2026

EXECUTIVE SUMMARY 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

1 Introduction: A Fundamental Disconnect in Election Security

This document is intended as an Executive Summary of a much more detailed analysis on the subject of the security of electronic voting systems in the United States. United States election systems are designated as "Critical Infrastructure," a status that mandates the highest levels of security rigor and public trust. This summary outlines a profound disconnect between the public security assurances made by the Election Assistance Commission (EAC) and the documented, systemic failures that leave these vital systems vulnerable to compromise. The core thesis of this analysis is that the EAC's oversight framework is fundamentally insufficient. It fails to address critical risks across standards development, operational security, supply chain integrity, and governance, thereby failing its mission to secure a vital component of U.S. democracy. This summary seeks to summarize these deep-seated security deficiencies, deconstruct the EAC's public claims, and present a conclusion based on the overwhelming weight of evidence.

2 Analysis of Systemic Security Deficiencies

A comprehensive review of publicly available evidence, including federal risk assessments and detailed forensic reports, reveals not isolated incidents but a pattern of pervasive security gaps across the entire election system lifecycle. This section synthesizes these failures into four critical domains: inadequate standards, operational failures, a compromised supply chain, and institutional opacity.

2.1 Inadequate Standards and Superficial Analysis

A significant gap exists between the EAC's Voluntary Voting System Guidelines (VVSG 2.0) and the security standards required for other critical infrastructure sectors. The VVSG 2.0 framework focuses narrowly on individual devices, largely ignoring the broader enterprise ecosystem of networks and vendor environments. Crucially, the guidelines fail to mandate specific, verifiable controls expected in any high-risk federal environment, including the lack of requirements for full Role-Based Access Control (RBAC), secure baselines such as CIS-level benchmarks, mandatory vulnerability patch-timeliness SLAs, minimum log retention durations technically aligned with federal law (52 U.S.C. 20701), and verifiable controls for firmware provenance and manufacturing geography.

This is compounded by the EAC's lack of a structured, failure-centric risk analysis model. Its conformance-based certification model, which validates a system against a checklist, stands in stark contrast to the ecosystem-level risk assessments conducted by the Cybersecurity and Infrastructure Security Agency (CISA), which identify pervasive weaknesses like unpatched systems and exposed network services. The absence of mature engineering methods like Failure Modes and Effects Analysis (FMEA) indicates a compliance-based posture that fails to account for operational and ecosystem-level risk.

2.2 Pervasive Operational and Configuration Failures

Forensic analysis of deployed systems provides concrete proof of profound operational failures in environments nominally aligned with EAC standards. The forensic reports from Mesa County, Colorado, on a Dominion Election Management System (EMS) server serve as a stark case study of these deficiencies:

- **Uncertified Administrative Tools Granting Direct Database Access:** The core EMS server was found to have uncertified, powerful database management tools installed, specifically Microsoft SQL Server Management Studio (SSMS). This provided a direct, unauthorized back-end pathway to election databases, completely bypassing the certified Dominion application software.
- **Firewall Misconfiguration Exposing Election Database to Global Internet:** The same EMS server was protected by a firewall rule explicitly configured to permit inbound database connections from **"any IP address worldwide."** This configuration effectively nullified the server's perimeter defenses, treating the entire internet as a trusted network for direct database access.
- **Pervasive Mismanagement of Passwords, Keys, and Privileged Accounts:** Forensic analysis documented a cascade of poor credentialing practices, including the use of generic administrative accounts, the storage of passwords and decryption keys in plaintext within system files, and the public, internet-based exposure of sensitive BIOS passwords for voting system hardware.

2.3 A Compromised Supply Chain and Conflicted Governance

The EAC has failed to enforce rigorous supply chain security controls commensurate with federal policy for critical infrastructure. While the VVSG requires vendors to have a high-level "strategy," it fails to implement specific prohibitions against using components from foreign adversaries—a standard codified in the National Defense Authorization Act (NDAA) for other critical systems. The Mesa County EMS server, for instance, was assembled using a motherboard manufactured in China. This introduces unmitigated risks from powerful,

out-of-band management engines (e.g., Intel ME, Dell iDRAC) that enable remote, OS-invisible control and represent a critical threat vector for a national security system.

This critical technical failure is enabled by a profound governance failure: a structural conflict of interest within the election technology ecosystem. An insular "circle of trust" exists between equipment vendors, former vendor employees holding positions within the EAC, and accredited Voting System Test Laboratories (VSTLs). This self-regulating model undermines any claim of independent oversight. A truly independent body would not tolerate Chinese-manufactured motherboards in critical election infrastructure without the rigorous, adversarial verification that is currently absent. Instead, this structure fosters a vendor-centric assurance narrative that prioritizes compliance over true security verification.

2.4 Institutional Opacity and the Deliberate Destruction of Evidence

A systemic lack of transparency magnifies all other technical and governance risks. Vendor contracts that shield systems from public inspection, the obstruction of Freedom of Information Act (FOIA) requests, and the denial of system access for independent review prevent any meaningful verification of security claims. This opacity creates an environment where severe vulnerabilities can persist without scrutiny or accountability.

The "trusted build" process in Mesa County serves as a definitive example of how this opacity becomes destructive. Under a state-mandated procedure, the re-installation of certified software resulted in the mass deletion of 28,989 files, including at least 695 legally required audit logs from the Windows operating system, web servers, and database servers. This deliberate destruction of forensic evidence makes it impossible to confirm or deny whether the system was compromised, rendering EAC claims of system auditability meaningless in practice. This systematic destruction of forensic evidence provides the critical context for evaluating the EAC's public security assurances, which rely on a presumption of auditability that these very procedures render impossible.

3 Deconstruction of EAC Public Assurances

This section directly contrasts the specific security claims made by the EAC Chairman with the contradictory evidence detailed in forensic reports and federal assessments. This point-by-point refutation demonstrates that the EAC's public narrative is fundamentally misaligned with the factual security posture of U.S. voting systems.

- **EAC Claim: "EAC Oversight of Source Code" ensures security.**

Reality: Source code review is insufficient and provides a false sense of security. Forensic evidence shows that deployed systems have been found operating with uncertified software, insecure network configurations, and globally exposed database ports. These operational vulnerabilities completely bypass the security logic of the certified application code. Furthermore, this claim is unverifiable in practice, as essential system logs required to confirm that the code behaved as intended have been systematically destroyed as part of official "trusted build" procedures.

- **EAC Claim: "Manufacturer Software Differences" prevent systemic risk.**

Reality: This assertion is misleading. While line-by-line code may differ, architectural diagrams and insider testimony document a shared architectural pattern (known as SAES) across major vendors, including **Smartmatic, Sequoia, and Dominion**. This shared design lineage creates common-mode vulnerabilities and analogous control points centered on the Election Management System database. Consequently, a single conceptual attack pattern can be effective across different vendor systems, creating the very systemic risk the EAC claims does not exist.

- **EAC Claim: "Certification and Trusted Builds" guarantee integrity.**

Reality: This claim is directly contradicted by forensic evidence. The "trusted build" deployed in Mesa County, Colorado, contained unauthorized software and critical security flaws, such as a firewall rule allowing worldwide database access. More alarmingly, the "trusted build" process itself was the mechanism used to systematically destroy thousands of essential forensic logs. This destruction of evidence makes it impossible for any independent party to verify the integrity of the system, rendering the "trusted build" an instrument of opacity rather than assurance.

- **EAC Claim: "Penetration Testing" addresses known vulnerabilities.**

Reality: The EAC's penetration testing is episodic and narrowly focused on individual devices in a lab setting. It fails to address the persistent, ecosystem-wide vulnerabilities documented by CISA, such as unpatched internet-facing systems, exposed risky services, and poor credential management across election offices. The documented real-world deployment failures—including exposed databases and plaintext passwords—are definitive proof that this testing model is not effective at securing the operational environments where elections actually take place. These documented, real-world failures prove the EAC's testing model is insufficient, leading to the inescapable conclusion that the system as a whole is unfit for its purpose.

4 Conclusion: A System Unfit for Critical Infrastructure

The evidence presented in publicly available forensic reports and federal assessments leads to an unambiguous conclusion: the EAC's oversight regime fails to meet the security standards required for critical national infrastructure. The documented failures in standards, operational security, supply chain management, and governance are not minor flaws but systemic deficiencies that expose the foundation of U.S. elections to unacceptable risk. The perceived benefits of convenience offered by current electronic voting systems do not outweigh their documented vulnerabilities. The integrity of election results under this paradigm is not negotiable but is demonstrably compromised.

Therefore, a fundamental paradigm shift is required. The nation must move away from the current opaque, high-risk electronic systems and toward a transparent model centered on hand-counted paper ballots, which allows for full public verification. The mission of the EAC should be refocused away from certifying insecure technology and toward developing robust audit standards for a transparent, verifiable, and trustworthy election process.

Please see the detailed report on the Security of Electronic Voting Systems in the U.S. for additional information in support of these assertions.