sustained investment in network modernization, segmentation, identity management, and monitoring capabilities. CISA's recommended mitigation measures—including paper-based voting records, rigorous post-election manual audits, SBOM adoption, and improved incident tracking—provide a path toward measurable, near-term improvements.