2026

The Security of Electronic Voting Systems in the U.S.

AN ASSESSMENT OF ELECTION ASSISTANCE COMMISSION ASSERTIONS

PATRICK COLBECK

January 2026

Made possible by funding from the Lindell Offense Fund

Table of Contents

1 Purpose

The purpose of this report is to provide an assessment of the following statement made by the Chairman of the Election Assistance Commission (EAC), Donald Palmer, to election integrity leaders in an email dated December 7, 2025:

"Here are a few facts that should be considered: EAC has reviewed the source code of every registered manufacturer and maintains the source code of every registered manufacturer and each system. The experts at the accredited labs and EAC will tell you independently that the source code and software is NOT the same for every manufacturer and there is no one master key to all systems - this is just a fallacy. I would also add that many of these newer systems offered by manufacturers have also been independently reviewed by Idaho National Lab (INL) whose mission is to seek to exploit the systems, identify vulnerabilities and then offer mitigation strategies to the manufacturers in the building of systems, and this "universal key" or "universal software" is not something that has ever been identified and reported by some of the best white hat hackers in the world or any of EAC/Lab experts or any three letter agency. The accredited labs and EAC have certified the trusted build of each of these systems and this trusted build is what the states and counties receive when they use an EAC certified system. The EAC also conducts penetration testing prior to a VVSG campaign to ensure known vulnerabilities have been remedied and seek to identify any new vulnerabilities. The EAC would like to do even more and conduct regular independent vulnerability testing of all voting systems and that is being considered by the House and Senate with the NDAA, but this is not a sure thing without funding and legislation."

This assessment seeks to evaluate whether or not the current efforts of the EAC are sufficient to effectively mitigate the risks to the security of our election systems which have been deemed to be "Critical Infrastructure" by the federal government.

2 Background

Before proceeding with this assessment, there is some important background information that is needed in support of this assessment.

2.1 EAC

The U.S. Election Assistance Commission (EAC) is an independent, bipartisan federal agency created by the Help America Vote Act of 2002 (HAVA) in response to the voting system failures and controversies surrounding the 2000 presidential election. Its statutory

mission is to help state and local election officials improve the administration of federal elections, primarily by serving as a national clearinghouse for election administration information, distributing federal funds for election improvements, and establishing technical guidelines for voting systems.

HAVA assigned the EAC several core responsibilities that are directly relevant to any evaluation of its effectiveness. These include: (1) developing and maintaining the Voluntary Voting System Guidelines (VVSG), which define functional, accessibility, and security requirements for voting equipment; (2) operating the nation's first federal voting system testing and certification program, including accrediting Voting System Test Laboratories and certifying or decertifying specific voting system configurations; (3) administering payments and grants to states to replace outdated voting systems and improve election administration; and (4) maintaining the National Mail Voter Registration Form and operating a public clearinghouse of election practices and data.

Structurally, the EAC is governed by four commissioners, two from each major political party, who are appointed by the President upon recommendations from congressional leaders and confirmed by the Senate. This design is intended to ensure bipartisan oversight of federal election standards and voting system certification, but it also means the agency's ability to set policy and enforce standards can be constrained when vacancies or partisan deadlock prevent the commission from reaching a quorum. Because many states have enacted laws requiring some level of compliance with EAC certification and VVSG standards, the EAC's guidance, testing program, and management decisions exert significant practical influence over what equipment is purchased, how billions in public funds are spent, and what security assurances are offered to the public.

2.2 CISA

The Cybersecurity and Infrastructure Security Agency (CISA) is the lead federal entity responsible for securing the nation's critical infrastructure, including election systems, and its role forms a key part of the environment in which the Election Assistance Commission operates. Established in 2018 when Congress elevated the former National Protection and Programs Directorate to agency status under the Cybersecurity and Infrastructure Security Agency Act, CISA is housed within the Department of Homeland Security and is charged with protecting both cyber and physical infrastructure across 16 designated critical infrastructure sectors.

In the election context, DHS previously designated election systems as part of the "Election Infrastructure Subsector" of the Government Facilities critical infrastructure sector, giving CISA a formal role as the sector risk management agency for election

infrastructure. CISA works on a largely voluntary basis with state and local election officials, the EAC, and private vendors to provide no-cost cybersecurity and physical security services, including vulnerability scanning, penetration testing, incident response assistance, training, and best-practice guidance tailored to election offices. Through cooperative agreements, CISA has also funded and supported the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), which distributes threat intelligence, monitoring, and incident response support to state and local jurisdictions.

CISA's work on election security is coordinated through the Election Infrastructure Subsector Government Coordinating Council (GCC), composed of state and local election officials, and the Sector Coordinating Council (SCC), composed of vendors and other private stakeholders. The agency regularly issues joint statements, guidance documents, and public communications with the EAC aimed at reassuring the public about election security and standardizing security practices nationwide. Because CISA's assessments, advisories, and risk summaries inform state procurement decisions and EAC standards discussions, its performance in identifying and mitigating election infrastructure vulnerabilities is a critical factor in evaluating whether the EAC's overall security posture and certification framework are effective in practice.

On July 28, 2020, months before the controversial 2020 election, CISA released a report called "Critical Infrastructure Security and Resilience Note". The report was remarkable in that it addressed a broad scope of technology-based vulnerabilities inherent with America's election system (See Figure 1).

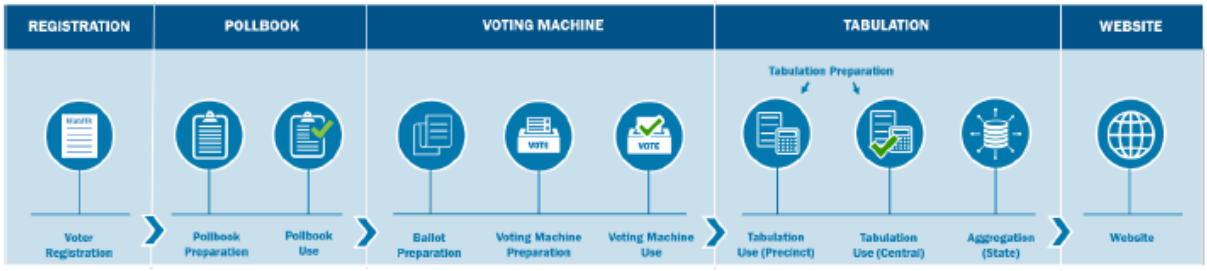

Figure 1 Election System Functional Ecoystem

The report went beyond highlighting these vulnerabilities and actually cited the consequences of an exploitation of these vulnerabilities (See Figure 2).

The key question is whether or not there is evidence that would indicate that one or more of these vulnerabilities were exploited by foreign or domestic adversaries during the 2020 election.

ELECTION COMPONENT	CONFIDENTIALITY CONSEQUENCE	INTEGRITY CONSEQUENCE	AVAILABILITY CONSEQUENCE
Voter Registration	Expose Non-public Voter Registration Information	Change Voter Registration Information	Prevent Access to Voter Registration Information
Pollbook Preparation	Expose Non-public Voter Registration Information	Change Voter Registration Information	Prevent Access to Voter Registration Information
Ballot Preparation	Expose Ballot Information	Change Ballot Information During Preparation	Prevent Ballot Preparation
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
Pollbook Use	Expose Non-public Voter Registration Information	Change Voter Registration Information (In Pollbook)	Prevent Access to Voter Registration Information
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
Website	Expose Information Not Intended for Public Disclosure	Change Reported Results	Prevent Reporting of Results

Figure 2 Potential Consequence of an Election Cyber Attack by Component

According to CISA, the answer appears to be no. On November 13, 2020, CISA issued the following joint statement from Elections Infrastructure Government Coordinating Council and the Election Infrastructure Sector Coordinating Executive Committees:

> "The November 3rd Election was the most secure in American history."

This is a remarkable claim considering that the only election components subject to certification by the EAC were the precinct and central tabulation components.

2.3 Evidence

Prior to the November 3, 2020 general election, there were numerous media reports[1] and documentaries exposing vulnerabilities with our electronic voting systems. As far back as 2006, CNN host Lou Dobbs aired concerns surrounding the foreign ownership of Smartmatic voting systems used to run elections in the United States.[2]

In the wake of the 2020 election, anyone attempting to share evidence of these security vulnerabilities was deemed a conspiracy theorist and lawyers who introduced lawsuits containing these assertions were sanctioned. On June 26, 2023, the U.S. House Select Subcommittee on the Weaponization of Government issued a report titled "**The Weaponization of CISA: How a 'Cybersecurity' Agency Colluded with Big Tech and 'Disinformation' Partners to Censor Americans**' indicating that the suppression of the release of this evidence was the real conspiracy.[3]

Despite this censorship, election investigators persevered with their efforts to expose evidence of election fraud. At first, the evidence was limited to open source information that could be obtained via observation or Freedom of Information Act (FOIA) requests. In rare circumstances, legal actions were successful in obtaining additional evidence via subpoenas and the discovery phase of civil lawsuits. While all of this evidence gathering was going on, there was a group of professional investigators that played the long game and developed a cadre of whistle-blowers with insider information as to how machines were used to steal elections. These evidence sources have been classified according to their evidentiary value in Table 1.

[1] https://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436
[2] https://www.youtube.com/watch?v=aWPluT_Y2TQ&pp=ygUbbG91IGRvYmJzIG9uIGNubiBzbWFydG1hdGlj
[3] https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf

Table 1 Evidence Classifications

EVIDENCE CLASS	DESCRIPTION	EVIDENTIARY VALUE
Class i – insider testimony	Insider who personally observed or participated in the events at issue (e.g., election official, vendor employee, poll worker) and can describe those actions first-hand.	Often the strongest evidence when the witness is credible and corroborated, because it is direct, first-hand testimony subject to cross-examination.
Class ii – outsiders with access to machines	Outsider (e.g., independent expert) who did not run the election but has direct access to forensic images or data from voting machines and related systems, and can analyze or explain what that data shows.	Valuable technical and corroborative evidence; typically carries substantial weight when the expert is qualified, methods are sound, and findings align with or support insider testimony and other evidence
Class iii – outsiders limited to osint	Outsider who relies only on publicly available/open-source information (media reports, public databases, social-media posts, etc.) Without direct access to internal systems or data.	Generally weaker on its own; may be admissible if properly authenticated and reliable, but is most effective as corroboration rather than as primary proof of fraud.

The assertions in this report draw primarily on the body of evidence found in Table 2. Additional evidence in support of the assertions in this assessment is available.

Table 2 Supporting Evidence

EVIDENCE[4]	CLASS
Senior Venezuelan Election Official Testimony	Class I
Former Venezuelan Head of Security for Hugo Chavez Testimony	Class I
Former Venezuelan Lieutenant General Hugo Carvajal Barrios Testimony	Class I
Former Venezuelan Major General Cliver Antonio Alcala Cordones Testimony	Class I
Internal Dominion Emails	Class I
StolenElectionsFacts.com	Class II
Stolen Elections by Ralph Pezzullo	Class II
Mesa County, CO Report #1	Class II
Mesa County, CO Report #2	Class II
Mesa County, CO Report #3	Class II
Various online documents (see footnotes)	Class III

The testimony provided by insiders and documented in the book Stolen Elections by Ralph Pezzullo identified at least 14 unique machine-based mechanisms featured in Smartmatic

[4] https://electioncrimebureau.com/evidence/

voting systems (i.e. SAES) that could be or have been used to manipulate election results (See Figure 3).

Figure 3 Smartmatic (SAES) Elements Used to Alter An Election

These election fraud mechanisms were also evident in Sequoia Systems (See Figure 4).

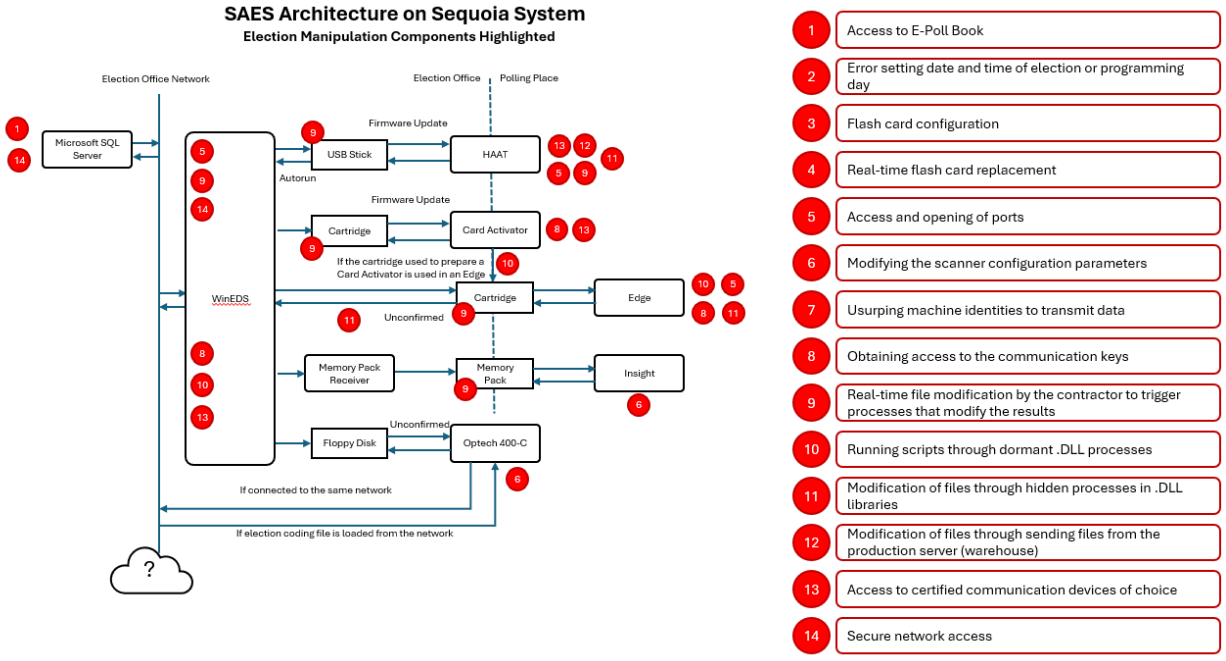

Figure 4 SAES Architecture Found in Sequoia System

These election fraud mechanisms were also evident in Dominion Voting Systems now known as Liberty Vote (See Figure 5).

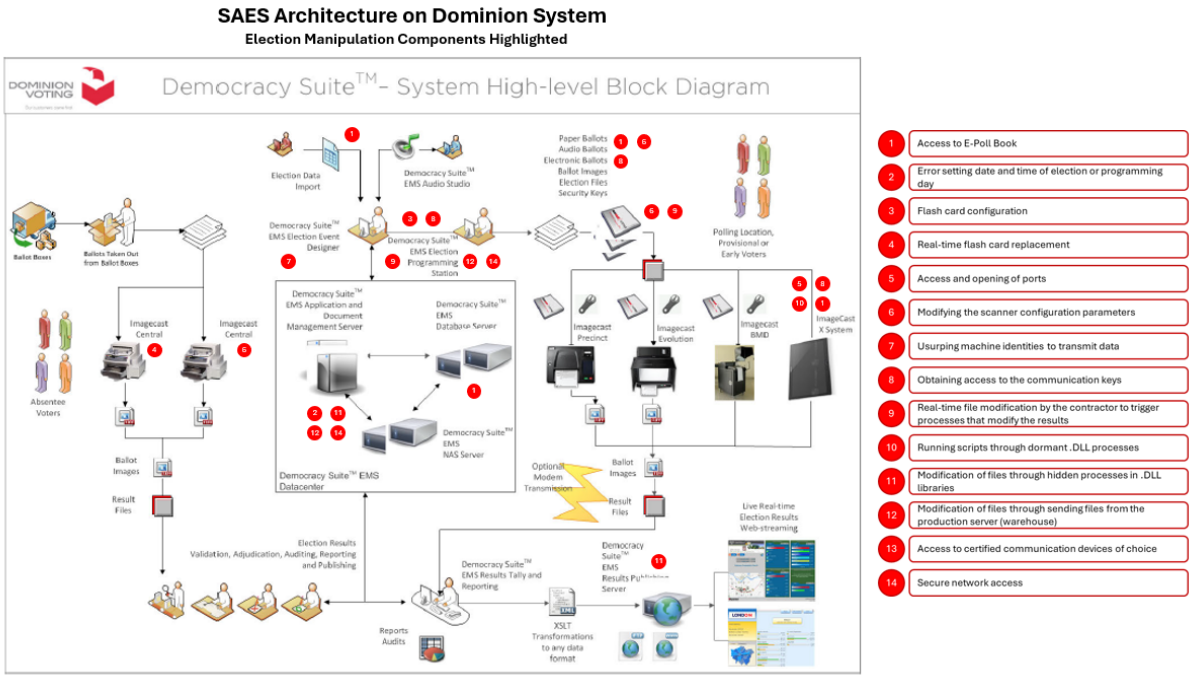

Figure 5 SAES Architecture Found in Dominion Voting System

These mechanisms were identified by insiders responsible for the development and deployment of machines used to subvert actual election results. These diagrams are highlighted in order to provide context for the assertions made in this assessment.

3 EAC Chairman Assertions

The primary thrust of the assertions of the EAC Chairman Donald Palmer is that U.S. voting systems are diverse, independently verified, and subject to strict security testing, contrary to claims that they share a single, exploitable master software. The EAC and related agencies maintain robust oversight and are seeking even stronger security measures through policy and funding.

3.1 EAC Oversight of Source Code

The EAC has reviewed and maintains the source code of every registered voting system manufacturer and each certified system. This implies that there is centralized oversight and documentation of all certified voting systems.

3.2 Manufacturer Software Differences

Each manufacturer's source code and software differ. The claim that there is a "single master key" or universal software that controls all systems is explicitly called a fallacy.

3.3 Independent Security Reviews

Systems have been independently reviewed by the Idaho National Laboratory (INL), which specializes in exposing vulnerabilities and recommending mitigations. INL and other experts have never identified or reported a universal key or software applicable to all systems.

3.4 Certification and Trusted Builds

Accredited labs and the EAC certify each system's "trusted build," meaning the exact, verified software version delivered to states and counties. This ensures the systems in use match what was tested and certified.

3.5 Penetration Testing and Vulnerability Management

The EAC performs penetration testing prior to each VVSG (Voluntary Voting System Guidelines) campaign to ensure old vulnerabilities are fixed and new ones are identified.

3.6 Future Security Enhancements

The EAC wants to conduct ongoing, independent vulnerability testing of all systems. This expansion of capability depends on congressional funding and legislation (potentially through the NDAA).

4 The Cost of Machines

Electronic voting systems impose substantial and recurring financial burdens on federal, state, and local governments, and these costs are concentrated in equipment procurement, replacement, maintenance, and associated infrastructure.

4.1 National and State-Level Capital Outlays

Public investment in electronic voting technology under the current EAC-centered framework is measured in the tens of billions of dollars over two decades.[5,6]

[5] https://www.eac.gov/sites/default/files/2025-01/EAC_2024_Annual_Report_FINAL_508c.pdf
[6] https://bipartisanpolicy.org/explainer/federal-election-funding-path/

- Federal Help America Vote Act (HAVA) and related appropriations have provided roughly $5 billion for voting equipment, modernization, and security since 2002.
- States and localities have added substantial matching and supplemental funds, with individual statewide replacement programs commonly running into the tens of millions of dollars, such as Michigan's estimated $55–$60 million voting equipment replacement plan[7] and Louisiana's projected $100 million system replacement.[8]

These large capital programs are cyclical because voting systems are treated as 10–15 year assets that must be replaced as they age or as standards change.[9]

- A 2022 analysis estimated that replacing outdated voting machines nationwide would cost at least $350 million for aged equipment, plus $105 million specifically to retire remaining DREs without paper audit trails, and another $230 million to replace post-2010 systems nearing end of life, yielding a replacement liability of roughly $685 million over the coming decade.[10]
- At the county level, recent procurements illustrate the scale: Pennsylvania counties reported replacement packages ranging from about $200,000 for small jurisdictions to $5.8 million for larger counties adopting full Dominion or ES&S suites.[11]

4.2 Ongoing Maintenance and Operational Expenses

Beyond initial acquisition, electronic voting systems generate substantial recurring costs for maintenance, licensing, and support over their useful life.

- Vendor pricing schedules show annual maintenance and extended warranty charges that typically amount to 5–10% of hardware cost per year, with line items such as $640–$1,025 per year per precinct scanner for years 6–10 of service, plus daily charges for on-site support during elections and upgrades.[12]
- At scale, if voting equipment nationwide is valued in the $1–$3 billion range, straightforward depreciation and maintenance assumptions imply $100–$300 million per year in equipment annualization alone, separate from staff, polling places, and other administrative costs.[13]

[7] https://sfa.senate.michigan.gov/Publications/Notes/2015Notes/NotesFal15jc.pdf
[8] https://bipartisanpolicy.org/explainer/federal-election-funding-path/
[9] https://statescoop.com/voting-equipment-replacement-cost-350m/
[10] https://statescoop.com/voting-equipment-replacement-cost-350m/
[11] https://whyy.org/articles/heres-who-makes-money-from-the-voting-machine-requirement-for-pa-counties/
[12] https://procure.ohio.gov/pdf/OT902619_MAC113_ESSPriceSheet.pdf
[13] https://electionlab.mit.edu/sites/default/files/2022-05/TheCostofConductingElections-2022.pdf

Election administration studies indicate that the overall cost to conduct U.S. elections—including personnel, polling locations, printing, technology, and overhead—runs into the billions annually, with electronic systems representing one of the largest single capital and IT expense categories.

4.3 Replacement Liability and Budgetary Exposure

Because EAC-certified systems are replaced in waves, jurisdictions face recurring "spikes" in capital needs to keep electronic equipment current with standards and vendor support.

- The identified $350 million replacement need for aged and obsolete voting machines is in addition to whatever new mandates may arise from future standards, decertifications, or security advisories.[14]
- Federal HAVA grants and one-time security appropriations (such as the $805 million in 2018 and 2020 election security funds) cover only a portion of these costs, leaving states and counties responsible for substantial unfunded capital and maintenance obligations as equipment ages and as vendors phase out support.[15]

4.4 Cost Summary

In aggregate, the current electronic voting paradigm commits governments to an ongoing stream of sizable expenditures: multi-hundred-million-dollar replacement cycles, annual maintenance contracts and support fees, and integration with other election IT systems. These cost commitments, anchored in EAC-certified technologies, form the financial baseline against which any alternative—whether enhanced auditing or a shift toward hand-marked paper ballots—must be evaluated.

5 Security Gaps

We've spent billions of dollars to procure, maintain and secure electronic voting systems. Do we have reason to believe that these measures have been sufficient to ensure the integrity of our elections using machines? Let's examine this question against the backdrop of the critical infrastructure designation for election systems.

5.1 Requirements Rigor

The latest version of EAC-derived requirements for electronic voting systems is VVSG 2.0. VVSG 2.0 significantly improves on prior versions, but when evaluated against the rigor

[14] https://statescoop.com/voting-equipment-replacement-cost-350m/
[15] https://www.eac.gov/sites/default/files/2025-01/EAC_2024_Annual_Report_FINAL_508c.pdf

normally expected for federal Critical Infrastructure, it still exhibits important gaps in scope, depth, and enforceability.

5.1.1 Scope and Threat Model Gaps

VVSG 2.0 focuses on voting systems as discrete products, not on the full election enterprise (EMS networks, domain controllers, remote access tooling, cloud services, vendor support environments), even though federal Critical Infrastructure guidance (e.g., NIST CSF, CISA advisories) assumes end-to-end, system-of-systems risk management.

The requirements mention risk assessment and supply-chain risk management, but at a high level; they do not impose detailed, verifiable controls for firmware provenance, manufacturing geography, component whitelisting, or continuous SBOM-driven vulnerability management that are increasingly standard for other critical sectors.

5.1.2 Network, Access Control, and Identity Gaps

VVSG 2.0 does not categorically prohibit all wireless-capable hardware in certified systems; instead it bans establishing wireless connections and relies on logical controls, leaving residual risk from embedded radios, misconfiguration, or covert channels that other critical sectors would manage via strict hardware bans and independent hardware security reviews.

Access-control requirements mandate multi-factor authentication (MFA) for "critical operations" and administrator accounts, but VVSG 2.0 explicitly does not require full role-based access control, and leaves many deployment patterns to vendor choice within tight MFA technology constraints (no NFC, no Internet-dependent authenticators). That is weaker than typical federal Critical Infrastructure practice, which assumes granular RBAC, centralized identity, and standardized MFA across all privileged access.

5.1.3 Logging, Monitoring, and Incident Response Gaps

VVSG 2.0 meaningfully improve logging—prescribing event types, prohibiting disabling of logs, requiring logs of new physical and logical connections, and mandating firewalls and intrusion detection on networked systems. But it does not specify:

- Minimum log retention durations aligned to 52 U.S.C. 20701 (22 months) in a way that is technically enforceable, tamper-evident, and resilient to "trusted builds."
- Requirements for centralized log aggregation across the election environment, correlation with network and OS logs, or continuous monitoring consistent with NIST SP 800-137-style security operations.

There is no explicit incident-response playbook requirement (containment, eradication, forensics, public communication), which is now routine for other Critical Infrastructure regulatory frameworks.

5.1.4 Configuration Hardening and Vulnerability Management Gaps

VVSG 2.0 calls for "secure configurations and system hardening," removal of non-essential services, exploit mitigation (ASLR, DEP), digital signatures/whitelisting, and malware detection, which are positive steps. However, it does not:

- Define a required secure baseline (e.g., CIS-level benchmark) for OS and database configuration that would preclude practices like default open database ports, generic accounts, and shared passwords.
- Mandate vulnerability scanning, patch-timeliness SLAs, or remediation metrics comparable to CISA's own expectations for federal civilian agencies (e.g., 15 days for critical external vulnerabilities).

The guidelines treat security largely as a design-time property; they provide far less detail on operational security controls, continuous assessment, and post-deployment hardening, even though real-world compromises in other critical sectors overwhelmingly exploit operational drift, not only design flaws.

5.1.5 Governance, Enforcement, and Lifecycle Gaps

VVSG 2.0 is voluntary; adoption and enforcement depend on EAC certification choices and state procurement law. Existing systems certified under older standards may continue in operation indefinitely unless formally decertified. That is fundamentally weaker than Critical Infrastructure regimes that apply mandatory, evolving requirements to all in-scope systems.

The VVSG Lifecycle Policy allows continued sale and use of VVSG 1.0–certified systems while vendors submit new platforms for 2.0 testing, and allows security patches to older systems without full recertification. There is no binding requirement to retire or upgrade legacy equipment by a date certain, even if it cannot meet 2.0-level controls.

Supply-chain provisions require a "strategy" but do not impose independent third-party audits, continuous vendor-risk monitoring, or federal approval of critical suppliers, as is increasingly common for electric, pipeline, and telecom sectors.

5.1.6 Summary: Critical Infrastructure vs. VVSG 2.0

Against the standard of other federally designated Critical Infrastructure, the main gaps in VVSG 2.0 are:

- System boundary: focuses on the voting device and EMS, not the full enterprise and vendor environments.
- Operational security: limited guidance on continuous monitoring, vulnerability management, and incident response.
- Identity and access: no full RBAC requirement and constrained, fragmented MFA implementation relative to federal best practice.
- Supply chain: high-level risk-management language without concrete, enforceable controls commensurate with foreign hardware/software risk.
- Enforcement: voluntary, non-retroactive adoption, with no hard deadlines for migrating off weaker, legacy systems.

VVSG 2.0 is a substantial improvement over earlier standards, but as a security regime for systems designated as Critical Infrastructure, it remains less prescriptive, less comprehensive, and less enforceable than frameworks applied to other high-consequence sectors.

5.2 Analysis Rigor

We now examine whether or not the analysis rigor applied to electronic voting systems is commensurate with their critical infrastructure designation.

5.2.1 CISA Cyber Risk Assessment Gaps

CISA's Cyber Risk Assessment depicts U.S. election infrastructure as a highly networked, variably secured critical-infrastructure ecosystem with persistent, exploitable weaknesses, while the EAC's election-system oversight is narrowly product-centric, episodic, and largely detached from those systemic cyber-risk realities.[16]

5.2.1.1 Scope: Ecosystem vs. Device

CISA defines "election infrastructure" broadly—voter registration systems, e-pollbooks, ballot preparation, voting-machine preparation, central tabulation, websites, storage, polling places, and election offices—and evaluates confidentiality, integrity, and

[16] https://www.cisa.gov/sites/default/files/publications/cisa-mail-in-voting-infrastructure-risk-assessment_508.pdf

availability risks across this whole ecosystem, including preparation and networking states.

The EAC's formal authority and practice focus on certifying voting systems (e.g., Dominion D-Suite 5.5-B) against VVSG and managing field anomalies at the device/system level (e.g., the ICP QR-code/provisional flag bug in Williamson County). The EAC investigation did not address county network exposure, patch posture, spear-phishing risk, or broader IT vulnerabilities that CISA identifies as major attack vectors.[17]

5.2.1.2 Risk Posture vs. Certification Assumptions

CISA's EI-subsector summary shows that, in the wake of the 2020 election, among assessed entities, 76% had spear-phishing weaknesses, 48% had at least one critical/high vulnerability on an internet-accessible host, 39% exposed risky services (FTP, RDP, SMB, SQL, etc.), and 34% ran unsupported OS on at least one internet-facing host. CISA also reports median remediation times of 103.7 days for critical vulnerabilities and 91.9 days for high vulnerabilities, far beyond its own 15/30-day expectations.

EAC certification and the Williamson County investigation implicitly assume that if firmware and configuration hashes match the certified "trusted build" and functional tests pass, risk is acceptably controlled. That model does not account for the real-world environment CISA describes, where compromised domain controllers, RDP, VPNs, or email provide ready paths to EMS networks and tabulation components, regardless of their formal certification status.[18]

5.2.1.3 Threat Model and Attack Surface

CISA emphasizes that attacks on preparation processes (ballot programming, voting-machine setup, tabulation prep) and centralized infrastructure can scale to entire jurisdictions or states; it explicitly warns that network connectivity and centralization multiply risk, and that even "best-practice" jurisdictions remain vulnerable to nation-state-level adversaries.

The EAC's oversight tools—VVSG conformance, VSTL testing, and post-hoc anomaly investigations—do not systematically test or monitor how certified systems are actually deployed in those higher-risk preparation networks, nor how vendor tools, remote support, or connected enterprise services change the attack surface. There is no EAC requirement

[17] https://www.eac.gov/sites/default/files/2022-03/EAC_Report_of_Investigation_Dominion_DSuite_5.5_B_0.pdf
[18] https://www.eac.gov/sites/default/files/2022-03/EAC_Report_of_Investigation_Dominion_DSuite_5.5_B_0.pdf

or process comparable to CISA's continuous vulnerability scanning or RVA/RPT campaigns across election-office IT.[19]

5.2.1.4 Controls: Recommended vs. Required

CISA prescribes concrete mitigations—aggressive patch management, segmentation, removal of unsupported OS, restriction of risky services, phishing training, and formal incident-response plans—and quantifies how implementing "recommended controls" changes attack difficulty and residual risk in its prioritization matrix.[20]

EAC VVSG requirements, by contrast, are voluntary for states, narrowly scoped to voting systems, and do not impose binding expectations on county IT networks, vulnerability remediation timeframes, or phishing defenses that CISA views as central to election security. The Williamson County case shows that EAC intervention ended once a software ECO cleared a specific device anomaly; there was no parallel effort to ensure that the surrounding infrastructure met CISA-level hygiene.[21]

5.2.1.5 Governance and Accountability

CISA treats election infrastructure as a National Critical Function and explicitly warns that "nearly any capable threat actor" can compromise low-control environments, urging continuous collaboration, scanning, and risk-based mitigation across all components.

The EAC remains primarily a standards-setter and certifier of products; its anomaly process is reactive and case-by-case, focused on decertification risk for specific systems rather than on systemic cyber-risk reduction across the designated critical infrastructure subsector.[22]

In sum, CISA's assessments reveal an environment with broad, persistent cyber weaknesses in the networks and processes that surround voting systems, while the EAC's oversight regime addresses only a narrow slice of that risk and does so through static, front-end certification and limited, post-incident investigations, leaving major CISA-identified risk vectors outside EAC's effective control.[23]

[19] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf
[20] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf
[21] https://www.eac.gov/sites/default/files/2022-03/EAC_Report_of_Investigation_Dominion_DSuite_5.5_B_0.pdf
[22] https://www.eac.gov/sites/default/files/2022-03/EAC_Report_of_Investigation_Dominion_DSuite_5.5_B_0.pdf
[23] https://www.eac.gov/sites/default/files/2022-03/EAC_Report_of_Investigation_Dominion_DSuite_5.5_B_0.pdf

5.2.2 Failure Modes and Effects Analysis

Failure Modes and Effects Analysis (FMEA) is a mature, engineering-grade method for identifying how complex systems can fail, what the consequences of those failures are, and which failure modes demand priority mitigation. In its classical form, FMEA proceeds bottom-up: for each component or process step, analysts enumerate possible "failure modes," assess the effects on the larger system, and then prioritize them using factors such as severity, likelihood of occurrence, and difficulty of detection. Software FMEA (SFMEA) extends this technique to software[24], treating security-relevant behaviors—such as unauthorized access, silent data alteration, or logging failures—as failure modes whose downstream impacts must be explicitly traced and mitigated.

Recent election-security research demonstrates how SFMEA can be applied directly to U.S. voting systems, particularly precinct-count optical scanners (PCOS). Building on the Election Assistance Commission's own 2009 PCOS threat trees, Towson University researchers used SFMEA to identify more than 60 additional threats and integrate them into an updated, bi-directional risk model that combines SFMEA with attack-tree analysis. Each threat was categorized as cyber, physical, or insider, assigned to a phase of the election process (pre-election, election day, post-election), and rated by attack cost, technical difficulty, and discovery difficulty via a Delphi panel of subject-matter experts. The resulting model now contains over 310 terminal threats and more than 60,000 minimal cut sets—concrete, multi-step attack scenarios that can compromise PCOS integrity.

Placed next to the EAC's current security posture, this kind of structured SFMEA-driven analysis exposes several gaps:

5.2.2.1 Static, incomplete threat models.

The EAC's 2009 PCOS threat trees were never systematically updated to reflect emerging cyber, physical, and insider threats, nor were their leaf nodes characterized by attack cost, technical difficulty, detectability, or relative likelihood. By contrast, SFMEA explicitly forces analysts to enumerate new failure modes, trace their effects, and quantify their practical risk, revealing substantial threat surface that current EAC artifacts simply omit.[25]

5.2.2.2 Device-centric, not failure-centric oversight.

EAC certification and investigations center on whether particular devices and software builds meet VVSG requirements and function correctly under test, as illustrated by the Williamson County Dominion D-Suite anomaly inquiry. SFMEA starts from the opposite

[24] https://www.sos-vo.org/system/files/2025-10/ASEM_2025_-_Abstract__185_-_Final.pdf
[25] https://www.sos-vo.org/system/files/2025-10/ASEM_2025_-_Abstract__185_-_Final.pdf

direction: for each function and process (e.g., EMS configuration, PCOS deployment, chain-of-custody, credential management), it asks "how can this fail or be misused—by code, by configuration, or by people—and what would the system-level effect be?" That orientation aligns more closely with the real-world failure patterns CISA documents in election infrastructure—phishing, unpatched systems, risky services, and weak detection—than the EAC's narrow focus on "trusted builds."

5.2.2.3 Lack of risk-based prioritization of mitigations.

Under the current regime, VVSG security requirements are largely flat: the guidelines enumerate controls, but provide little structured basis for prioritizing which failures and attack paths most urgently require mitigation or decertification action. SFMEA, especially when combined with expert scoring, produces precisely that: a ranked list of high-severity, high-likelihood, hard-to-detect failure modes tied to specific components and processes. This enables regulators to target requirements and enforcement where they yield the greatest reduction in systemic risk—for example, privileging mitigations against insider-enabled misconfiguration or credential theft over low-impact, easily detected faults.

5.2.2.4 Fragmented treatment of insider and process risk.

The EAC's standards and reports concentrate on technical properties of voting equipment and formal procedures, but they do not embed a rigorous model of insider behavior or process failures into the security analysis itself. The Towson SFMEA-driven work explicitly includes insider failure modes—such as poll-worker lapses, improper seal handling, or administrative misuse—alongside cyber and physical threats, and traces how these can combine into minimal attack cut sets that defeat technical controls. That approach reflects the socio-technical reality CISA describes for critical infrastructure, where human factors are as pivotal as code vulnerabilities.[26]

5.2.2.5 Absence of a structured "assurance case" for election systems.

In other safety-critical sectors (nuclear, aviation, rail), regulators increasingly expect system owners to maintain explicit safety or assurance cases built from systematic analyses such as FMEA and fault trees. Election systems, despite their critical-infrastructure designation, lack comparable, regulator-mandated threat analysis cases that demonstrate the system has been thoroughly examined for cyber, physical, and insider risks and that residual risk is acceptable. The SFMEA + attack-tree framework provides exactly the scaffolding needed to construct such cases for voting systems, but the

[26] https://www.cisa.gov/sites/default/files/publications/cisa-mail-in-voting-infrastructure-risk-assessment_508.pdf

EAC has not yet incorporated this level of structured risk argument into its certification, monitoring, or decertification processes.[27]

5.2.2.6 The Case for FMEA

In sum, FMEA and SFMEA highlight that the EAC's security analysis is narrow, static, and device-centric, whereas critical-infrastructure-grade assurance requires dynamic, failure-centric modeling that spans software, hardware, processes, and human actors. Adopting SFMEA-based methods—as exemplified by the updated PCOS threat model—would allow the EAC to move from certifying individual builds against a checklist to governing election technology through a transparent, quantitative understanding of how it can fail and how those failures can be prevented, detected, or contained.

5.2.3 Supply Chain

The EAC's security analysis remains tightly bounded by VVSG device- and software-conformance and does not incorporate the level of supply-chain scrutiny that Congress now applies to other critical systems, including explicit statutory prohibitions on procuring covered technologies from foreign adversaries in the FY2019 and FY2023 National Defense Authorization Acts (NDAAs).

5.2.3.1 Limited EAC Scope vs. Federal Prohibitions

EAC certification and scopes of conformance formally attest that a particular voting system configuration has been tested by an accredited lab and shown to meet VVSG functional and security requirements in a controlled environment. These artifacts do not constitute a comprehensive audit of upstream component provenance, fabrication geography, or supplier ownership. Test plans and reports for major systems (ES&S, Dominion, Smartmatic) describe architecture and software behavior but generally stop at the vendor's system boundary; they do not map or vet underlying chips, boards, radios, or other subcomponents against foreign-adversary risks. This narrow scope stands in sharp contrast to broader federal procurement rules that recognize the national-security implications of foreign-sourced information and communications technology (ICT).

In the FY2019 NDAA, Congress enacted Section 889, which prohibits federal agencies and federal grant recipients from procuring or using telecommunications and video-surveillance equipment or services from specified Chinese companies (Huawei, ZTE, Hytera, Hikvision, Dahua, and their affiliates) where such equipment is a substantial or essential component of any system, or critical technology as part of any system. Implementing regulations (FAR 52.204-25) extend this prohibition to covered equipment or

[27] https://swehb.nasa.gov/display/SWEHBVC/8.05+-+SW+Failure+Modes+and+Effects+Analysis

services used by contractors themselves, underscoring that the federal government regards embedded Chinese ICT in critical systems as a systemic national-security risk, not a mere commercial detail.

More recently, the FY2023 NDAA and related measures expand similar logic to other critical technologies and sectors—for example, tightening prohibitions on unmanned aircraft systems and certain semiconductor products from China, Russia, Iran, and North Korea when used in "critical systems," i.e., national-security systems that handle sensitive command, control, or intelligence functions. While these provisions do not yet explicitly name election equipment, they codify a clear federal policy trajectory: critical infrastructure should not rely on components or platforms tied to foreign adversaries for core functions.

5.2.3.2 Gap Between EAC Certification and Supply-Chain Risk Policy

Despite this policy environment, EAC security analysis does not currently:

- Require comprehensive hardware or software bills of materials (HBOM/SBOM) that would allow election officials or federal partners to check for covered Chinese or other adversary-linked components within certified systems.[28]
- Align certification decisions with Section 889-style prohibitions—e.g., by screening voting-system subcomponents and vendor networks for covered telecommunications or surveillance technologies, or by conditioning certification on demonstrated compliance with these federal procurement standards when systems are funded with federal grants.[29]
- Integrate NDAA-driven foreign-adversary restrictions on critical technologies (e.g., legacy chips or control systems produced in China and other covered countries) into its evaluation of whether a system is appropriate for use in designated critical-infrastructure election environments.[30]

Because EAC campaigns remain device- and software-centric, voting systems can be fully "EAC certified" while:

[28] https://electionline.org/wp-content/uploads/2021/02/Supply_Chain_White_Paper_2021-1.pdf
[29] https://www.wiley.law/alert-Interim-Rule-Banning-Huawei-and-Other-Chinese-Telecommunications-Equipment-and-Services-to-Take-Effect-on-August-13-2019
[30] https://www.wiley.law/alert-Interim-Rule-Banning-Huawei-and-Other-Chinese-Telecommunications-Equipment-and-Services-to-Take-Effect-on-August-13-2019

- Embedding Chinese-manufactured ICT components that would be banned from many other federal critical-system procurements under Section 889.[31]
- Lacking any documented assurance that their semiconductor, networking, or storage components are free of adversarial control or susceptible to the same coercive leverage and disruption risks that led Congress to prohibit such equipment elsewhere.[32]

5.2.3.3 Consequences for Election Infrastructure

For election systems—formally designated as critical infrastructure—this creates a material assurance gap. Federal law now recognizes that allowing adversary-linked ICT into critical telecom, surveillance, UAS, and semiconductor supply chains presents unacceptable risk, and it has imposed binding prohibitions and contractor-wide usage bans in those domains. Yet the EAC's security analysis and certification processes have not been updated to reflect or enforce analogous safeguards for election equipment, even though the same classes of components (network interfaces, embedded controllers, storage, FPGAs, legacy chips) are present.

The result is that states can deploy EAC-certified voting systems that meet VVSG functional criteria but would fail Section 889-style scrutiny if they were treated as federal critical systems for procurement purposes—a misalignment that leaves election infrastructure exposed to foreign-sourced hardware and software risks that Congress has already deemed intolerable in other critical sectors.

5.3 Configuration Management Rigor

Configuration-management failures in the development, testing, configuration, and deployment of election systems have produced concrete, exploitable security risks that are not meaningfully addressed by current EAC security analysis. These risks are amplified by dependence on third-party platforms such as SolarWinds, whose own configuration and update-pipeline weaknesses have already enabled a nation-scale compromise affecting U.S. government and critical-infrastructure networks, including networks in the elections space.

5.3.1 Insecure third-party platforms and SolarWinds-style risks

The SolarWinds Orion compromise demonstrated how a single vendor's mismanaged configuration and update environment can become a universal attack vector into

[31] https://www.eac.gov/what-section-889-fy-2019-ndaa
[32] https://www.ndtahq.com/protecting-us-supply-chains-from-foreign-influence/

government and critical-infrastructure customers, including entities supporting election operations.

- SolarWinds' Orion software was compromised via its build/update process, allowing attackers to ship signed, trojanized updates that were then installed by thousands of customers, including U.S. federal agencies, state and local entities, and critical-infrastructure operators.[33]
- Public reporting and SEC filings describe weak internal controls, including poor password management (e.g., the "solarwinds123" password exposed on an internet-facing server) and insufficient hardening of update and remote-access services.[34]
- CISA itself used SolarWinds products and later issued guidance acknowledging that Orion and related components were present in SLTT and critical-infrastructure networks, including those tied to election infrastructure, requiring emergency detection and mitigation.[35]

Election-system vendors and many state and local jurisdictions have also used SolarWinds monitoring and configuration tools; this means that any EMS, voter-registration, or supporting system reachable from an Orion-monitored network segment could have been exposed to the same supply-chain intrusion vector. EAC's certification and security documentation, however, do not substantively address how such third-party platform risks are modeled, mitigated, or monitored over time.

5.3.2 Development and test-pipeline weaknesses in certified systems

Configuration management is not only a deployment issue; it starts in development and test pipelines where insecure components, libraries, and tools can be introduced and then propagated into "trusted builds."

- CISA's Election Infrastructure Subsector Cyber Risk Summary, based on vulnerability scanning and assessments for the 2020 cycle, found that 48% of election-infrastructure entities had at least one internet-accessible host with a critical or high-severity vulnerability, and 34% ran unsupported operating systems

[33] https://www.sec.gov/newsroom/press-releases/2023-227
[34] https://thehackernews.com/2021/03/solarwinds-blame-intern-for-weak.html
[35] https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack

on internet-facing hosts, indicating chronic weakness in patch, lifecycle, and configuration management across the ecosystem.[36]

- The same report documents that 39% of entities exposed "potentially risky services" (FTP, RDP, SMB, SQL, etc.) to the internet; FTP alone was present at 27.9% of entities, despite well-known abuse of FTP for credential theft and arbitrary file delivery by malware families such as LokiBot.
- In Mesa County, forensic analysis of a Dominion Democracy Suite EMS server used in 2020 showed that Microsoft SQL Server Management Studio (SSMS)—a powerful, general-purpose database tool not listed in the vendor's certification application or lab report—had been installed and left in place on the EMS since 2017, enabling direct back-end access to all election databases outside the certified application layer.[37]

Together, these findings mirror SolarWinds' pattern: insecure components and mismanaged services are introduced during development and testing, are not fully mitigated or removed before release, and then propagate into many production environments under the cover of compliance language and certifications that do not track real-world configurations.

5.3.3 Misconfigured network, firewall, and service configurations in deployment

In the field, EAC-certified systems have been deployed with network and service configurations that directly contradict basic security principles, creating conditions analogous to those exploited in SolarWinds-related intrusions.

- The Mesa EMS server's SQL Server instance was configured with TCP/IP, Named Pipes, and Shared Memory all enabled, listening on the default port 1433 bound to all interfaces, and protected by a custom Windows firewall rule that explicitly allowed inbound SQL connections from "any IP address worldwide," rather than restricting access to a small set of internal hosts.[38]
- Forensic testing demonstrated that, once a network path existed (including via a wireless access point added to emulate existing wireless-capable devices), a non-Dominion Windows workstation and even an iPhone running a commodity SQL

[36] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf
[37] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf
[38] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-3-signed.pdf

client could connect directly to the EMS database, read data, and modify vote records, all without passing through Dominion's certified application controls.[39]

- CISA's assessment data show that many EI entities already run exposed administrative interfaces and leave critical and high-severity vulnerabilities unremediated for 90 days or more, a combination that is ideal for attackers using SolarWinds-style lateral-movement techniques (credential dumping, pass-the-hash, exploitation of unpatched services) to pivot from compromised monitoring platforms into EMS or voter-registration systems.[40]

EAC's security narratives emphasize "trusted builds" and penetration testing of reference configurations, but there is no evidence of robust, ongoing verification of actual deployed configurations or enforcement of least-privilege firewall and service policies. This gap allows SolarWinds-class attack paths (compromised management software plus weak internal network segmentation) to remain open in certified environments.

5.3.4 Logging, auditability, and "trusted build" practices

SolarWinds underscored how critical detailed logs and configuration histories are to detecting and scoping sophisticated intrusions. Under EAC-aligned processes, logging and configuration evidence necessary to reconstruct attacks have been actively destroyed or allowed to be overwritten.[41]

- In Mesa County, comparison of pre- and post-"trusted build" forensic images of the same EMS server revealed that 28,989 files were deleted during a state-mandated Dominion upgrade, including at least 695 log and event-log files required to reconstruct system behavior.
- Deleted and overwritten files included IIS web-server logs, SQL Server installation and error logs, Windows Defender logs, and multiple Windows event-log archives, all within the 22-plus-month statutory record-retention window, and all explicitly needed to confirm or exclude unauthorized access, configuration changes, or exploitation of known vulnerabilities.
- Vendor-supplied and Secretary-of-State-approved procedures configured log retention as small circular buffers and did not require full log preservation prior to

[39] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[40] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf
[41] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf

destructive updates, despite the 2002 Voting Systems Standards' clear requirement for comprehensive, durable audit trails.

This practice functionally replicates one of the central problems in the SolarWinds incident: a lack of complete, tamper-resistant telemetry about build, deployment, and runtime behavior. EAC's endorsement of "trusted builds" that destroy or overwrite core logs leaves election systems with little forensic resilience against SolarWinds-style supply-chain or lateral-movement attacks.

5.3.5 Data-layer design and configuration vulnerabilities

Beyond network and OS configuration, weaknesses in the internal data model and database configuration of certified systems create additional risk pathways that traditional penetration tests and high-level EAC reviews do not appear to cover.

- Mesa forensic analysis showed that Dominion's TabulationStore and AdjudicableBallotStore databases lacked strong referential-integrity constraints, enabling batches and ballots to be added, removed, or reassigned without database-level errors or obvious inconsistencies in EMS front-end reports.[42]
- The same analysis documented mid-election creation of new tabulation and adjudication databases, with selected batches copied from original databases into the new ones and others omitted, using sequences of operations not available through normal EMS functions accessible to county officials.[43]
- Expert testimony further indicates that Dominion software stores passwords and encryption-related material in plain text within database and configuration files, making it feasible for an attacker who gains system or backup access—through any of the network, OS, or supply-chain paths described above—to escalate privileges and modify votes "indetectably" from within the data layer.[44]

These are configuration and design problems inside the certified application stack itself, not just in surrounding infrastructure. EAC's focus on disproving a "single master key" across vendors does not address the existence of reusable architectural flaws that can be exploited wherever the same schema and code are deployed, analogous to the reuse of Orion update mechanisms across SolarWinds' customer base.[45]

[42] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[43] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[44] https://electioncrimebureau.com/wp-content/uploads/2025/09/922651931-70-2-Exhibit-PM-Transcript-of-EUO-Confidential-Witness.pdf
[45] https://www.sec.gov/newsroom/press-releases/2023-227

5.3.6 Implications for EAC security analysis

Taken together, these demonstrated lapses show that EAC's current security analysis framework does not adequately account for configuration-management risk across the full lifecycle of election systems, particularly in the face of SolarWinds-class supply-chain threats.

- In development and testing, neither EAC nor state processes appear to enforce strict control over auxiliary tools (e.g., SSMS), password storage practices, or third-party monitoring platforms (e.g., SolarWinds) whose compromise would expose the election environment.
- In configuration and deployment, certified systems have been operated with globally permissive firewall rules, exposed database services, wireless-capable components, and out-of-band management controllers, all of which provide potential paths for attackers who have already compromised a SolarWinds-like platform or another foothold in the network.
- In operations and post-election maintenance, "trusted build" and log-retention practices have destroyed essential audit data, making it impossible to reliably determine whether SolarWinds-style intrusions, configuration changes, or data-layer manipulations have occurred.[46]

These gaps show that EAC's emphasis on source-code escrow, lab testing, and static certification artifacts falls far short of the continuous, configuration-centric security oversight that modern supply-chain and platform compromises—of which SolarWinds is the clearest example—have proven to be essential for protecting U.S. election systems.

5.4 Credential Management Rigor

Credential-management failures in EAC-covered election systems create direct, demonstrated attack paths to alter election data, bypass auditing, and replicate the same classes of weaknesses that made the SolarWinds compromise possible. These lapses span weak and shared passwords, plaintext storage of decryption keys, use of generic administrative accounts, exposure of BIOS passwords, and insecure third-party platforms, and they are not adequately addressed by current EAC security analysis or certification practices.[47]

[46] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf
[47] https://electioncrimebureau.com/wp-content/uploads/2025/09/922651931-70-2-Exhibit-PM-Transcript-of-EUO-Confidential-Witness.pdf

5.4.1 Plain-text passwords, decryption keys, and generic EMS accounts

Forensic examinations and sworn testimony show that critical EMS credentials and decryption keys are stored in plain text and routinely tied to generic accounts, making compromise both easy and difficult to attribute.

- A confidential technical witness who examined Dominion systems, including the Mesa County EMS image, testified that Dominion software stores passwords "in plain text," recoverable from databases, election backups, configuration files, and the physical "button" device, allowing anyone with file-system access to extract valid credentials without cracking.[48]
- The same witness explained that once these plaintext credentials and associated encryption "levers" are obtained, an attacker can manipulate the system and "change votes at will," while using the vendors' own processes so that standard audits cannot distinguish genuine from falsified data.[49]
- Mesa forensic reports further document that the EMS server relied on generic Windows user IDs and shared administrative accounts, directly violating VSS requirements for individual accountability, and that these accounts—plus any plaintext decryption or database credentials stored on the server—were fully exposed via unauthorized tools such as Microsoft SQL Server Management Studio (SSMS).[50]

When powerful, generic EMS accounts exist and their passwords and keys are stored in clear text, a single host-level compromise immediately yields untraceable, system-wide control over election data.

5.4.2 Internet exposure of BIOS passwords and device-level control

Credential-management failures extend into firmware and hardware, where exposure of BIOS passwords undermines any assumption of device-level integrity for certified systems.

- Public reporting and case materials describe how the Colorado Secretary of State's office, under Jena Griswold, left hundreds of BIOS passwords for voting-system

[48] https://electioncrimebureau.com/wp-content/uploads/2025/09/922651983-70-1-Exhibit-AM-Transcript-of-EUO-Confidential-Witness.pdf
[49] https://electioncrimebureau.com/wp-content/uploads/2025/09/922651931-70-2-Exhibit-PM-Transcript-of-EUO-Confidential-Witness.pdf
[50] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf

devices accessible over the internet, including passwords controlling low-level hardware configuration and boot security.[51]

- BIOS passwords protect the ability to alter boot order, enable or disable USB and network interfaces, and change firmware security settings; publishing them effectively gives adversaries a roadmap to bypass or weaken hardware protections once they gain physical or remote presence in a county environment.
- In Colorado Dominion deployments, these exposed BIOS passwords coexist with out-of-band management controllers (Dell iDRAC) and multiple wireless-capable components, significantly increasing the risk that attackers can reconfigure firmware, implant persistent code, or attach unauthorized devices beneath the operating system and EMS software.[52]

EAC's certification framework, which focuses on software and "trusted builds," does not meaningfully address how publicly exposed BIOS-level credentials compromise the trustworthiness of certified hardware in the field.

5.4.3 Weak, shared, and generic credentials in critical roles

As SolarWinds demonstrated, a single weak or exposed credential on a critical service can open an entire ecosystem to compromise; election infrastructure mirrors this pattern through weak, shared, and generic credentials, especially for administrative functions.

- A researcher discovered that SolarWinds used the trivial password "solarwinds123" for an internet-facing update/FTP server and that these credentials were exposed in a public GitHub repository, enabling outsiders to upload malicious files into the vendor's update pipeline.[53]
- The SEC's case against SolarWinds alleges that the company repeatedly failed to enforce its own password policies, allowed unencrypted passwords, and granted excessive administrative privileges, even as it publicly touted strong access controls.[54]
- Mesa County's EMS server used generic user IDs and shared administrative passwords as the primary means of controlling access, with no multi-factor authentication and no binding of high-risk operations to uniquely identified users;

[51] https://statescoop.com/colorado-voting-system-passwords-leak-secretary-state-griswold/
[52] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf
[53] https://thehackernews.com/2021/03/solarwinds-blame-intern-for-weak.html
[54] https://www.sec.gov/newsroom/press-releases/2023-227

this structure makes it impossible to prove which individual, if any, performed a given change.[55]

- Widespread use of generic "admin," "emsadmin," or county-wide accounts in election offices, coupled with shared passwords, means that once a single shared credential is phished, guessed, or captured, an attacker can impersonate multiple roles without leaving an individualized audit trail.

These practices directly contradict the individual accountability and least-privilege principles embedded in the VSS and VVSG, yet they persist in EAC-certified deployments.

5.4.4 Sector-wide exposure to credential theft and risky services

CISA's election-infrastructure data show that many EI entities operate with risky, internet-exposed services and unpatched systems ideal for credential-stealing malware and password attacks, which interact dangerously with generic and plaintext credentials on EMS systems.

- The Election Infrastructure Subsector Cyber Risk Summary found that 48% of EI entities had at least one internet-accessible host with a critical or high-severity vulnerability, and 39% ran "potentially risky services" such as FTP, RDP, SMB, and SQL directly exposed to the internet.[56]
- FTP was the most prevalent risky service, present at 27.9% of EI entities; CISA has warned that malware like LokiBot specifically targets credentials for services such as FTP by scraping configuration files and keylogging, then reusing those credentials across victim networks.[57]
- EI entities also showed high susceptibility to phishing: 73% of entities in risk and vulnerability assessments exhibited spear-phishing weaknesses, and election entities had a higher phishing click-rate than other SLTT and critical-infrastructure sectors, increasing the likelihood that generic and admin credentials are captured.[58]

[55] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[56] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf
[57] https://www.techtarget.com/healthtechsecurity/news/366595559/DHS-CISA-Alerts-to-Rise-in-Credential-Theft-Focused-LokiBot-Malware
[58] https://www.techtarget.com/healthtechsecurity/news/366595559/DHS-CISA-Alerts-to-Rise-in-Credential-Theft-Focused-LokiBot-Malware

In environments where generic EMS accounts exist, passwords and keys are stored in plain text, and BIOS passwords are public, any successful credential-theft campaign can very rapidly escalate into full control over election systems.

5.4.5 Authentication, authorization, and audit gaps

The way access control and logging are implemented in EAC-covered systems amplifies credential-management risk by allowing shared identities, broad privileges, and missing or destroyed audit trails.

- Mesa analysis shows that EMS and SQL access relied on shared administrative accounts and Windows Authentication from any host on the same network (with firewall rules allowing connections from "any IP address worldwide"), so any compromised generic account could directly connect to election databases.[59]
- The Colorado "trusted build" process deleted or overwrote at least 695 log and event-log files on the Mesa EMS server, including Windows event logs, IIS logs, SQL logs, and Windows Defender logs, wiping the evidence needed to reconstruct misuse of generic accounts, credential-stuffing attempts, or privilege escalation.[60]
- CISA's EI report highlights exposed administrative interfaces, unencrypted transmission of sensitive data, and poor patch management as common findings, all of which become far more severe when authentication is based on shared, generic accounts and plaintext passwords.[61]

These factors mean that even when attackers exploit generic or exposed credentials, there may be no durable, per-user trace of their actions—yet EAC security assurances continue to rely on claims of auditability and controlled configurations.

5.4.6 Interaction with SolarWinds-class supply-chain compromises

SolarWinds demonstrates how credential failures at a vendor and customer level can combine to produce deep, long-lived compromises; the same dynamic exists in election environments that use SolarWinds-like platforms alongside weak local credential practices.

[59] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[60] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf
[61] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf

- The SUNBURST campaign abused trojanized Orion updates and weak internal controls to harvest credentials inside victim networks, then moved laterally into sensitive systems across federal, SLTT, and critical-infrastructure environments.[62]
- CISA and others confirm that SolarWinds products were deployed on government and critical-infrastructure networks, including those supporting election processes, which had to assume that credentials, tokens, and administrative accounts may have been compromised.[63]
- In election environments where EMS servers hold plaintext decryption keys and passwords, where generic EMS admin accounts are widely used and BIOS passwords are publicly known, any SolarWinds-style foothold—or similar compromise of a third-party management platform—can be leveraged swiftly into auditable-resistant manipulation of election systems at scale.[64]

EAC certification does not currently impose or verify robust credential-management standards across this chain—from vendor build systems and platform credentials, through BIOS and firmware passwords, down to local EMS admin accounts and database keys—despite clear evidence that failures at each layer have already occurred.

5.4.7 Credential Management Summary

Overall, the presence of plaintext decryption keys and passwords on EMS servers, the documented exposure of hundreds of BIOS passwords on the internet by the Colorado Secretary of State's office, the widespread use of generic and shared administrative accounts, and sector-wide susceptibility to credential theft demonstrate a systemic credential-management failure under EAC's watch. Any serious security evaluation of U.S. election systems must treat these credential-management lapses—including generic admin accounts—as central attack vectors, comparable in importance to the credential and access-control failures that enabled the SolarWinds supply-chain attack.

5.5 Circle of Trust

Do we have sufficient grounds for trust in those responsible for ensuring our systems are secure?

---

[62] https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
[63] https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack
[64] https://electioncrimebureau.com/wp-content/uploads/2025/09/922651983-70-1-Exhibit-AM-Transcript-of-EUO-Confidential-Witness.pdf

A tightly interlinked "circle of trust" built around vendors, former vendor staff now inside the EAC, the two VSTLs, CIS, and potentially compromised state and local officials creates a structurally unsound security regime in which the same actors who design, configure, and defend systems are effectively asked to police their own failures, including failures with direct foreign-adversary implications.[65,66]

5.5.1 Conflicted governance and revolving doors

The EAC's reliance on personnel and laboratories with deep vendor and industry ties means that design, testing, certification, and "independent" review are concentrated in a small, homogeneous community that shares assumptions and incentives.

- Mesa forensic reports document an illegally certified Dominion configuration in Colorado that still passed through the EAC/VSTL pipeline, despite uncertified software, disabled auditability, and firewall rules that allowed global database access, showing that this circle repeatedly failed to identify even gross violations of the 2002 VSS.
- When former vendor employees or vendor-aligned experts rotate into EAC or state roles, they import the same architectures, justifications, and threat models they previously sold, making it less likely that fundamental design defects or supply-chain risks will be challenged rather than rationalized.

In such a governance model, "oversight" often becomes a process of documenting compliance narratives rather than independently challenging insecure designs.

5.5.2 Vendors and foreign-adversary supply chains

Vendor systems under EAC jurisdiction incorporate hardware manufactured and assembled in foreign environments that U.S. intelligence has explicitly identified as high-risk for hostile supply-chain operations.

- The Mesa EMS server hardware was assembled in Mexico with a motherboard manufactured in China; the forensic report cites U.S. government and DNI warnings about foreign intelligence entities exploiting global supply chains to implant hardware or firmware backdoors in precisely this kind of critical infrastructure equipment.[67]

[65] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[66] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf
[67] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf

- Despite those warnings, EAC certification and VSTL testing did not require any meaningful mitigation of foreign-manufacturing risk—no systematic teardown, no hardware provenance validation, no disabling of back-channel management engines such as Intel ME or Dell iDRAC that enable out-of-band control invisible to operating-system logs.[68]

By treating these systems as ordinary COTS servers while simultaneously declaring them "critical infrastructure," the circle of trust accepts foreign-adversary attack surfaces that would be intolerable in defense or intelligence contexts.

5.5.3 VSTLs, CIS, and the illusion of independent assurance

The two VSTLs and organizations such as CIS are frequently cited as independent validators, but their assessments occur within a tightly bounded scope and rely heavily on vendor-supplied configurations and documentation.[69]

- Mesa reporting shows that Colorado certification relied on testing by an unaccredited lab and still failed to detect uncertified software, open SQL ports accessible from "ANY IP ADDRESS worldwide," and disabled logging—defects any competent security lab should have identified immediately.
- CISA's own Election Infrastructure Subsector Cyber Risk Summary acknowledges that 48% of EI entities had at least one internet-accessible host with a critical or high-severity vulnerability, 39% ran risky services such as FTP, RDP, SQL, and SMB directly on the internet, and 34% ran unsupported operating systems on public-facing hosts, confirming that whatever CIS and VSTLs are doing is not preventing systemic exposure.

The result is a layered but self-referential assurance stack: vendors configure, VSTLs test to vendor-driven scopes, CIS publishes "best practices" often not implemented, and EAC cites those same actors as proof of security.

5.5.4 Corrupt or captured state and local officials

When state and county officials are either politically captured or directly implicated in misconfiguration and record destruction, their participation in this circle of trust becomes a liability rather than a safeguard.

[68] https://www.eac.gov/sites/default/files/TestingCertification/VSTL_Program_Manual_Version_3_0.pdf
[69] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf

- Mesa County forensic work documents that the Colorado Secretary of State's "trusted build" process erased at least 695 log and event files on the EMS server—including Windows, IIS, SQL, and Defender logs—destroying mandated election records and the very evidence needed to verify absence of intrusion or misuse.[70]
- The same state office approved a configuration that used generic administrative accounts, left 36 wireless-capable components in the election environment, permitted global SQL access, and relied on self-signed encryption vulnerable to man-in-the-middle attacks, all while publicly asserting that systems were "secure," "air-gapped," and rigorously tested.[71]

In such conditions, local certification and procedural sign-offs are not independent checks; they are part of the failure surface that EAC security analysis must assume is compromised.

5.5.5 Compound risk to systems under EAC watch

When these elements are combined—foreign-manufactured platforms, vendor-centric designs, VSTLs and CIS operating inside the same ecosystem, and state/local officials willing to violate logging and record-retention laws—the EAC's security analysis becomes structurally incapable of detecting or correcting the most damaging risks.[72]

- CISA's EI data show pervasive phishing weaknesses (73% of assessed EI entities), long patching delays (median >90 days for critical/high vulnerabilities), and extensive use of unsupported software, exactly the conditions in which sophisticated foreign adversaries and criminal groups excel at gaining and maintaining covert access.
- Because the same small circle designs, configures, certifies, and later investigates these systems, any successful intrusion that leverages supply-chain tampering, out-of-band management, weak configurations, or deleted logs can be misattributed to "operator error" or simply declared unprovable, preserving vendor reputations and EAC narratives at the expense of verifiable election integrity.

This closed, conflicted circle of trust is itself a demonstrated security risk, and any credible reform of EAC security analysis must begin by replacing it with truly independent, adversarial, and supply-chain-aware scrutiny.

[70] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf
[71] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[72] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf

5.6 Lack of Transparency

Opaque contracts, FOIA obstruction, and categorical denial of access to election systems under EAC jurisdiction convert technical weaknesses into uncheckable risks by preventing the public and independent experts from verifying whether states and vendors are actually complying with law, certification conditions, or basic security practice.[73]

5.6.1 Illusory contracts and vendor control

Contract provisions that treat core configuration data, logs, and system images as proprietary or off-limits to public inspection create an illusion of accountability while shielding noncompliant practices.[74]

- Mesa County's forensic reports show that Dominion's "trusted build," implemented jointly with the Colorado Secretary of State, deleted at least 695 log and event files—including IIS, SQL Server, Windows, and Defender logs—despite federal and state record-retention mandates and 2002 VSS requirements that audit trails be generated and preserved for at least 22 months.[75]
- Because vendor documentation and state rules defined "election records" narrowly as ballots and summary reports, but treated system logs and configuration as technical artifacts, the most security-relevant data could be destroyed or withheld while officials still claimed full legal compliance, leaving EAC oversight with contract-driven narratives rather than verifiable evidence.[76]

This contractual opacity allows vendors and state officials to shape what can be seen and thus what can be questioned, undermining any claim that certification and audits are grounded in complete system information.

5.6.2 FOIA obstruction and destruction of audit evidence

Obstruction of public-records access and the deliberate elimination of log data deprive both courts and citizens of the evidentiary foundation needed to evaluate security claims.[77]

- The post-election "trusted build" process in Mesa County, CO deleted 28,989 files from the EMS server, including 505 of 807 .log files and numerous .evtx event logs

[73] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[74] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf
[75] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[76] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf
[77] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf

that the VSS explicitly treats as election records essential to reconstruct system behavior and verify tabulation integrity.[78]

- Because these logs were erased and overwritten, no later FOIA request or litigation discovery can recover the full record of connectivity, user actions, or configuration changes, effectively guaranteeing that external reviewers cannot prove or disprove intrusion, misconfiguration, or manipulation—even when they are allowed to examine the system.[79]

When records necessary for independent verification are destroyed or withheld, FOIA formally exists but cannot deliver substantive transparency, and EAC security analysis that relies on state assurances inherits the same blind spots.

5.6.3 Denial of access to machines and technical data

Blanket denials of access to machines, images, and security-relevant documentation prevent the independent penetration testing and forensic work that could reveal systemic noncompliance missed by VSTLs and state reviews.[80]

- In many jurisdictions, election officials "have denied qualified third-party investigators the access to election system equipment including logs, network and security equipment configurations, and network diagrams" needed to detect unauthorized access or misoperation, even though simple tests using standard tools exposed the ability to flip results from non-Dominion computers and cell phones.[81]
- CISA's subsector risk summary shows that, across the EI subsector, 48% of entities had at least one internet-accessible host with a critical or high-severity vulnerability, 39% ran risky services such as FTP, RDP, or SQL on public-facing systems, and 34% ran unsupported operating systems—conditions that require aggressive, independent technical scrutiny but are typically masked behind generic statements that "systems are secure and air-gapped."[82]

[78] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf
[79] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[80] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf
[81] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-county-forensic-report-no-2.pdf
[82] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf

If independent experts cannot examine hardware, images, and full configurations, the EAC's reliance on lab reports and self-attestation becomes an exercise in trusting unverified claims from the same parties who configured and operated insecure systems.

5.6.4 How opacity magnifies security risk under EAC watch

Together, illusory contracts, FOIA obstruction, and denials of access create a structural environment in which grave technical weaknesses can persist indefinitely without detection or remediation.[83]

- Mesa County's case demonstrates that unauthorized software (SSMS), global SQL exposure, disabled logging, and mass deletion of audit trails can coexist with EAC/VSTL "certification" and state assurances precisely because the public and independent experts are blocked from seeing the full system state and history.[84]
- CISA's data confirm that unpatched, exposed, and poorly configured systems are common across the subsector, meaning that Mesa County is almost certainly not an outlier but one of the few instances where a clerk preserved images before a vendor-state process wiped logs and thus made the failures visible.[85]

In this environment, the EAC's security analysis is compromised not only by technical gaps but by an information regime designed to prevent effective external challenge, converting what should be verifiable critical-infrastructure security into an untestable set of assurances.

6 EAC Assurance Assessment

Publicly available evidence shows that the EAC Chair's assertions present an idealized account of EAC control and assurance that is not borne out by the actual behavior, configuration, and provenance of deployed systems, especially Dominion D-Suite, nor by the broader cyber-risk posture of U.S. election infrastructure.

[83] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf
[84] https://tinapeters.us/wp-content/uploads/2023/08/Mesa-EMS-Server-Image-Forensic-Report-No-1-09-15-21.pdf
[85] https://electioncrimebureau.com/wp-content/uploads/2024/09/CONFIDENTIAL-TLP-AMBER_EI-Subsector-Cyber-Risk-Summary-1.pdf

Table 3 EAC Assurance Assessment Summary

EAC CHAIR ASSERTION	REASONS FOR CONCERN
EAC OVERSIGHT OF SOURCE CODE	Code review and escrow do not extend to how systems are actually configured and operated; forensic evidence (e.g., Mesa County) shows uncertified tools, open databases, and erased logs in EAC-aligned deployments, making code-centric assurances unverifiable and inadequate for critical-infrastructure risk.
MANUFACTURER SOFTWARE DIFFERENCES	While vendors' codebases differ, insider testimony and architectural diagrams show a common SAES-derived EMS/database pattern across Smartmatic, Sequoia, and Dominion/Liberty Vote, creating shared control points and de facto common-mode vulnerabilities that the EAC's "no single master key" rhetoric does not address.
INDEPENDENT SECURITY REVIEWS	"Independent" reviews (INL, VSTLs, CIS) operate within a closed vendor-centric circle of trust; major configuration, credential, and logging failures passed through this ecosystem without detection, and the absence of a reported "universal key" is used rhetorically rather than as evidence of comprehensive, adversarial testing.
CERTIFICATION AND TRUSTED BUILDS	Trusted builds have been deployed with unauthorized software, globally exposed SQL services, shared administrator accounts, and trusted-build procedures that delete critical logs, demonstrating that EAC certification does not ensure secure configuration, preservation of audit evidence, or ongoing integrity of fielded systems.
PENETRATION TESTING AND VULNERABILITY ASSESSMENTS	EAC pen-testing tied to VVSG campaigns is narrow, episodic, and device-centric; CISA data show persistent critical vulnerabilities, risky internet-exposed services, and slow remediation across election infrastructure, proving that EAC-aligned testing and vulnerability management do not control real-world attack surfaces.
SUPPLY CHAIN MONITORING	VVSG 2.0 only calls for high-level supply-chain "strategy" and does not require SBOM/HBOM, independent provenance checks, or NDAA-style exclusions; EAC-certified systems can include foreign-manufactured hardware with powerful out-of-band controls and depend on high-risk third-party platforms (e.g., SolarWinds-class tools) without meaningful federal oversight.

U.S. election systems have been formally designated as **critical** infrastructure, a label that suggests they should receive the same level of security rigor applied to other vital systems such as defense and national-security networks. However, publicly available assessments and oversight reports indicate that this standard of care has not, in practice, been consistently extended to election infrastructure, revealing substantial gaps between the designation and the actual protections in place.[86]

[86] https://www.youtube.com/watch?v=zxNj-eQoO-Y

6.1 EAC Oversight of Source Code

The EAC's claimed review and maintenance of all voting-system source code does not, in practice, provide critical-infrastructure-grade assurance over U.S. election systems.

6.1.1 Assertion and implied assurance

EAC Chair Donald Palmer asserts that the EAC "has reviewed the source code of every registered manufacturer and maintains the source code of every registered manufacturer and each system," implying centralized, comprehensive technical oversight of all certified voting systems. This framing suggests that escrowed source code and lab review meaningfully constrain real-world security risk and that any serious systemic exploit (such as a universal backdoor) would necessarily have been detected and prevented under this regime.

6.1.2 Narrow scope vs. ecosystem risk

EAC source-code oversight is tightly bounded to specific certified configurations tested in laboratory conditions and does not extend to the broader election ecosystem where systems actually operate. CISA's Election Infrastructure Cyber Risk Summary shows that election environments commonly feature internet-exposed services, critical and high-severity vulnerabilities, unsupported operating systems, and weak phishing defenses, all of which can be exploited to bypass or subvert certified software regardless of its nominal source-code pedigree. In practice, attackers need only compromise surrounding networks, domain controllers, or third-party tools (including SolarWinds-class platforms) to gain control over election databases and processes while the EAC's code-centric assurances remain formally intact.

6.1.3 Gaps between source code, builds, and deployment

The EAC's focus on reviewing and escrowing source code does not ensure that deployed binaries and configurations actually correspond to what was reviewed. Forensic analysis in Mesa County showed uncertified software (e.g., SQL Server Management Studio), globally open SQL ports, and wireless-reachable EMS databases, all in an EAC-aligned, state-certified deployment—conditions that enabled direct vote-record manipulation from non-election devices, including an iPhone client, without passing through the certified application layer. These findings demonstrate that configuration and operational drift can create powerful attack paths that are orthogonal to any static review of source code and that the EAC's processes neither detect nor systematically prevent such divergence.

6.1.4 Logging, auditability, and code-centric blind spots

Strong source-code oversight is only meaningful if paired with robust, preserved logging and configuration evidence that allows detection and reconstruction of misuse. Mesa County's trusted-build process deleted at least 695 log and event-log files—including IIS, SQL Server, Windows, and Defender logs—within the 22-month record-retention window, destroying the very telemetry needed to verify whether certified software behaved as intended or was subverted at runtime. By accepting trusted-build practices that erase critical logs, the EAC's code-centric assurance model becomes effectively unverifiable in the field; it is impossible to prove that the code behaved securely when the key forensic artifacts have been overwritten or removed under EAC-aligned procedures.

6.1.5 Structural limitations and conflicts of interest

The same small community of vendors, VSTLs, and aligned experts that designs and configures systems also supplies the documentation and test scopes that underpin EAC source-code review, creating a closed "circle of trust." Mesa County reporting shows that this circle allowed an illegally certified configuration with disabled auditability and globally open database access to pass through the EAC/VSTL pipeline without detection, indicating that the oversight structure is not reliably adversarial or independent. In this context, maintaining source code under EAC custody does not equate to rigorous, external challenge of vendor designs; it often formalizes vendor narratives rather than uncovering deep, systemic flaws.

6.1.6 Overall effectiveness assessment

As a result of these structural and operational gaps, EAC oversight of source code is not sufficient to mitigate the principal risks facing election systems designated as critical infrastructure. The regime is device- and code-centric, episodic, and heavily dependent on vendor-supplied artifacts, while the dominant threats documented by CISA and independent forensic work exploit network posture, configuration management, credential handling, logging practices, and supply-chain exposures that lie largely outside EAC's current source-code oversight model. Consequently, the EAC's assertion that it has reviewed and maintains all manufacturers' source code overstates the real security assurance provided and should not be treated, on its own, as evidence that U.S. election systems are robustly protected against sophisticated or systemic compromise.

6.2 Manufacturer Software Differences

The EAC's assertion that each manufacturer's software is different and that there is no "single master key" is technically accurate at the codebase level but misleading as a

security assurance, because core architectures, functions, and attack surfaces are shared across vendors and deployments in ways that can enable systemic compromise.

6.2.1 The assertion and its intent

EAC Chair Donald Palmer states that "the source code and software is NOT the same for every manufacturer and there is no one master key to all systems – this is just a fallacy." This is used to imply that diversity of vendor codebases inherently protects U.S. elections from coordinated software-based manipulation at scale and that claims of systemic machine-driven fraud must therefore be unfounded.

6.2.2 Shared architecture across vendors

Evidence presented in this report shows that Smartmatic's SAES platform incorporates at least 14 distinct software mechanisms that can alter or conceal election outcomes (e.g., weighted tallying, remote configuration, selective result transmission). These mechanisms were later reflected in Sequoia systems and then in Dominion systems (now marketed as Liberty Vote), illustrating that distinct vendor lines share a common architectural **pattern** rather than completely independent designs. Diagrammatic comparisons in the report highlight repeating elements—centralized EMS databases, configurable tallying logic, remote management channels, and result-reporting layers—that create similar control points across all three product families, despite differences in proprietary code.

6.2.3 Systemic risk despite code differences

From an attacker's perspective, the critical question is not whether every line of code is identical, but whether different systems expose similar functions and trust assumptions that can be abused in comparable ways. The enclosed analysis, drawing on insider testimony and forensic work, indicates that the same categories of manipulative capability (e.g., database-layer modification, configuration-based result shaping, selective log retention) exist across vendors, which means a single conceptual "attack key" can be adapted across multiple platforms even if there is no literal universal binary or password.

6.2.4 EAC oversight limits on cross-vendor patterns

The EAC's certification and lab processes are organized around vendor-specific submissions and do not systematically model cross-vendor failure modes or the propagation of a common architecture (such as the SAES pattern) through the commercial ecosystem. There is no evidence in the report that EAC/VVSG threat modeling explicitly addresses how similar EMS database designs, remote support practices, and election-configuration workflows across vendors could enable a repeatable class of exploit that scales beyond a single manufacturer. This vendor siloing allows the EAC to truthfully deny

existence of a "universal key" while failing to address the reality that a small set of shared design conventions can create nearly universal avenues of manipulation across systems.

6.2.5 Misalignment with critical-infrastructure expectations

In other critical-infrastructure sectors, regulators explicitly look for and mitigate "common-mode failures" where different products expose similar vulnerabilities due to shared design patterns, supply chains, or protocols. By focusing on manufacturer differences and using that diversity as a talking point against systemic risk, the EAC departs from this best practice and understates the significance of the common SAES-derived architecture and associated attack surfaces documented across Smartmatic, Sequoia, and Dominion/Liberty Vote systems.

6.2.6 Overall effectiveness assessment

As a result, the EAC's "Manufacturer Software Differences" assertion functions as a rhetorical rebuttal to the notion of a single universal key but does not demonstrate that EAC oversight effectively mitigates cross-vendor, architecture-level risks in election systems. The available evidence supports the conclusion that, while the codebases differ, the convergence on similar EMS/database-centric designs and control points creates de facto common vulnerabilities that the current EAC oversight framework has neither fully acknowledged nor robustly addressed.

6.3 Independent Security Reviews and the "No Universal Key" Assertion

The EAC's reliance on Idaho National Laboratory (INL) and other "independent security reviews" to support its "no universal key" claim provides, at best, limited assurance for critical-infrastructure-grade security and does not address the systemic architectural and configuration risks documented across U.S. election systems.

6.3.1 The EAC's independence and "no universal key" claim

EAC Chair Donald Palmer asserts that many newer systems "have also been independently reviewed by Idaho National Lab (INL)," that these experts "seek to exploit the systems, identify vulnerabilities and then offer mitigation strategies," and that "this 'universal key' or 'universal software' is not something that has ever been identified and reported by some of the best white hat hackers in the world or any of EAC/Lab experts or any three letter agency." This framing uses the absence of a reported single universal exploit from INL and other reviewers as affirmative proof that such systemic capabilities do not exist, and as evidence that EAC-aligned oversight is robust.

6.3.2 Limits of the "no universal key" argument

Evidence cited in this report documents that Smartmatic's SAES architecture, with at least 14 mechanisms capable of altering or concealing results, informed subsequent Sequoia and Dominion/Liberty Vote designs, creating a family of systems that share core architectural control points even if their exact binaries differ. In that context, the practical question is not whether a literal, single password or binary works on every device, but whether a common set of EMS/database structures, remote-management pathways, and configuration levers provide a repeatable pattern of manipulation across many deployments; the report shows that such SAES-style patterns exist and can be reused, which contradicts the spirit of the EAC's "no universal key" reassurance even if it remains technically correct in a narrow sense.

6.3.3 Questionable independence and scope of reviews

The same report highlights a tightly interlinked "circle of trust" in which vendors, vendor-aligned experts, Voting System Test Laboratories (VSTLs), CIS, and state officials operate within a small, homogeneous community that designs, configures, tests, certifies, and later "independently" evaluates the very systems at issue. Mesa County forensic reports show that an illegally certified Dominion configuration—with unauthorized tools (SSMS), globally open SQL access, shared administrative accounts, and mass deletion of logs—passed through the EAC/VSTL pipeline undetected, demonstrating that this ecosystem has repeatedly failed to catch gross security and auditability violations despite formal certifications and implied third-party review.

6.3.4 Gaps between lab-style testing and real-world risk

CISA's Election Infrastructure Cyber Risk Summary shows that, across assessed election entities, 48 percent had at least one internet-accessible host with a critical or high-severity vulnerability, 39 percent exposed risky services such as FTP, RDP, SMB, or SQL to the internet, and 34 percent ran unsupported operating systems, conditions that enable credential theft and lateral movement into EMS environments. These ecosystem-level weaknesses—including SolarWinds-class supply-chain risks and widespread weak/generic credential practices—are largely outside the narrow, device-centric scope of VVSG testing and any INL penetration testing that focuses on isolated voting systems, meaning that even rigorous lab exploitation exercises can miss the system-of-systems attack paths that matter most for real elections.

6.3.5 Absence of a structured, cross-vendor threat model

The enclosed analysis shows that advanced methods such as Software FMEA and attack-tree modeling identify hundreds of concrete, multi-step attack scenarios against precinct scanners and EMS environments, many of which depend on configuration, credential, and process weaknesses rather than on a single universal software artifact. The EAC's public posture—including reliance on INL's failure to report a universal key—does not reflect this more mature, failure-centric view of risk and does not demonstrate that cross-vendor architectural patterns, such as SAES-derived EMS/database structures, have been systematically analyzed and mitigated across the ecosystem.

6.3.6 Overall effectiveness assessment

Taken together, the record supports the conclusion that EAC-cited "independent security reviews" and the associated "no universal key" assurance are insufficient as evidence of effective oversight of election systems. These assertions rest on narrow, lab-bounded testing, a self-referential circle of trusted actors, and a literal reading of "universal key," while documented evidence shows shared architectures, configuration and credential failures, deleted logs, and unremediated ecosystem-level vulnerabilities that can enable scalable manipulation without any single master password or universal binary.

6.4 Certification and Trusted Builds

The EAC's "certification and trusted build" assurances are undermined by evidence that trusted builds have been deployed with insecure configurations, undocumented software, and even systematic destruction of audit logs, making them ineffective as a primary safeguard for critical-infrastructure election systems.

6.4.1 The EAC's trusted build assertion

EAC Chair Donald Palmer states that "the accredited labs and EAC have certified the trusted build of each of these systems and this trusted build is what the states and counties receive when they use an EAC certified system," implying that tested software versions are faithfully delivered and operated, and that this linkage is a core security control. In this narrative, certification plus trusted build functions as a guarantee that what runs in the field matches what was evaluated and that deviations would be detectable and corrected.

6.4.2 Trusted builds vs. real-world configurations

The evidence cited in this report shows that in Mesa County, Colorado, a Dominion Democracy Suite EMS server operated under an EAC-aligned, state-mandated trusted

build while running uncertified tools such as Microsoft SQL Server Management Studio (SSMS), with SQL configured on default port 1433 and firewall rules allowing inbound connections from any IP address worldwide. Forensic testing demonstrated that non-Dominion workstations and even an iPhone SQL client could directly modify election databases without passing through the certified application, proving that a formally "trusted" build can coexist with deployment-time configurations that enable unlogged, out-of-band manipulation of votes.

6.4.3 Destruction of logs under "trusted build" procedures

Mesa County forensic reports further document that a Colorado Secretary of State–approved trusted build process deleted 28,989 files from the EMS server, including at least 695 log and event-log files (Windows, IIS, SQL Server, Defender) that federal VSS treat as essential election records for reconstructing system behavior over the 22-month retention period. By endorsing upgrade procedures that overwrite or erase core logs, the EAC's trusted build regime eliminates the very telemetry needed to verify that certified software and configurations have not been subverted, paralleling one of the central lessons of the SolarWinds compromise: without durable, tamper-resistant logs, post-hoc assurance collapses.

6.4.4 Gaps in lifecycle and configuration control

The report explains that VVSG 2.0 and the EAC lifecycle policy allow continued use of older, weaker systems and permit patches and configuration changes without full recertification, with no hard deadlines for retiring legacy equipment that cannot meet modern controls. Combined with CISA data showing widespread unpatched vulnerabilities, risky internet-exposed services, and unsupported operating systems in election infrastructure, this means that a certified trusted build is often dropped into an environment whose surrounding network, credential practices, and third-party platforms (including SolarWinds-class tools) remain insecure and ungoverned by EAC oversight.

6.4.5 Misalignment with critical-infrastructure best practice

In other critical sectors, trusted builds are embedded in a broader configuration-management regime that enforces secure baselines, tracks all deviations, and preserves complete logs to support forensic reconstruction and continuous monitoring. The enclosed analysis shows that EAC certification does not require CIS-level secure baselines for OS and database configurations, does not mandate vulnerability scanning and remediation SLAs, and does not integrate third-party platform risks or

supply-chain scrutiny into its trusted-build concept, leaving major attack surfaces unaddressed.

6.4.6 Overall effectiveness assessment

On the record presented, EAC assertions about certification and trusted builds overstate the real assurance delivered to states and counties. Trusted builds, as currently implemented and overseen, have been associated with erased logs, permissive network exposure, generic and plaintext credentials, and unauthorized tools on core EMS servers, demonstrating that the EAC's build-centric certification model fails to control or even reliably observe the operational conditions that determine whether election systems remain trustworthy in practice.

6.5 Penetration Testing and Vulnerability Assessments

The EAC's claim that its penetration testing and vulnerability management around VVSG campaigns are sufficient to secure election systems is not supported by the risk posture documented in this report; testing is narrow, episodic, and device-centric, while systemic vulnerabilities in real deployments remain widespread and unremediated.

6.5.1 The EAC's penetration-testing assertion

EAC Chair Donald Palmer asserts that "the EAC also conducts penetration testing prior to a VVSG campaign to ensure known vulnerabilities have been remedied and seek to identify any new vulnerabilities," presenting this as a key control compensating for other risks. Framed this way, periodic pen-testing around standards updates is meant to reassure stakeholders that certified systems are not only designed securely but are also actively challenged and improved over time.

6.5.2 Device-focused tests vs. ecosystem-scale risk

The enclosed analysis explains that EAC penetration testing and certification focus on voting systems as discrete products—specific devices and software builds—rather than on the full election ecosystem that includes EMS networks, domain controllers, remote-access tools, cloud services, and vendor-support environments. By contrast, CISA's Election Infrastructure Cyber Risk Summary finds that, across election entities, 48 percent had at least one internet-accessible host with a critical or high-severity vulnerability, 39 percent exposed risky services such as FTP, RDP, SMB, and SQL to the internet, and 34 percent ran unsupported operating systems on public-facing systems, revealing a pervasive attack surface that EAC's product-centric testing does not systematically address.

6.5.3 Persistent vulnerabilities despite supposed remediation

If EAC-aligned penetration testing and vulnerability management were effectively ensuring that "known vulnerabilities have been remedied," the sector-wide metrics documented by CISA would be expected to improve toward federal expectations. Instead, CISA reports median remediation times of roughly 90–104 days for critical and high vulnerabilities—three to six times its own 15–30 day expectations—and continued exposure of obsolete platforms and dangerous services, indicating that vulnerabilities in the actual operating environment are neither promptly nor consistently remediated despite EAC assurances.

6.5.4 Configuration and credential failures outside test scope

The report's detailed Mesa County forensic work shows an EAC-aligned, state-certified Dominion EMS deployment running with Microsoft SQL Server listening on the default port 1433, enabled protocols including TCP/IP and Named Pipes, a firewall rule allowing inbound SQL connections from any IP address worldwide, generic and shared administrative accounts, and plaintext storage of passwords and decryption keys. Penetration-style experiments demonstrated that a non-Dominion workstation and even an iPhone SQL client could connect directly to election databases and modify vote records without going through certified application controls—conditions that basic security testing should have flagged immediately, yet were present in a system that had passed through the EAC/VVSG pipeline.

6.5.5 Lack of continuous, independent assessment

The report demonstrates that EAC penetration testing is episodic—tied to VVSG campaigns—rather than continuous, and that there is no EAC mechanism comparable to CISA's ongoing vulnerability scanning, risk and vulnerability assessments (RVAs), or red-team engagements across election-office IT. At the same time, "independent" assessments are largely performed within a closed circle of vendors, VSTLs, and aligned experts, and public or genuinely adversarial testing is often blocked by vendor contracts, FOIA obstruction, and denials of access to machines and logs, leaving major vulnerabilities undiscovered until whistleblowers or court-ordered forensics expose them.

6.5.6 Overall effectiveness assessment

Taken together, the record indicates that EAC assertions about penetration testing and vulnerability management significantly overstate the actual level of security assurance provided to U.S. election infrastructure. Testing is constrained to lab scenarios and reference configurations, does not govern or continuously measure real-world network, credential, and configuration hygiene, and has demonstrably failed to prevent or detect

conditions—such as globally exposed databases, insecure third-party platforms, and erased logs—that are fundamentally incompatible with critical-infrastructure-grade protection of election systems.

6.6 Supply Chain Security

The report shows that EAC efforts to ensure supply chain security for election systems are narrow, largely declarative, and significantly out of step with the level of provenance and adversary-focused scrutiny now expected for other federally designated critical infrastructures.

6.6.1 Limited supply-chain scope in VVSG and certification

VVSG 2.0 mentions supply-chain risk management but only at a high level, emphasizing that vendors should have a "strategy" rather than imposing concrete, verifiable controls on firmware provenance, manufacturing geography, component whitelisting, or SBOM-based vulnerability management. EAC certification and lab test scopes stop at the vendor's system boundary; they do not map or vet underlying chips, boards, embedded controllers, radios, or other subcomponents against foreign-adversary risk, even though those subcomponents are integral to critical election functionality.

6.6.2 Misalignment with federal adversary-based procurement policy

Congress has already recognized the national-security implications of foreign-sourced ICT by prohibiting federal agencies and grant recipients from using certain Chinese telecom and surveillance technologies under Section 889 of the FY2019 NDAA and by extending similar logic to other critical technologies in later NDAAs. This report notes that EAC processes do not require hardware or software bills of materials (HBOM/SBOM), do not screen components or vendor networks for Section 889–style covered equipment, and do not align certification decisions with these federal restrictions, allowing EAC-certified systems to embed components that would be barred from other federal critical systems.

6.6.3 Foreign manufacturing and out-of-band control surfaces

Mesa County forensic work illustrates that EMS servers used in EAC-aligned environments are built on hardware manufactured and assembled in foreign jurisdictions that U.S. intelligence has explicitly flagged as high-risk for supply-chain compromise. The report explains that such platforms commonly include powerful out-of-band management engines (e.g., Intel ME, Dell iDRAC) that enable remote, OS-invisible control, yet EAC certification does not require disabling or hardening these channels, conducting hardware

tear-downs, or independently validating provenance—controls that would be routine for defense or intelligence systems with comparable criticality.

6.6.4 Third-party platforms and SolarWinds-class risks

The enclosed analysis details how election jurisdictions and vendors rely on third-party management and monitoring platforms such as SolarWinds Orion, whose compromised update pipeline enabled nation-scale intrusions into federal and critical-infrastructure networks, including those involved in election support. Despite this, EAC documentation and certification do not substantively address how third-party platforms in development, test, and production pipelines are secured, monitored, or constrained, leaving a major supply-chain attack vector outside formal oversight even as systems are labeled "certified" and "trusted."

6.6.5 Governance, revolving doors, and vendor-centric assurance

The report's "circle of trust" section highlights that vendors, former vendor staff now in regulatory roles, VSTLs, and organizations like CIS operate within a tight, self-referential ecosystem that designs, configures, certifies, and later "independently" reviews election technology. Mesa County's illegally certified Dominion configuration—with Chinese-manufactured hardware, unauthorized software, global SQL exposure, and mass deletion of logs—passed through this ecosystem without detection, indicating that the same actors who control supply-chain choices also control the assurance narrative, with little adversarial challenge.

6.6.6 Overall effectiveness assessment

On the evidence presented, EAC supply-chain security efforts amount to general language about "strategies" and vendor attestations, not a robust, adversary-aware regime suitable for systems designated as critical infrastructure. The absence of mandatory SBOM/HBOM disclosure, lack of alignment with NDAA-style foreign-adversary restrictions, tolerance of foreign-manufactured platforms with powerful out-of-band controls, and unaddressed dependence on high-risk third-party tools collectively show that EAC oversight does not meaningfully mitigate the supply-chain attack surfaces that modern national-security policy treats as intolerable in other critical sectors.

7 Recommendation

The EAC's mission should be re-focused to protect the integrity of our elections rather than to subsidize the deployment of electronic voting systems burdened by significant security

risks. In support of this mission, the EAC should be tasked with the development of robust pre-election and post-election audit standards. This mission could be further extended to train and deploy audit teams dedicated to conducting audits of elections in accordance with these standards nationwide.

8 Conclusion

Overall, the factual record available from public sources contradicts the core reassuring implications of the EAC Chair's assertions. Certified systems have contained unlisted tools and insecure configurations; trusted builds have destroyed required audit records; documented database manipulations and logging practices have rendered key contests non-verifiable; systemic cyber weaknesses persist across the election infrastructure subsector; and federal authorities have been slow to act on urgent, expert warnings. The Chair's statements do not grapple with these realities and therefore cannot be treated as an adequate or complete description of the true security posture and governance of U.S. voting systems.

In this light, we are compelled to ask the following fundamental question:

"Do the perceived benefits of electronic voting systems outweigh the risks?"

Based upon even the small sample of evidence cited in this report, the answer should be a resounding "No". The integrity of election results is not negotiable, yet all too many people have prioritized the perceived convenience of machines over integrity. Integrity is not simply one of many factors to consider when it comes to the conduct of our elections. It is THE factor.

Americans are called on to provide an inordinate amount of trust into individuals and organizations which have on many occasions been shown to have abused that trust. Hand counts of paper ballots do not require this level of trust. Everything about the hand count process is transparent and subject to public inspection. There is no proprietary source code. There are no sensitive security configuration settings. There are no usernames and passwords to manage. The entire hand count process can be livestreamed around the world for all to see without risk of a team of lawyers seeking an injunction upon the disclosure of the vote. Transparency is the key to the restoration of confidence in the results of our elections. The elimination of electronic voting systems is the key to achieving this transparency.

9 About the Author

Patrick J. Colbeck is an aerospace engineer, author, certified Microsoft Small Business Specialist, and former Michigan state senator with extensive experience at the intersection of technology, public policy, and election administration. He began his career as a Senior Design Engineer at Boeing, where he worked on components of the Environmental Control and Life Support System and the Quest Airlock module for the International Space Station, and later provided systems engineering support on advanced simulation systems for the U.S. Department of Defense. After his aerospace work, he founded and led technology and consulting firms focused on information technology solutions across diverse industries, and authored *Information Technology Roadmap for Professional Service Firms* on strategic IT deployment.

Colbeck was elected in 2010 to represent Michigan's 7th Senate District and served two terms from 2011 to 2019, becoming the first state senator in three decades to be elected directly to the Senate without prior public office. Following his legislative service, Colbeck ran for the Republican nomination for governor of Michigan in 2018 and has remained active in public policy debates, particularly on election administration and security. Drawing on his combined engineering and legislative background, he has written and spoken extensively on election systems, information technology, and government accountability, including books such as *Wrestling Gators: An Outsider's Guide to Draining the Swamp* and *The 2020 Coup: What happened? What we can do?* that chronicle his policy work and concerns about election integrity.

He now serves as the Chief Operating Officer for Lindell Management. In this capacity he has continued to be a vocal advocate for election integrity.