



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elections is shaped by the interaction of three major factors: (1) software vulnerability management constrained by outdated certification regimes; (2) inconsistent transparency from election system vendors on vulnerabilities and patch status; and (3) the cybersecurity immaturity of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.