The Case Against Electronic Voting Systems

An Unnecessary National Security Risk

August 2026

V1.0

LINDELL OFFENSE FUND
LindellPlan.com

Made possible by funding from the Lindell Offense Fund

“A rigorous systems critique, not a fraud claim: electronic voting turns elections into black boxes that cannot prove their own correctness—and that is itself the national security failure.”

Grok AI

"A system where audit logs self-attest, patches are legally penalized, and the public tally has no federal standard is an enterprise built to be believed, not verified."

Gemini AI

Table of Contents

1 Executive Summary

The concerns documented in this memorandum are not a list of unrelated defects. They form a single escalating structure. Each area of concern makes the next one easier to execute and harder to detect, and the last one — the absence of any evidence capable of settling the question — is what makes the first four unfalsifiable. They are presented in that order, from the collection of information to the impossibility of proof.

Each area is also, on the record assembled here, a **national security** matter and not merely an administrative one. Election infrastructure carries a federal critical-infrastructure designation. The systems described below aggregate the personal data of the entire American electorate, expose it through programmatic interfaces governed by no federal standard, have been placed in the hands of foreign-linked contractors and offshore development operations, and cannot produce the forensic record that any other critical-infrastructure sector would be required to produce after an incident. An adversary — foreign or domestic — does not need to defeat these systems. It needs only to use them as designed.

1.1 Area A — An intelligence platform feeding sensitive election data to parties positioned to act on it

The registration, pollbook, ballot-production and tabulation systems are joined into one data enterprise, and the information that enterprise holds is exactly the information required to plan a manipulation: who is registered, who has voted, who has not, in which precinct, on which machine, with how much time remaining.

- **Every voting system certified for use in Michigan was required to interface with the statewide Qualified Voter File.** Dominion's Michigan contract answers "Y" to requirement 1.2.B.11 — "Contractor shall demonstrate how data can flow from the State Qualified Voter File (QVF) into EMS" — and confirms that "Democracy Suite EMS is capable of importing election definition data from the QVF using the Election Data Translator module" and that "Michigan ENR codes are imported from the QVF file during the election definition phase" (Michigan contract 071B7700117, Exhibit 2 to Schedule A, Attachment 1.1; supplied as Exhibit 13). The registration database, the tabulation software, and the election-night reporting system are, by state requirement, one chain.
- **CISA has confirmed nine distinct vulnerabilities** in the Dominion ImageCast X, including the ability to install malicious code that spreads via removable media, to forge technician authentication

and obtain root access, to extract county-wide cryptographic secrets from poll-worker cards, and to **"print an arbitrary number of ballots without authorization"** (CISA ICSA-22-154-01).

- **CISA's own internal assessment of the 2020 election year** found 34% of assessed election entities running unsupported operating systems on internet-accessible hosts, 48% carrying a critical or high-severity vulnerability on an internet-accessible host, and a median remediation time for critical vulnerabilities **with publicly known exploits of 108 days** — longer than most election cycles (CISA, *Election Infrastructure Subsector Cyber Risk Summary*, March 2021, marked TLP:AMBER; Exhibit 9).
- **A federal standards body published the file-level manifest of a certified voting system**, including its cryptographic class names, with SHA-1, MD5 and CRC32 hashes, on a public object store (NIST; Exhibit 2).
- **Third-party programmatic read access to registration data was documented and then quietly removed.** Earlier published versions of Rock the Vote's registration API documented `GET /api/v3/registrations.json`, returning registrant name, address, party, race, telephone and email (V3 source, commit e4fa5583b1). The V4 release notes list those read endpoints under **"Removed"** (current API docs). No security rationale for the removal was published, and **nothing in the record establishes that the underlying capability was disabled rather than merely undocumented.**
- **The vendor whose technology lineage runs through the current fleet is under federal criminal indictment.** A superseding indictment returned October 16, 2025 in the Southern District of Florida charges **SGO Corporation Limited, "commonly known as 'Smartmatic,'"** together with its co-founder and Chief Operating Officer, with FCPA conspiracy and international money laundering, alleging a slush fund created "by **over-invoicing the cost per voting machine supplied for the 2016 Philippine elections**" and at least $1 million in bribes to the chairman of that country's election commission (DOJ; superseding indictment).

The national security consequence. A single compromise of this enterprise yields the electorate's personal data, the operational state of the count in real time, and the ability to influence what ballots exist. No other critical-infrastructure sector concentrates that much sensitive information behind that little federal standard.

1.2 Area B — A ballot ordering system capable of supplying the gap between the actual count and a desired count

Once the intelligence in Area A is available, the second capability required is the ability to produce ballots on demand — enough to close a known gap, in the correct styles, for the correct precincts.

- **The vendor markets exactly this capability.** Dominion's Mobile Ballot Printing material carries the slogan **"BALLOTS WHEN & WHERE YOU WANT THEM!"** and its own architecture diagram shows the **Voter Registration System as a direct input** to the ballot-printing module, with output to a vote center, a precinct, **and a central office** (Exhibit 1).
- **CISA has confirmed that the authorization check on that capability can be defeated.** CVE-2022-1747: the voter session activation mechanism "is susceptible to forgery. An attacker could leverage this vulnerability to **print an arbitrary number of ballots without authorization**" (CISA).
- **Ballot-on-demand printing is outside EAC certification scope entirely.** No federal body certifies the equipment that manufactures the ballots.
- **The data set required to compute the gap was requested in writing at an American central count facility in 2020.** An outside private party at Green Bay's central count instructed staff to "**pull the numbers on the absentee ballots returned and outstanding per ward**" so that he could "determine which wards were on which voting machines" (Exhibit 5). Returned plus outstanding per ward, mapped to machines, is the complete input set for the question *how many more ballots, of which style, at which machine*.
- **At the same facility the same party arranged a hidden, password-free wireless network** designated for "**the sensitive machines that need to be connected to the internet**" (Exhibit 3), and, per the same record, controlled which ballots were counted.
- **Michigan's own 2024 absentee records cannot be reconciled, and the state never showed its arithmetic.** The statewide daily-ballots-cast records captured by citizen observers contain **208,075 rows covering 82,647 unique voter identifiers — an excess of exactly 125,428 records**, the figure that entered public circulation. The Department attributed this to a formatting defect and asserted that "each of these voters only had one vote recorded for this election," while a records request produced a version of the file showing no duplicates. **The state has never published the query, the script, or the reconciliation that would demonstrate how the figure arose**, and the two productions — the citizen capture and the records-request response — do not agree, with the state as the common source of both.

The national security consequence. A ballot supply that is a software output rather than a controlled physical inventory removes the one control that requires no trust in software: counting the paper before the election.

1.3 Area C — Direct manipulation of vote tallies at the county or tabulator level

- **Malicious code can be installed on a voting machine in under a minute, can modify "all records, logs, and counters" to be internally consistent, and can spread machine to machine** — demonstrated in working form on certified equipment by Princeton researchers (Princeton CITP).
- **Malicious code can propagate from a county's central election management system to every ballot-marking device in the jurisdiction** — CISA's CVE-2022-1743, independently confirming an academic finding.
- **The mechanism that would report the tampering grades itself.** CISA, CVE-2022-1740: the "on-screen application hash display feature, audit log export, and application export functionality rely on **self-attestation mechanisms**."
- **Manipulation would not need to be widespread to be decisive.** The 2020 presidential election was decided by 11,779 votes in Georgia, 10,457 in Arizona and 20,682 in Wisconsin. A single county in each state — Fulton, Maricopa, Milwaukee or Dane — is large enough to supply the entire margin. **The absence of evidence of nationwide exploitation is not responsive to a threat model that requires exploitation in five counties.**
- **Whether direct manipulation has occurred can be neither proven nor disproven from the available record, and this memorandum asserts neither.** The two most prominent competing claims — Halderman's laboratory demonstrations and Lenberg's "logical bumper" — are **theories**. Neither has been shown to have occurred in a live federal election, and both have documented, reasonable competing explanations. That symmetry is not a weakness in the argument; it is the argument.
- **The standard rebuttal — "just look at the ballots" — presumes a chain of custody that the record does not always show.** In *Bailey v. County of Antrim*, **four separate counts of the same election produced four different presidential vote totals**: 12,423, then 17,327, then 15,949, then 15,718. Judge Kevin Elsenheimer, dismissing the case, stated from the bench: "**Nor am I saying that the processing of election data here wasn't corrupted or corruptible. I don't have the facts to make that determination.**"

1.4 Area D — Interoperability and artificial intelligence

The systems in Areas A through C are joined by mandated data formats, and that interoperability is now the surface on which machine-speed tooling operates.

- The mandated chain runs **registration database → election management system → tabulator → election-night reporting**, in Michigan's case through a single state-specified file format, with results returned in the Michigan Standard Results File Format (Exhibit 13).
- **The layer at the end of that chain is subject to no federal standard of any kind.** The EAC states of election-night reporting software: "**There are no federal standards governing the design, security, and setup of this critical aspect of the electoral process**" (EAC).
- **The unofficial public feed and the official canvass are two outputs of the same certified machine.** Dominion's own *Results Tally & Reporting* guide lists among the EMS's functions "Publishing the unofficial Election Results for further processing or reporting (i.e. by news and media feeds)" (Colorado Secretary of State-hosted copy).
- **Interoperability converts a local compromise into a systemic one.** In *Curling v. Raffensperger* the court recorded expert opinion that the copying and distribution of Georgia's voting system software "materially increased the risk that a future Georgia election would be attacked **because all 159 Georgia counties used the same voting system**" (order of Nov. 10, 2023).
- **The certification regime guarantees the interfaces stay frozen.** Maricopa County stated on the record that "if the County were to implement a software or security update without it being tested and approved by the EAC, the County's tabulation equipment would lose its federal and state certification" (Maricopa County). Dominion's patch for the nine CISA vulnerabilities took from June 2022 to **March 16, 2023** to be certified, and Georgia announced it would not install it until after the 2024 presidential election.

The national security consequence. A uniform, standardized, unpatchable interface layer across thousands of jurisdictions is the ideal target for an adversary with automated tooling: one exploit, developed once, applies everywhere, and applies for years.

1.5 Area E — No evidence capable of allowing an independent party to confirm or refute the result

This is the finding on which the requested action rests, and it is the one that requires no allegation of wrongdoing by anyone.

- **The layer through which the public learns the result has no standard, no log requirement, and no audit requirement.** Direct analysis of the archived 2020 national results feed shows that on November 4, 2020, within a four-hour window, **50 of 51 presidential races had their cumulative vote totals discarded and reset to zero — 134,998,591 votes — with no public log**

and no published explanation. After excluding every reset, **416 further downward revisions** remain across 45 races, 330 of them after the feed reported counting essentially complete. In Pennsylvania, Georgia and Wisconsin the volume of unexplained downward revision **equals or exceeds the certified margin of victory** (analysis of Exhibit 11; method and limits in the appendix).

- **The paper record cannot settle the question where custody is not demonstrated.** Antrim County produced four different totals for the same election. Fulton County investigators reported **3,075 duplicate ballot images** and stated they "were unable to determine how many of the 3,075 duplicate images represented ballots that were included in the results used to certify the 2020 election."
- **The forensic record has been destroyed by the vendor at a state's direction.** A Mesa County forensic report records that "Dominion's installation of the Trusted Build update on the EMS in May of 2021, as ordered by the Colorado Secretary of State, destroyed all data on the EMS hard drive" — a machine subject to the 22-month federal retention requirement of 52 U.S.C. § 20701.
- **The audit mechanism asks the software to grade itself**, and the software's own vulnerability class permits it to lie (CVE-2022-1740).
- **Independent examination is not lawfully available.** Source code is proprietary, cast vote records are withheld or aggregated, and independent examination of equipment has drawn criminal referral.
- **Even the state's own remedy was mischaracterized.** In *Bailey*, the Secretary of State's counsel conceded at oral argument that the December 2020 Antrim hand recount **was not an audit under MCL 168.31a(2)** — while the Department's own press release had called it "a zero-limit risk-limiting audit" confirming the result "to absolute certainty."

1.6 The conclusion this supports.

It is not necessary to prove that any specific election was altered in order to justify the requested action, and this memorandum does not claim to have proven it. The finding is narrower, better supported, and sufficient: **the United States conducts its federal elections on systems that cannot be independently verified, cannot be promptly patched, cannot be lawfully examined, and cannot produce a record capable of settling a dispute about their own output.** A government that cannot demonstrate the integrity of its election infrastructure has a national security problem regardless of whether that infrastructure has been attacked.

1.7 The recommendation.

An Executive Order establishing **hand-marked, hand-counted paper ballots as the primary method of conducting federal elections**, with machine assistance permitted only where a jurisdiction demonstrates necessity and only under a mandatory manual audit of the human-readable record that governs in any conflict. The cost objection is addressed directly in the Remedy: the comparisons offered against hand counting omit the full cost of the machine regime — federal certification and oversight, recurring vendor fees, the pending multi-billion-dollar replacement cycle, and the cost of the integrity measures this memorandum shows to be missing — and they treat cost rather than verifiability as the governing priority. **Roughly four in five countries in the largest international survey do not use electronic voting at any level, and of the eleven that abandoned it, the leading stated reason was concern about the trust and security of the vote.**

2 Statement of Purpose

This memorandum is submitted to make the affirmative case for an Executive Order ending the use of electronic voting systems in federal elections and establishing hand-marked, hand-counted paper ballots as the primary method by which those elections are conducted.

Its purpose is narrow and deliberately so. It does not seek to relitigate any past election, and it does not assert that any past federal election was altered. It seeks to establish a single proposition, drawn almost entirely from the government's and the vendors' own records: **that the systems presently used to conduct federal elections are incapable of demonstrating the correctness of their own output to any independent party, and that this incapacity is a property of their design rather than an accident of their administration.**

Three consequences follow, and they are the reason this is a federal matter and a national security matter.

First, a system that cannot be verified cannot be defended. Where the audit log self-attests, where the counted portion of the ballot is unreadable by the voter, where the software may not lawfully be examined, and where the reporting layer keeps no immutable record of its own revisions, there is no forensic capability. An adversary who succeeded would leave no trace that anyone outside a county office could find; an adversary who failed would be indistinguishable from an adversary who succeeded. Every other designated critical-infrastructure sector is required to be able to answer the question "what happened." This one is not.

Second, the concentration of sensitive data is itself the exposure. The chain documented in Area A joins the personal records of the entire American electorate to the machinery that produces and counts ballots, through mandated interfaces, with third-party programmatic ingress, foreign-linked contractors, and offshore development in the supply chain. That is an intelligence target of the first order, and its governance is voluntary.

Third, the remedy is available now and does not depend on resolving any contested factual dispute. Hand-marked paper counted by humans in public, under observation, is the only architecture yet devised in which the correctness of an election does not depend on trusting either the vendors or the officials who administer it. It is already the mandated legal fallback in multiple states, precisely because electronic systems are known to fail. It is the ordinary practice of most of the world's democracies. The question before the President is not whether it is more convenient. It is whether the integrity of a federal election result should be a demonstrable fact or a trusted assertion.

The document proceeds by stating the evidentiary standard it applies, then the five escalating areas of concern, then the trade that produced them, then the remedy.

3 Standard of Proof

This memorandum applies a single evidentiary rule in both directions.

No assertion is credited because of who made it. A vendor's statement that its product is secure, a state official's statement that an anomaly was a "programming mistake," and a private analyst's statement that a system was manipulated are treated identically: as claims requiring documentary support. Where support exists, it is cited to the primary record. Where it does not, the matter is recorded as **unresolved** — not as settled in favor of the party with the larger institutional letterhead.

The burden of proof rests on those asserting that the systems are secure. This is not a rhetorical inversion. It is the ordinary allocation of burden in every other domain of federal safety regulation. A pharmaceutical manufacturer does not tell the FDA "no one has proven our drug unsafe"; it produces evidence of safety. An aircraft manufacturer does not tell the FAA "no crash has been attributed to this design"; it demonstrates airworthiness. The proponent of a system bearing a critical-infrastructure designation carries the burden of demonstrating that it performs as claimed.

That allocation matters more here than in most fields, because of an asymmetry documented throughout this memorandum: **the parties asked to prove malfeasance are the same parties denied access to the evidence that would prove or disprove it.** Source code is proprietary. Cast vote records are withheld or

released in aggregate. Election management server images are, in at least one documented case, destroyed by a vendor update performed at a state's direction. Independent examination of equipment has been met with criminal referral. A system cannot simultaneously withhold the evidence and demand that its critics produce it.

"No evidence of exploitation" is not evidence of no exploitation. CISA's own advisory on Dominion's ImageCast X states that the agency "has no evidence that these vulnerabilities have been exploited in any elections" (CISA ICSA-22-154-01). That sentence is accurate and it is also nearly uninformative, because the same advisory documents a vulnerability class in which the attacking software can conceal itself from the audit mechanism. Where the detection capability is absent, the absence of detections carries no evidentiary weight. Any security engineer will say so; so will any accident investigator.

3.1 Materiality: the threat model does not require widespread exploitation

A recurring category error governs public discussion of this subject. Assurances are offered at national scale — no evidence of *widespread* fraud, no evidence of exploitation *in any election* — against a threat model that has never required either.

A presidential election is decided in a handful of jurisdictions. The certified 2020 margins were:

State	Certified margin	Margin as %	Smallest single county capable of supplying it
Georgia	11,779	0.23%	Fulton
Arizona	10,457	0.31%	Maricopa
Wisconsin	20,682	0.63%	Milwaukee or Dane
Pennsylvania	80,555	1.16%	One southeastern county
Nevada	33,596	2.39%	Clark
Michigan	154,188	2.78%	Wayne

(Certified margins as compiled in the companion analysis supplied as Exhibit 14; the county-level arithmetic follows directly from the certified margins and the counties' certified totals.)

The operational consequence is decisive. **An adversary seeking to change a presidential outcome does not need access to 3,000 counties. It needs access to five, and it needs to know which five — which is precisely what the intelligence described in Area A provides.** A finding of "no widespread exploitation" is therefore not a finding about the threat. It is a finding about a threat nobody has posited.

The same logic governs the evidentiary demand. Evidence of exploitation in a handful of counties would, by construction, look local, anomalous, and dismissible as error — which is exactly how the documented anomalies in this memorandum have been treated.

3.2 "Programming mistake" is a conclusion, not an explanation

When an electronic voting system produces an impossible or contested result, the standard institutional response is to attribute it to human or programming error and declare the matter closed. Sometimes that attribution is documented. Often it is not. The two cases must be distinguished, and the distinction turns on one question: **was the artifact produced, examined by an independent party, and shown to generate the observed anomaly?**

Where the standard is met. In Mesa County, Colorado, a forensic report alleged the "unauthorized creation of new election databases during early voting… on October 21, 2020, followed by the digital reloading of 20,346 ballot records… making the original voter intent recorded from the ballots unknown," and asserted there was "no function or feature on the EMS server that could be executed inadvertently or deliberately by a local election official that would cause this combination of events" (Mesa County Report #3). The rebuttal met the burden: a District Attorney investigation using **video evidence, staff interviews, and an operational recreation of the disputed events** concluded the extra databases "were created by human action when the Elections Manager attempted troubleshooting during adjudication," and that all ballots were accounted for through required system backups (Colorado County Clerks Association analysis). That is a real examination and it is credited here as such.

It also contains its own indictment. Report #3's Finding 6 records that **"Dominion's installation of the Trusted Build update on the EMS in May of 2021, as ordered by the Colorado Secretary of State, destroyed all data on the EMS hard drive."** Whatever the correct interpretation of the underlying anomaly, a vendor update ordered by a state destroyed the forensic record of a federal election on a machine subject to the 22-month federal retention requirement of 52 U.S.C. § 20701. That is not disputed by either side.

Where the standard is not met. The Michigan absentee-records matter, treated in full in Area B, is the controlling example: a state offered a mechanism as the explanation for an anomaly in its own published records, declined to produce the mechanism, and denied the records request that sought it. Under the standard applied here that anomaly's cause is **asserted and corrected by assertion, and remains unverified.**

3.3 The reliability of "debunked" as a status

A large number of election-technology claims carry the public status "debunked." The provenance of that status is documented, and it is not independent of the parties whose systems are at issue.

The Election Integrity Partnership, a consortium centered on the Stanford Internet Observatory, processed **639 in-scope tickets** during the 2020 cycle, of which "72%… were related to delegitimizing the election results," and reported that **"35% of the URLs we shared with Facebook, Instagram, Twitter, TikTok, and YouTube were either labeled, removed, or soft blocked"** (*The Long Fuse*, court-filed copy, pp. 27, 42). The Center for Internet Security — which operates the Elections Infrastructure Information Sharing and Analysis Center — "reported 16% (N = 101) of our tickets," and the report states that "content reported by election officials to the EI-ISAC was also routed to the EIP ticketing system," with the EI-ISAC serving as "a singular conduit for election officials to report false or misleading information to platforms" (pp. 12–13, 28, 42).

A House Judiciary Committee majority staff report — a partisan committee product, and labeled as such here — states that "led by Stanford, the EIP was devised and founded in close coordination with CISA," that "CISA and the EIP were completely intertwined," and that CISA "had personnel with direct access to the EIP ticketing system" (staff report, pp. 11, 44, 55). It records that the Democratic National Committee submitted tickets and the Republican National Committee declined the invitation (p. 36). EIP's own director disputes the characterization, stating that "CISA did not send any examples of potential misinformation to EIP," that platforms "not EIP, decided which action to take," and that the partnership "began under the Trump administration… reviewed and approved by Trump Administration attorneys" (EIP statement).

A necessary legal correction. The Fifth Circuit held in *Missouri v. Biden* that "CISA likely significantly encouraged the platforms' content-moderation decisions and thereby violated the First Amendment" (opinion, pp. 59–60). **That holding was reversed.** In *Murthy v. Missouri* the Supreme Court held that "neither the individual nor the state plaintiffs have established Article III standing" and stated "we lack jurisdiction to reach the merits" (slip opinion). There is no surviving merits holding that CISA violated the First Amendment, and this memorandum does not cite one. The Court did, however, describe the underlying conduct as fact: "Until mid-2022, CISA, through its 'switchboarding' operations, forwarded third-party reports of election-related misinformation to the platforms."

The consequence for this memorandum's method is procedural, not substantive: **the public status of an election-technology claim is not evidence about the claim.** Every assertion here is evaluated against

primary documents, and its suppression history is treated as irrelevant in both directions — a claim is not strengthened by having been suppressed, and it is not weakened either.

The institutional conflict in the assurances themselves

CISA occupied both roles simultaneously: the agency responsible for assessing the security of election infrastructure, and a participant in the process by which claims about that infrastructure's security were routed to platforms for action. Its own TLP:AMBER assessment documented that a third of assessed entities ran unsupported operating systems, while its public posture emphasized the security of the enterprise. Both were CISA products. **An agency that both grades the exam and manages the publicity about the grade cannot be the sole authority on its own performance.** That is an institutional observation and requires no inference about anyone's state of mind — which is why this memorandum reaches its conclusions from CISA's own documents rather than from claims about CISA's personnel.

3.4 The central assurance depends on controls that were not implemented

The most authoritative document asserting that known voting-system vulnerabilities are not practically exploitable is MITRE's *Independent Technical Review: Security Analysis of Georgia's ImageCast X Ballot Marking Devices*, hosted by the Georgia Secretary of State (MITRE report). Its conclusion is quoted constantly: the proposed attacks were "operationally infeasible given two parameters: the normal operating procedures of a voting precinct and associated officials, and scale considerations."

Three features of that document are rarely quoted alongside it.

First, MITRE did not dispute that the vulnerabilities exist. It assumed they were valid: "The researcher's proposed QR code tampering attacks are assumed to be valid"; "The researcher's proposed creation and use of unofficial smart cards is assumed to be a valid attack vector." The dispute was never about whether the holes were real.

Second, MITRE's finding of infeasibility rests explicitly on assumed compensating controls which were "derived and adapted from recommended mitigations in the June 2022 Cybersecurity & Infrastructure Security Agency (CISA) advisory" (Appendix B, Table 13).

Third, the researcher whose findings MITRE reviewed has documented that Georgia did not implement those mitigations. That gap — between the controls MITRE assumed and the controls actually in place — is the entire distance between "secure" and "vulnerable," and it was never closed on the record. Computer scientists publicly challenged the report on related grounds (open letter to MITRE).

Applying the standard stated at the outset: the assertion "these systems are operationally secure" has not been substantiated. It has been asserted, conditioned on facts not established, by a contractor engaged by the party being reviewed.

Where the record contradicts a claim favorable to this memorandum's conclusion, the contradiction is stated. Several widely circulated claims do not survive contact with primary sources. They are identified as they arise. A brief addressed to the President that omitted them would not survive its first serious technical review, and the case is strong enough that it does not need them.

4 Areas of Concern

4.1 Area A — The Intelligence Platform

Every certified system in Michigan was required to interface with the voter registration database

This is not an inference from architecture diagrams. It is a procurement requirement, answered "Y" by the vendor, in a state contract.

Michigan's contract with Dominion Voting Systems, 071B7700117, Exhibit 2 to Schedule A, Attachment 1.1, records the following mandatory technical requirements and the vendor's responses (supplied as Exhibit 13):

Requirement	Text	Dominion's answer
1.2.B.11	"Contractor shall demonstrate how data can flow from the State Qualified Voter File (QVF) into EMS and the formats in which data can be imported/exported"	**Y** — "Democracy Suite EMS is capable of importing election definition data from the QVF using the Election Data Translator module"
§ 1.5 C, State Uniform Data Format	Compliance with the Michigan QVF Export File Format as "the State's current uniform data structure for use with Contractor's voting system EMS software"	**Y**
1.2.D.16	The ENR system shall import Ballot Definition Data using the Michigan QVF Export File Structure	**Y** — "Michigan ENR codes are imported from the QVF file during the election definition phase"
Results output	Results exported in the **Michigan Standard Results File Format (MSRFF)**	**Y**

The same requirement set applies to the other certified vendors. Hart InterCivic's contract, 071B7700128, § 1.5 C, provides:

> "Contractor agrees and will comply with Michigan-specific uniform data format requirements and Federal IEEE Standards. Exhibit 3 to Schedule A, Michigan QVF Export File Format contains the State's current uniform data structure for use with Contractor's voting system EMS software."

(Michigan contract 071B7700128; state contract register.) The ES&S bid states the same requirement more plainly still — **1.2.B.11: "Bidders shall demonstrate how data can flow from the State Qualified Voter File (QVF) into EMS"** — and its response describes the mechanism: "By extracting the Michigan QVF Export File records by type (0 through 9), into individual files, the EVS Election Management product supports import of the Michigan QVF Export File Structure" (ES&S bid).

Three vendors were approved for statewide use in Michigan on January 24, 2017 — Dominion, ES&S and Hart InterCivic (Michigan Secretary of State) — and all three were required to interface with the Qualified Voter File. The QVF interface is not a vendor design choice that a state might have avoided by selecting a different bidder. It is the condition of doing business.

An accuracy correction required by the standard. What these documents establish is a **required file-format-level data path** from the statewide voter registration database into the vendor's election management software and onward into the election-night reporting system. They do not establish a requirement that vendors maintain a live network connection to the registration database, and this report does not claim one.

The documented architecture. Michigan's electronic pollbook manual states that "the electronic pollbook software is **downloaded from the Qualified Voter File (QVF) software** and is loaded to a laptop prior to each election," and that after the election the pollbook "generates a voter history file that can be uploaded into QVF," both transfers via encrypted flash drive (Michigan EPB manual). The software running on election-day pollbook laptops originates in the statewide voter registration database, and data flows back into it.

And the direction of travel is toward live connectivity. The Michigan House Fiscal Agency's analysis of the electronic pollbook rule states that **"current law neither provides for nor prohibits a live connection of the EPB to the internet,"** that 2023 PA 81's early voting pollbook "was made as a web-based application with a secure live connection to the QVF," and that under the proposed rule jurisdictions "would be permitted to access the EPB on election day via a live secure connection to the

QVF." The analysis specifies **no network architecture, no encryption standard, no authentication method, and no offline fallback requirement** (House Fiscal Agency).

Federal guidance runs the opposite way. Draft VVSG 2.1 states it "does not permit devices or components using external network connections to be part of the voting system," and expressly contemplates "externally networked devices or components, such as those used for e-pollbooks" (draft VVSG 2.1). VVSG 2.0 implementation guidance states systems "must not be configured to establish a connection to an external network" (NIST). **The federal standard forbids what state practice is moving toward, and the federal standard is voluntary.**

The national security consequence. Where a required data path exists between the voter registration database and the ballot-production and tabulation software, the two systems share a trust boundary. An adversary with write access to voter registration data influences what ballot styles are produced, for whom, and in what quantity — without ever touching a tabulator. An adversary with read access obtains the roster of the American electorate and the operational state of the count. The two targets are not independent, and no federal requirement isolates them.

Nine confirmed vulnerabilities, including unauthorized ballot printing

On June 3, 2022, CISA issued advisory ICSA-22-154-01 covering nine CVEs in the Dominion Democracy Suite ImageCast X (CISA). The advisory's own language:

CVE	WEAKNESS	CISA'S DESCRIPTION
CVE-2022-1739	Improper verification of cryptographic signature	"does not validate application signatures to a trusted root certificate… An attacker could leverage this vulnerability to install malicious code, which could also be spread to other vulnerable ImageCast X devices via removable media"
CVE-2022-1740	Mutable attestation reporting	The "on-screen application hash display feature, audit log export, and application export functionality rely on self-attestation mechanisms. An attacker could leverage this vulnerability to disguise malicious applications on a device"
CVE-2022-1741	Hidden functionality	"has a Terminal Emulator application which could be leveraged by an attacker to gain elevated privileges on a device and/or install malicious code"
CVE-2022-1742	Improper protection of alternate path	"allows for rebooting into Android Safe Mode, which allows an attacker to directly access the operating system"
CVE-2022-1743	Path traversal	"can be manipulated to cause arbitrary code execution by specially crafted election definition files. An attacker could leverage this vulnerability to spread malicious code to ImageCast X devices from the EMS"

CVE-2022-1744	Execution with unnecessary privileges	Applications "can execute code with elevated privileges by exploiting a system level service"
CVE-2022-1745	Authentication bypass by spoofing	The technician authentication mechanism "is susceptible to forgery. An attacker with physical access may use this to gain administrative privileges"
CVE-2022-1746	Incorrect privilege assignment	The poll-worker mechanism "can expose cryptographic secrets used to protect election information… potentially affecting other election equipment"
CVE-2022-1747	Origin validation error	The voter session activation mechanism "is susceptible to forgery. An attacker could leverage this vulnerability to **print an arbitrary number of ballots without authorization**"

Read together, these describe a system in which the audit log cannot be trusted to report tampering with the system that writes it (CVE-2022-1740), malicious code can propagate from the central election management system to every device in a jurisdiction (CVE-2022-1743), and an unauthorized party can generate unlimited ballots (CVE-2022-1747). The last of those is the ballot-ordering mechanism described in Area B, confirmed by the federal cybersecurity agency as a property of a certified device.

Two of CISA's own recommended mitigations are admissions about prevailing practice. The advisory instructs jurisdictions to **"use separate, unique passcodes for each poll worker card"** and to **"disable the 'Unify Tabulator Security Keys' feature on the election management system and ensure new cryptographic keys are used for each election."** One does not recommend unique passcodes where passcodes are already unique, and a vendor does not ship a feature called *Unify Tabulator Security Keys* unless the intended behavior is a single key across many tabulators.

CISA's own assessment of the 2020 election year

CISA's *Election Infrastructure Subsector Cyber Risk Summary* (March 2021), covering November 3, 2019 through November 3, 2020, reports the following for election infrastructure entities enrolled in its scanning and assessment services (Exhibit 9, marked TLP:AMBER):

FINDING	CISA'S FIGURE
ENTITIES WITH CRITICAL OR HIGH-SEVERITY VULNERABILITY ON AN INTERNET-ACCESSIBLE HOST	**48%**
ENTITIES RUNNING AN UNSUPPORTED OPERATING SYSTEM ON AN INTERNET-ACCESSIBLE HOST	**34%** (33.6%)
ENTITIES RUNNING A RISKY SERVICE ON AN INTERNET-ACCESSIBLE HOST	**39%**

ASSESSED ENTITIES WITH SPEARPHISHING WEAKNESSES	**76%** (73% of assessments)
MEDIAN DAYS TO REMEDIATE, ALL SEVERITIES	**103.7 days**
MEDIAN DAYS TO REMEDIATE CRITICAL VULNERABILITIES WITH KNOWN PUBLIC EXPLOITS	**108 days**
AVERAGE VULNERABILITY BACKLOG PER ENTITY AT YEAR END	74.2
ENTITIES EXPOSING FTP	28%
ENTITIES EXPOSING RPC	13%
ENTITIES EXPOSING REMOTE DESKTOP PROTOCOL	12.3%
PHISHING CLICK RATE, ELECTION ENTITIES	**17.4%**
PHISHING CLICK RATE, ALL OTHER STATE/LOCAL/TRIBAL CRITICAL INFRASTRUCTURE	9.6%

The unsupported operating systems counted were Windows 7, Vista, XP, Server 2003 and Server 2008.

Three observations follow directly. **One-third of assessed election entities were running operating systems that no longer received security patches at all. Critical vulnerabilities for which working public exploits existed remained unremediated for a median of 108 days** — meaning that a vulnerability disclosed at the start of a primary season would, on average, still be open when voting concluded. And **election personnel clicked test phishing links at roughly 1.8 times the rate of comparable government personnel**, in the sector designated as critical infrastructure precisely because it is targeted.

This document is CISA assessing itself and its own stakeholders, four months after the election it covers, in a channel restricted from public view. It is the most candid federal statement of election infrastructure security posture available, and it does not describe a secure enterprise.

A federal agency published the file manifest

NIST's Information Technology Laboratory maintains a **Voting Software Reference Data Set**. Its page states that "NIST has also made available a supplementary set of Dominion Voting D-Suite 5.12-NV software," and links directly to a spreadsheet on a public Amazon S3 bucket (NIST; Exhibit 2). The linked object is:

> s3.amazonaws.com/rds.nsrl.nist.gov/voting/Nevada_2020-01-23/ Nevada_Voting_Jan_2020.xlsx

The spreadsheet's columns are SHA-1, MD5, CRC32, FileName, FileSize, ProductCode and OpSystemCode. Its rows include `RSAKeyPairGenerator.class`, `EphemeralKeyManager$EphemeralKeyPair.class`, `SerializationHandler.class`, and `ManualPrecinctInput$1.class`. The page was created June 27, 2016 and updated January 28, 2020.

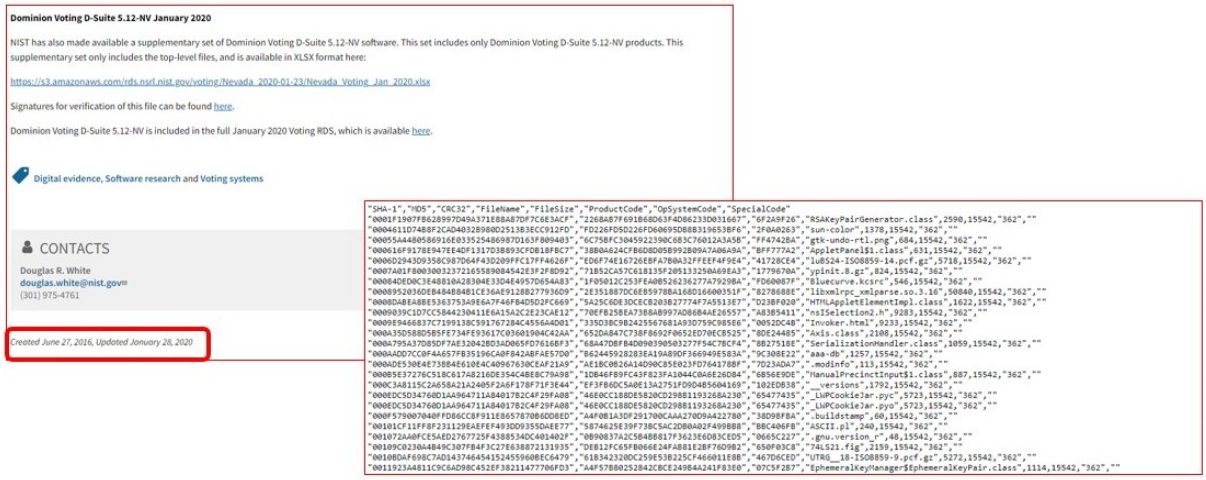

Exhibit 2. A compiled slide reproducing (left) the NIST Voting Software Reference Data Set page describing the "supplementary set of Dominion Voting D-Suite 5.12-NV software" with its public S3 link, and (right) rows from the published manifest itself, including the `RSAKeyPairGenerator.class` and `EphemeralKeyManager$EphemeralKeyPair.class` entries with their SHA-1, MD5 and CRC32 values. The headline is the compiler's characterization, not NIST's. The underlying page and spreadsheet are verifiable at the linked NIST URL.

The stated purpose of a reference data set is legitimate: it lets an examiner confirm that a machine is running the software it is supposed to be running. But the artifact produced is a complete inventory of a certified voting system's build, naming its cryptographic components, published on a public object store with no access control.

The intent question. Two readings are available. Under the benign reading, NIST published a verification aid and did not adequately consider that the same file is a reconnaissance aid. Under the adverse reading, the publication was deliberate. **The record does not resolve which is correct, and this memorandum does not assert the adverse reading.** What the record does establish is that the effect is the same either way: an adversary planning to modify a certified system was handed, by a federal standards body, the file names, sizes and hashes of the target — and, critically, the knowledge of exactly which hash values a modified build would need to reproduce in order to pass a hash-verification check.

That last point connects to CVE-2022-1740. Hash verification on these devices relies on self-attestation — the running software reports its own hash. The published academic finding is that "malware that has infected the ICX can completely conceal itself from the kind of hash validation performed in Georgia, which relies on the running software to self-attest to its integrity" (summarized in a City and County of San Francisco memo). A published manifest of expected hashes, combined with a verification mechanism

that asks the software to grade itself, is a control that provides the appearance of assurance without the substance.

Under the burden of proof stated at the outset, the relevant question is not whether NIST intended harm. It is whether any federal official can point to a documented risk assessment weighing the reconnaissance value of that publication against its verification value. No such assessment was located.

External programmatic access to voter registration data, and a read capability that was removed from the documentation

Third parties hold authenticated, programmatic pathways into state voter registration systems. The architecture is documented by the operators themselves.

Rock the Vote's "Connected Voter Registration" describes "a simple, secure, **one-way** transfer of voter registration applications from approved and authorized third-parties to the state election office," via an "Application Programming Interface (API) that connects the interface a user sees with the internal systems that states use to process registration data." Authorized parties are "Designated Partners" — "authorized and trusted third parties with **pre-approved IP addresses**" — each assigned "a unique platform key," which "acts as a password" and can be revoked (Rock the Vote).

The "one-way" characterization describes the current published documentation. It does not describe the documentation's history.

Earlier published versions of the same API documented **read** endpoints alongside the write endpoints. At repository commit `e4fa5583b1`, dated March 18, 2019, the specification documents:

- **`GET /api/v3/registrations.json`** — "For a given partner… returns partner-specific registration records," with optional `email` and `since` filters. The response records contain **status, create_time, first_name, middle_name, last_name, home_address, home_city, home_state_id, home_zip_code, mailing address fields, race, party, phone, email_address, opt_ins, survey answers, finish_with_state, and created_via_api.**
- **`GET /api/v3/gregistrations.json`** — the government-partner analogue, for entities such as a local elections office.
- Additional read endpoints: `GET /api/v3/registrations/pdf_ready`, `GET /api/v3/partners/[partner_id].json`, `GET /api/v3/state_requirements.json`, and `GET /api/v2/gregistrations.json` from the prior version.

(V3 source at commit e4fa5583b1)

The current V4 documentation's release notes list, under the heading **"Removed": GET /api/v4/registrations and GET /api/v4/gregistrations** (Rock the Vote API documentation). Read capability was not eliminated outright; it survives in narrower form through `POST /api/v4/registrant_reports` and `GET /api/v4/registrant_reports/<ID>/download`, which returns a CSV.

The documented revision history of the specification is as follows (repository commit log):

DATE	COMMIT	MESSAGE
2016-08-25	initial	"WIP RtV docs"
2018-10-02	ea93b2c524	"**add 'before' to GET registrations call**"
2019-08-30	1a640aed42	"Updated docs for pending V4 updates"
2019-09-18	f9943b656e	"v4 updates"
2022-05-19	6128335437	"remove gregistrant support"
2022-09-21	fb0b5d42f8	"updated copy"

Three points follow, and the third is the one that matters.

First, the honest scope limitation, stated because the standard requires it. The documented read endpoints were **partner-scoped**. They returned only records the authenticated partner itself had submitted — "the records returned are only those pertinent to the authenticated entity." **Nothing in either version documents a voter-roll lookup, a registration-status query against a state's official list, or bidirectional synchronization with a state voter registration database, and no such capability is asserted here.** A claim that non-governmental organizations can read or edit state voter rolls is not supported by this record.

Second, what is supported is still significant. Registrant personally identifiable information — full name, residential address, mailing address, party, race, telephone and email — was retrievable over an ordinary HTTP GET by an authenticated party whose authentication rested on a platform key and an IP allowlist. That is a documented external read surface over the personal data of American voters, governed by no federal standard.

Third, and this is the point the record actually establishes: removal from the documentation is not evidence of removal from the system. The V4 release notes state that the endpoints were removed. **No security rationale for the removal was published, and no source examined in the preparation of this memorandum establishes the actual runtime configuration of the interface at any point in time.** The read functionality may have been disabled. It may equally have been retained and merely

withdrawn from the published specification. **On the record available, we do not know which, and neither does any party outside the operator.** Under the standard applied throughout this document, a vendor's or an operator's assertion about its own configuration is a claim requiring documentary support, and no such support — no audit, no attestation, no independent examination — exists here.

That is the finding: **an external programmatic interface to the personal data of American voters, whose documented read capability was withdrawn from publication without explanation, and whose actual capabilities no independent party can verify.**

The related aggregation point belongs in the same frame. The suggestion that ERIC holds "read / write access" appears in the record as a **question posed in advocacy testimony**, not as an established fact (Michigan House committee testimony); ERIC's own documentation describes a member-push, report-return model in which "at least every 60 days, each member submits their voter registration data and licensing and identification data from motor vehicle departments (MVD) to ERIC" (ERIC). **That is not an allegation of improper access. It is a description of a repository that aggregates full voter registration records plus state motor vehicle licensing and identification data across member states** — a high-value intelligence target by construction, whose transfer method, protocol, encryption and credentialing are not stated in its public documentation.

Foreign entities in the handling chain

Directive: the transfer of sensitive election records to foreign entities exacerbates the national security risk. **The record supports a narrower and more defensible version of that proposition.**

- **Offshore software development, on the vendor's own admission.** Dominion spokesman Chris Riggall, on the record: "**Like many of America's largest technology companies… some of our software development is undertaken outside the U.S. and Canada, specifically, in Serbia, where we have conducted operations for 10 years**" (CSO Online). The same statement adds that "all of our software is developed in-house by DVS employees and this work is not outsourced to third parties." That is a documented instance of development labor for American election software performed abroad.
- **Foreign-manufactured components, on the vendor's own admission.** ES&S states: "**ES&S utilizes a global supply chain and some components used in our voting machines are produced in countries outside the USA**," and that "some components may be sourced from China-based manufacturers," while maintaining that "**all ES&S tabulation software is developed and compiled exclusively in the USA**" and that final hardware configuration is "performed exclusively

in the USA." Its FAQ refers to "our overseas manufacturing site" audited on-site by the EAC (ES&S). Independent reporting on shipping records found many parts, including electronics and tablets, made in China and the Philippines (NBC News).

- **Corporate lineage.** Dominion originated in Toronto; Staple Street Capital acquired a controlling interest in 2018 for **$38 million**; the company was sold in 2025 to a firm led by Scott Leiendecker and renamed **Liberty Vote**, described as "100 percent American-owned" (CBC News).
- **An allegation concerning poll-worker data and contractors in China.** In October 2022 the Los Angeles County District Attorney charged Konnech Inc.'s founder Eugene Yu with "conspiracy to embezzle public funds; grand theft by embezzlement of public funds" over a $2.65 million poll-worker-management contract that "specified that only U.S. citizens and permanent residents would have access to Los Angeles County's poll-worker data," alleging that third-party contractors in China were sent election-worker data (NPR; FactCheck.org). Detroit City Clerk Janice Winfrey terminated the city's contract "out of an abundance of caution," and at least four jurisdictions stopped using the software (NPR).

The defensible national security finding. Federal elections are conducted on equipment containing foreign-manufactured components, running software some of which was written abroad, supported by ancillary contractors whose data-residency obligations have been the subject of contested litigation — and **no federal regime requires disclosure, attestation, or audit of where the software of a certified voting system is written, where its components are manufactured, or where the personal data handled by uncertified ancillary systems is processed.** The Konnech episode's actual lesson is not that a crime was proven; it is that a data-residency term in a county contract became the subject of a criminal prosecution, a dismissal, a $5 million settlement and a proclamation of innocence, and **at the end of that process no authoritative finding exists about where the data went.** That is precisely the evidentiary vacuum this memorandum is about.

The vendor lineage, and a federal criminal indictment

The persistence of a design pattern across nominally competing vendors is easier to understand once the corporate and technical lineage is traced. The following is drawn from the evidence compilation supplied as Exhibit 10, with each element traceable to a primary record.

Corporate chain.

- Smartmatic was incorporated in Delaware on April 11, 2000.

- **Smartmatic acquired Sequoia Voting Systems on March 9, 2005**, and began integrating "its new Venezuela-developed technology with the legacy product line."
- **Dominion Voting Systems acquired Sequoia's assets — including software, firmware and hardware intellectual property — in 2010** (announced June 4, 2010), having acquired Premier on May 19, 2010 with Department of Justice approval.

The intellectual property did not stay behind. In *Smartmatic Corp. v. SVS Holdings, Inc.*, Delaware Court of Chancery C.A. No. 3585-VCL (April 4, 2008), the court recorded that Hart InterCivic's counsel **stated on the record** that "Sequoia currently uses [Smartmatic's] intellectual property [currently found in Sequoia's machines] pursuant to certain license agreements," and that the proposed transaction included Smartmatic granting Hart "a license to use its intellectual property currently found in Sequoia's machines." This is not an allegation by a critic. It is a representation by a competing vendor's counsel, in open court, three years after the acquisition.

The product line is named in the integration-era documentation. The Smartmatic–Sequoia glossary defines **SAES — "Smartmatic Automated Election System" — as "voting software with Venezuelan government shareholding."** It defines the **SAES 3000** as the "Direct Recording Electronic, voting machines used in all the elections of President Hugo Chavez," evolving into the SAES 3300, 4000 and 4200. It defines **HAAT** as the "precinct level accumulator for consolidating and printing the consolidated results and **for transmission of unofficial results** from all precinct voting devices," and **Edge2Plus** as a DRE "developed exclusively for the American market." NIST hosts a Sequoia/Smartmatic technical report from this period (NIST).

Note what HAAT is: a precinct accumulator whose documented function includes transmitting unofficial results. The election-night reporting architecture examined in Areas D and E is not a later American addition. It is in the product definition, in the Venezuelan-shareholding product line, from the beginning.

And the company at the head of that lineage is now a federal criminal defendant. On **October 16, 2025**, a superseding indictment was returned in the United States District Court for the Southern District of Florida, No. 1:24-cr-20343-KMW, adding **SGO Corporation Limited — "commonly known as 'Smartmatic' or the 'Smartmatic Group'"** — as a corporate defendant alongside four individuals originally indicted in August 2024 (DOJ FCPA case page; DOJ press release).

ITEM	THE GOVERNMENT'S ALLEGATION
CORPORATE DEFENDANT	**SGO Corporation Limited**, "commonly known as 'Smartmatic'"

INDIVIDUAL DEFENDANTS	**Roger Alejandro Piñate Martinez**, 50 — charged as Smartmatic "co-founder, part owner, and executive" and SGO's "director, stockholder, and **Chief Operating Officer**"; **Jorge Miguel Vasquez**, 64, who "managed hardware development and manufacturing worldwide"; **Elie Moreno**, 45, project director for Smartmatic Philippines; **Juan Andres Donato Bautista**, 61, former Chairman of the Philippine Commission on Elections
CONDUCT ALLEGED	Between 2015 and 2018, causing "at least **$1 million in bribes**" to be paid to the COMELEC chairman to obtain and retain business, "including the release of favorable value added tax (VAT) reimbursements"
SOURCE OF THE FUNDS	A slush fund created "by **over-invoicing the cost per voting machine supplied for the 2016 Philippine elections**"
CONTRACT VALUE AT ISSUE	₱8,518,813,380.96 ≈ **$182,351,868** across three 2015 contracts covering 93,977 voting machines and transmission services
CONCEALMENT ALLEGED	"used coded language, created fraudulent contracts and sham loan agreements, and routed transactions through bank accounts in Asia, Europe, and the U.S."
CHARGES	Conspiracy to violate the FCPA, 18 U.S.C. § 371; substantive FCPA, 15 U.S.C. § 78dd-2; money laundering conspiracy, 18 U.S.C. § 1956(h); three counts of international money laundering, 18 U.S.C. § 1956(a)(2)(A)
MAXIMUM PENALTIES	20 years per money laundering count; 5 years per FCPA count

(All rows: DOJ press release and superseding indictment.)

Why this bears on trustworthiness, stated precisely. The government's allegation is that the mechanism used to generate corrupt funds was **the price charged per voting machine**. If proven, that is a finding that the commercial relationship between an election vendor and an election authority was itself the instrument of the offense — that the invoice for the machines was the vehicle. A vendor whose per-machine pricing is alleged by the United States to have concealed bribes to the official responsible for buying the machines is not a party whose unaudited assurances about its own software should be accepted on trust. **That is the entire evidentiary use made of this indictment here.**

The limits, stated in the same paragraph, because omitting them would forfeit the point.

- **These are allegations, not findings.** Piñate has pleaded **not guilty** and no longer works at Smartmatic, though he remains a shareholder; SGO moved on **March 10, 2026** to dismiss the superseding indictment for vindictive and selective prosecution, asserting that it had cooperated since 2021 and produced millions of pages (SGO motion to dismiss; San Francisco Chronicle).
- **No vote manipulation is alleged.** Reuters, reporting the original indictment: "**No voter fraud has been alleged**" (Reuters). The conduct charged is Philippine bribery and money laundering. No United States election outcome is implicated in the indictment, and none is implied here.

- **No defendant has pleaded guilty.** DOJ states that "Bautista and Moreno are fugitives and remain at large"; Bautista has been in Canadian custody since a 2023 arrest, and in August 2025 the Ontario Superior Court committed him to await surrender on extradition (DOJ; GMA News).

Architectural continuity is alleged in sworn testimony and must be labeled as allegation. A Colorado federal filing contains testimony from a former senior Venezuelan election official asserting that Dominion's software in United States counties exhibits "the same structure and vulnerabilities" as Smartmatic systems used in Venezuela, specifically naming **"encryption flaws, plaintext credentials, small/overwriting logs, adjudication pathways, and remote access avenues"**; that Smartmatic engineers later held positions inside Dominion's US operation; and, on examining the Mesa County forensic images, that the witness observed "the same system bugs which would be used to manipulate or change an election… errors in the encryption systems." Dominion's US Patent 8,876,002 describes networked configuration, remote software loading, warehouse support and asset tracking for voting devices.

This is testimony in a contested matter and is not treated here as established fact. But two things about it are checkable and check out. The five categories the witness named — encryption flaws, plaintext credentials, overwriting logs, adjudication pathways, remote access — **correspond one-to-one with findings independently documented by CISA, by state-commissioned reviews, and by academic examination.** And a declassified 2026 intelligence assessment concluded that Smartmatic's Venezuelan connections present a "moderate overall threat to US national security interests" (CIA/NIC memo, declassified June 29, 2026).

Practices that persist across two decades and every vendor

The pattern is not one vendor or one generation. It is the same set of practices, found by every serious examination, for twenty years — which is why the intelligence exposure is structural rather than incidental.

Shared credentials, admitted and defended. Maricopa County's own reviewer confirmed generic accounts as fact and defended them: "Since access to the network is closed to outside resources and access to the BTC is controlled and monitored, it is understandable why Maricopa County chose to use generic accounts and passwords." The compensating controls offered were physical: key fobs, badge access, cameras (county response).

Unsupported operating systems in the field. Georgia's Democracy Suite 5.5-A "uses Android 5.1.1, which has not been updated (even to address security vulnerabilities) since 2015" (SF memo). CISA's

TLP:AMBER assessment found 34% of entities running unsupported operating systems on internet-accessible hosts.

Broken authentication and recoverable cryptographic secrets. "The ICX uses smartcards to authenticate service technicians, poll workers, and voters, but the smartcard authentication protocol is completely broken." Attackers "can create counterfeit technician cards that give them root access to the machine, steal county-wide cryptographic secrets from access cards used by poll workers, and create 'infinite' voter cards that allow an unlimited number of ballots" (same source). CISA independently confirmed the same three findings as CVE-2022-1745, -1746 and -1747.

Updates that create new escapes. "As a result of a botched Dominion software update installed by Georgia, anyone can attach a keyboard and press alt+tab to access Android Settings, then open a root shell or install arbitrary software" (same source).

Default passwords and deliberate password bypasses. Ohio's Project EVEREST, an official state-commissioned review, found: "Most service menu items require the user to enter a password. The iVotronic **defaults to specific passwords** unless they have been explicitly changed" (§ 7.2.8). And: "The iVotronic system contains a **backdoor that bypasses all passwords** when a Factory QA PEB (also called a Debug PEB) is inserted." That PEB type "behaves essentially as a supervisor PEB but… does not require the entry of any passwords," and "can be used to neutralize the security of any iVotronic administration features that depend on passwords, **no matter how carefully passwords are managed by a county**" (§§ 6.1.1, 7.2.10) (EVEREST final report, EAC-hosted).

Cryptography implemented so as not to function. EVEREST: "the ES&S system does not employ cryptography at all in the M100-based optical scan system. The iVotronic DRE system does use cryptography, but errors in its implementation render the protection completely ineffective," and "although much of data on the PEB is encrypted, there is unencrypted information stored along with it that allows an attacker to easily discover the key" (§§ 6.4, 6.4.2). California's Top-to-Bottom Review reached the same conclusion across vendors: **"We could not find a single instance of correctly used cryptography that successfully accomplished the security purposes for which it was apparently intended."** One Diebold password was **"diebold."** Sequoia "invented their own password encryption algorithm," under which "the password 'sekret' encrypts to 'sekretXYZ'" (Wagner, California TTBR overview).

Physical keys common to every machine in the country. EVEREST, § 7.3.5, on the M100 scanner: **"These two keys differ from each other, but are the same for all M100 machines. These keys are**

available online from ES&S for $5.00 each," and "the key blanks for a scanner and ballot box key are easily duplicated, so a compromise of either key could affect machines nation-wide." Firmware upload to the M100 "does not require a password" (§ 7.3.1).

Implicit trust between networked components. California's review of Hart: "When you connect a polling-place machine to the county's central PC, it trusts the PC implicitly." / "The county PC can instruct the machine to overwrite its software, and it will blindly comply. **(No authentication!)**" And in the reverse direction: "The voting machine can exploit buffer overruns in the code on the PC to take control of the PC" (Wagner). CISA confirmed the same propagation path in a current system fifteen years later, as CVE-2022-1743.

A caveat required by the standard: the EVEREST and California findings concern 2006–07 equipment, some since decertified. They are cited to establish the persistence and cross-vendor character of the pattern, not to describe the current fleet. For current systems the governing documents are the nine CISA CVEs and CISA's own 2021 risk summary.

One class of vulnerability is unambiguously a designed feature, because the vendor named it. A configuration option called *Unify Tabulator Security Keys*, which CISA instructs jurisdictions to disable, is not an oversight. Someone specified it, implemented it, and shipped it as the default in enough deployments that the federal cybersecurity agency had to tell jurisdictions to turn it off. The same is true of the Terminal Emulator application that CISA classifies under CWE-912, *Hidden Functionality* (CVE-2022-1741), and of the Factory QA PEB that Ohio's reviewers described as "a backdoor that bypasses all passwords." Undocumented password-bypass mechanisms and shipped key-unification features are engineering decisions. They may have been made for convenience of servicing rather than for manipulation — but they were made, and **this memorandum does not assert that they were made for the purpose of manipulation.** The intent question is unresolved on the available record and does not need to be resolved, for the reason given in Area D: the certification regime guarantees that such features persist whatever their origin.

4.2 Area B — The Ballot Ordering System

"Ballots when and where you want them"

Dominion Voting Systems markets a Mobile Ballot Printing capability under the slogan **"BALLOTS WHEN & WHERE YOU WANT THEM!"** (Exhibit 1).

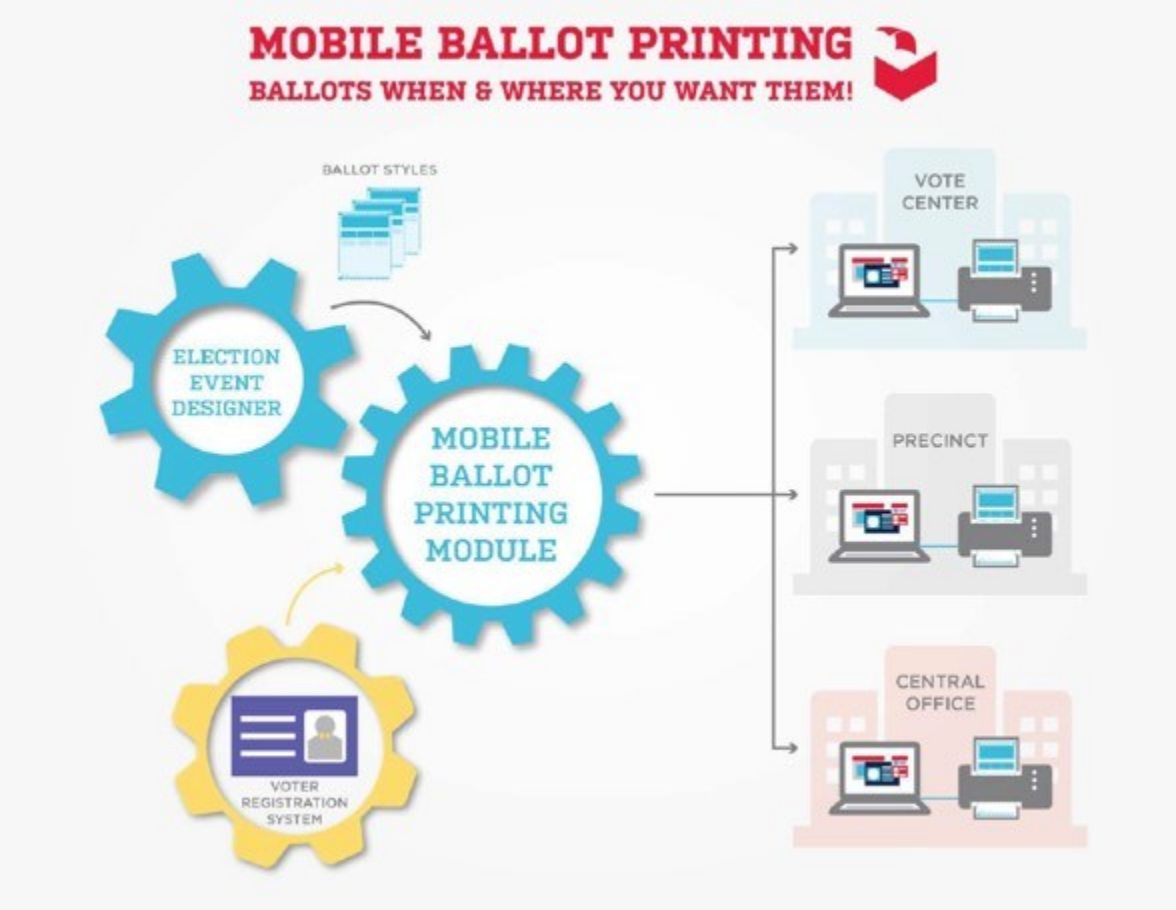

Exhibit 1. Dominion Voting Systems Mobile Ballot Printing. The vendor's own diagram shows the Voter Registration System as a direct input to the Mobile Ballot Printing Module, alongside ballot styles from Election Event Designer, with laptop-and-printer output stations at a Vote Center, a Precinct, and a Central Office.

The vendor's own architecture diagram shows two inputs to the Mobile Ballot Printing Module:

1. **Election Event Designer**, supplying ballot styles
2. **Voter Registration System**

and three destinations, each a laptop paired with a printer:

3. **Vote Center**
4. **Precinct**
5. **Central Office**

Every element of the ballot-ordering concern is in that diagram, drawn by the vendor. Ballots are not pre-printed, counted, and controlled as physical inventory; they are **generated on demand from a software definition**. The voter registration database — the system Area A establishes is joined to the tabulation chain by state requirement — is a **direct input** to ballot production. And production is possible at a **central office**, not only at a polling location under the observation of poll workers and challengers from both parties.

The security consequence is a change in the nature of the control. A pre-printed ballot is an accountable physical object: a known quantity, delivered under seal, reconciled against ballots issued, spoiled and returned. A print-on-demand ballot is an output of software. The control that prevents excess ballots is no longer a locked room and a count — it is a software authorization check.

CISA has confirmed that this specific check can be defeated. CVE-2022-1747: the mechanism used to activate a voting session "is susceptible to forgery. An attacker could leverage this vulnerability to **print an arbitrary number of ballots without authorization**" (CISA).

That is the federal cybersecurity agency stating that a certified ballot-production device can be made to produce unlimited unauthorized ballots. The vendor's slogan and the CVE describe the same capability, from opposite ends.

Ballot-on-demand printing is outside the scope of EAC certification entirely. It is not a certified component of the voting system. ES&S lists among its ballot-on-demand key features "integration with your voter registration system" (ES&S Michigan bid) — a vendor claim of exactly the registration-to-ballot-production coupling that Dominion's diagram depicts, in a product category no federal body certifies.

A contemporaneous record of the ballot-ordering calculation

The clearest documentary evidence that this architecture has operational value to a party seeking to control an election outcome is not a technical paper. It is an email and a set of findings from Green Bay, Wisconsin, in 2020.

The information request. The Wisconsin Office of Special Counsel found that Michael Spitzer-Rubenstein, an outside private party serving as an "on-site contact" at the Green Bay central count facility, instructed staff to "**pull the numbers on the absentee ballots returned and outstanding per ward**" — and the report states the purpose in his own framing: **"so he could determine which wards were on which voting machines"** (Exhibit 5, OSC Second Interim Report, p. 69, finding 5).

Consider precisely what that request obtains. Absentee ballots **returned** per ward is how many votes are already in hand. Absentee ballots **outstanding** per ward is how many more could still arrive. Which wards are on which machines is where each ward's ballots will be processed. Together, those three data points are the complete input set for the question: *how many additional ballots of which style would be required, and at which machine, to reach a target.* This is the ballot-ordering calculation, requested in writing, by an outside party, at a central count facility, days before an election.

The network. At the same facility, the same party arranged the wireless infrastructure. A PSAV event-technology director wrote on October 27, 2020, at Spitzer-Rubenstein's instruction:

> "One SSID will be hidden and it's: **2020vote** There will be **no password** or splash page for this one and it should only be used for **the sensitive machines that need to be connected to the internet**."

Two other networks were configured: `gbvote` for poll workers, and `Hyatt_Meeting` with the password `Hyatt123` for media (Exhibit 3, OSC Second Interim Report App. p. 65).

Exhibit 3. The wireless configuration email as produced in the record: Michael Spitzer-Rubenstein (michael@voteathome.org) forwarding, on October 30, 2020, a message sent October 27, 2020 at 5:11 PM by Trent Jameson, Director of Event Technology at PSAV, covering the Hyatt Regency and KI Convention Center. The highlighted passage is the hidden, password-free `2020vote` network designated for "the sensitive machines that need to be connected to the internet." Highlighting appears in the produced document.

A hidden, entirely unauthenticated wireless network, created specifically for "the sensitive machines that need to be connected to the internet," at a central ballot counting facility, on election night. The OSC further found that Spitzer-Rubenstein "ensured that 'both networks reach[ed] [his] hotel room on the 8th floor'" (Exhibit 4, p. 69).

The control over ballots. The OSC found he had "unfettered access to the Central Count, ballots, and ballot counting," developed the central count diagram and staff procedures, assigned inspectors, "pushed for control of ballot curing process," and "put himself in charge of transporting ballots to City Hall and then to Central Count on election day; and then counting them." Its finding: **"On election day, Spitzer Rubenstein had access to ballots and determined which ones would be counted or not counted."** Forty-seven boxes of ballots arrived, some after the 8 p.m. statutory deadline, and were counted; his contemporaneous text to the City Attorney at 9:29 p.m. read "I don't think anyone challenged the ballots when they came in" (Exhibits 4 and 6, pp. 69–70).

Provenance, stated plainly. The Gableman Office of Special Counsel was a partisan-commissioned body; the Wisconsin Assembly terminated it, and it was the subject of sanctions litigation. **Its conclusions are not treated as authoritative here.** But the documents it reproduces — the PSAV email of October 27, 2020, and the 9:29 p.m. text message — are contemporaneous business records that exist independently of the report's credibility. Those documents are what is cited.

What they establish, and what they do not. They do not establish that ballots were fabricated in Green Bay; no such finding was made and none is asserted here. They establish something more useful for federal policy: **that an outside private party at an American central count facility in 2020 sought precisely the data set required to perform a ballot-allocation calculation, arranged an unauthenticated internet path to the counting machines, and exercised control over which ballots were counted — all in the same building, on the same night, documented in writing.** The mechanism in the vendor's own marketing diagram is not hypothetical. Someone assembled its inputs.

Michigan 2024: 125,428 excess records, and a state that never showed its math

In October 2024 the Michigan Secretary of State's published `DailyBallotsCast` report contained duplicate voter-identifier lines. The figure that entered public circulation — **125,428** — has been characterized by the state and by fact-checking organizations as an artifact of a formatting defect. **This memorandum does not assert that 125,428 illegal ballots were cast.** What it asserts is narrower, verifiable, and considerably more troubling as a matter of federal policy: **the arithmetic is reproducible from records captured by citizen observers, the state's competing production does not agree with those records, the state is the common source of both, and the state has never published the query, script, or reconciliation that would show how the figure arose.**

The reproducible arithmetic. The statewide daily-ballots-cast records captured by citizen watchdogs during the 2024 general election, in the state's own export format, were examined directly in the preparation of this memorandum (analysis file supplied as Exhibit 15; the underlying capture is in the possession of the submitting party and is available on request, being too large to append). The file contains:

MEASURE	VALUE
DATA ROWS	**208,075**
DISTINCT VOTER IDENTIFIERS	**82,647**
EXCESS RECORDS OVER DISTINCT VOTERS	**125,428**
ELECTION DATE ON EVERY ROW	2024-11-05
RANGE OF VOTE_RECORDED_DATE VALUES	2024-09-23 to 2024-10-28

The excess is exactly 125,428. That is the arithmetic provenance of the circulating figure: it is not an invention, and it is not an estimate. It is 208,075 minus 82,647, computed from the records themselves.

The distribution of records per voter identifier:

RECORDS FOR A SINGLE VOTER ID	VOTER IDS
2	54,386
3	18,675
4	6,378
5	2,141
6	684
7	231
8	93
9	37
10	10
11	6
12	2
14	2
16	1
29	**1**

The largest group is a single voter identifier carrying **29 records**, all bearing the same `vote_recorded_date` of October 25, 2024, across numerous distinct Detroit addresses — including one address that appears twice.

What the analysis supports for the state's explanation. Two findings are consistent with the state's account of an export defect rather than duplicate voting, and they are reported first because the standard requires it. **Only two voter identifiers in the entire file carry more than one distinct `vote_recorded_date`**; the remaining 82,314 show a single date with differing absentee-voter addresses, which is the signature of an address-history join rather than multiple ballots. And **77,712 voter identifiers have exactly as many records as they have distinct addresses** — again consistent with a one-row-per-historical-address fan-out.

What the analysis does not support, and what the state has never addressed.

FINDING	COUNT
ROWS WHERE THE ABSENTEE-REPORT JURISDICTION DIFFERS FROM THE QVF JURISDICTION	**100,430**

ROWS WHERE THE ABSENTEE-REPORT COUNTY DIFFERS FROM THE QVF COUNTY	**52,241**
VOTER IDS WITH DIFFERING AV_REPORT_JURISDICTION_NAME VALUES ACROSS THEIR ROWS	**70,781**
VOTER IDS WITH MORE RECORDS THAN DISTINCT ADDRESSES	**4,935**
VOTER IDS CONTAINING BYTE-IDENTICAL DUPLICATE ROWS	**4,554**, comprising **5,258 identical rows**

That last row is the one an address-history join cannot produce. A join that emits one row per historical address produces rows that differ in the address field. It does not produce **5,258 byte-for-byte identical rows across 4,554 voters.** Something other than a clean address fan-out generated part of this file, and the state has never said what.

The excess records are concentrated in the jurisdictions where a presidential margin would be decided:

COUNTY	EXCESS RECORDS
WAYNE	21,910
OAKLAND	15,571
MACOMB	10,930
KENT	10,549
GENESEE	5,855
WASHTENAW	4,751
LIVINGSTON	4,100
INGHAM	3,850

The state's position, and its evidentiary status. The Department attributed the anomaly to a formatting error in a data export, stated that "the Qualified Voter File only allows one ballot to be accepted per voter in every election – a formatting error has been corrected," and that "each of these voters only had one vote recorded for this election" (quoted by PolitiFact; AFP Fact Check). AFP filed its own records request and reported that "the document shows no duplicate votes."

Here is the difficulty with that corroboration, and it is a serious one. The records-request response and the citizen capture are **two productions of the same underlying report by the same custodian, and they do not agree.** One shows 125,428 excess records; the other, per the requester's account of it, shows none. **The state is the common source of both.** A records-request response produced after the anomaly became public, by the agency whose report contained the anomaly, is not an independent check on that agency's report — it is the agency's second account of its own records. Under the standard applied throughout this memorandum, that is a claim requiring documentary support, not corroboration in itself. **The possibility that the records-request response reflected a corrected, regenerated, or otherwise**

altered extract rather than the file as it stood in October 2024 cannot be excluded on the available record, and cannot be confirmed either. The submitting party's position is that the citizen capture is the contemporaneous artifact; that position and the state's cannot both be right, and no independent party has been permitted to reconcile them.

And the reconciliation was never produced. The script or process that generated the duplicate lines was not produced. A public-records request seeking the material needed to replicate the error was denied, the denial was appealed, and the appeal was denied; a related communications request drew a fee estimate of $5,313.66 (requester's account, letsfixstuff.org). No denial letters or fee estimates have been published, and no litigation was located, so the procedural history rests on the requester's own narrative and is recorded here as such. Michigan's Election Fact Center page no longer carries the 2024 statement; the state's words survive through third-party quotation.

The finding. The Secretary of State never showed her math. The state asserted a mechanism, asserted a correction, declined to produce either, and denied the request that sought them. The arithmetic that produced 125,428 is reproducible from the contemporaneous records; the explanation for it is not verifiable by anyone. Under the standard applied here the matter is **unresolved**, and the reason it is unresolved is that the party with exclusive custody of the evidence declined to produce it.

That pattern — not the number — is the finding that matters for federal policy. In the ballot-ordering context, its significance is specific: the public report of who has voted and who has not, in the state where absentee ballot volume is largest, contained more than 125,000 records that the state has never accounted for, in a file whose purpose is to report the running state of the count. If Area A establishes that the running state of the count is the intelligence an adversary needs, Area B establishes that the public artifact reporting it could not be reconciled and was never explained.

Why the paper record cannot resolve the dispute

The standard answer to every concern in this Area is: the paper ballot is the record; look at the ballots. Georgia's Secretary of State general counsel stated the principle directly: "The paper ballot is the record of the vote" (Georgia Recorder).

The principle is correct. Its application to these systems fails for three documented reasons.

First, on ballot-marking devices, the tabulated portion of the ballot is not the human-readable portion. The tabulator reads a barcode or QR code. The voter can read only the text. CISA's advisory identifies this as the specific risk requiring audit: jurisdictions must audit "the human-readable portions

of physical ballots and paper records… especially crucial to detect attacks where the listed vulnerabilities are exploited such that **a barcode is manipulated to be tabulated inconsistently with the human-readable portion of the paper ballot**" (CISA). MITRE described the QR code as "a non-authoritative portion of a Georgia ballot" (MITRE) — which is precisely the problem: the non-authoritative portion is the portion that is counted. CISA notes that the device "provides the configuration option to produce ballots that do not print barcodes for tabulation," meaning the defect is a configuration choice states have made, not a technical necessity.

Second, where a print-on-demand ballot is produced by the system itself, examining the ballot cannot detect it. A ballot printed by an authorized device with a valid style is indistinguishable from a legitimate ballot by inspection. The only control is the count of ballots issued against ballots cast — and where ballots are generated on demand, that count is itself a software output.

Third, the paper record's integrity depends on custody, and custody has failed on the record. In Fulton County, Georgia, state investigators reported **3,075 duplicate ballot images**, and said they "were unable to determine how many of the 3,075 duplicate images represented ballots that were included in the results used to certify the 2020 election." The State Election Board reprimanded the county 2–1 and imposed an independent monitor; one board member dissented, stating "with over 140 violations of election laws and rules, it would be a travesty not to refer this to the Attorney General" (Georgia Recorder). The associated consent order identified 36 discrepancies in batch tally sheets, attributed them to human error rather than intentional misconduct, and concluded they did not affect the outcome (AP).

Both halves of that record deserve weight. The state's position — that the results survived three separate counts — is documented. So is the fact that investigators could not determine whether 3,075 duplicate ballot images entered the certified result. **"We counted it three times and got the same answer" and "we cannot determine what was in the count" are both true statements about Fulton County, and the second one is the one that matters for whether the paper record can settle a dispute.**

The Antrim County record, treated in Area C, makes the same point with four different totals for the same ballots.

4.3 Area C — Direct Manipulation of Vote Tallies

What is established about capability

Malicious code can be installed in one minute and can conceal itself completely. Feldman, Halderman and Felten, on the Diebold AccuVote-TS: "an attacker who gets physical access to a machine or

its removable memory card for as little as one minute could install malicious code"; such code "could steal votes undetectably, **modifying all records, logs, and counters** to be consistent with the fraudulent vote count it creates"; and it could spread "automatically and silently from machine to machine during normal election activities — a voting-machine virus." They built working demonstrations (Princeton CITP).

Malicious code can propagate from the central system to every device in a jurisdiction. "The most critical problem we found is an arbitrary-code-execution vulnerability that can be exploited to spread malware from a county's central election management system (EMS) to every BMD in the jurisdiction," via "a classic 'Zip Slip' vulnerability… coupled with a badly designed system-level service that facilitates privilege escalation" (City and County of San Francisco memorandum summarizing the Halderman report). CISA independently confirmed this as **CVE-2022-1743**.

The audit log cannot be trusted to report tampering. CISA, **CVE-2022-1740**: the "on-screen application hash display feature, audit log export, and application export functionality rely on **self-attestation mechanisms**. An attacker could leverage this vulnerability to disguise malicious applications on a device" (CISA).

These three findings, together, are the entire argument of this Area. A system in which code can be installed in a minute, propagate to every device from a single point, and defeat the mechanism that would report it, is a system whose output cannot be verified from its own records. That conclusion is established by the same academic and federal sources whose authority is invoked to dismiss manipulation claims. It does not depend on any contested finding.

And it is a county-level and precinct-level exposure, not a national one. The propagation path CISA confirmed runs from a county election management system to the devices in that county. As the materiality analysis in the Standard of Proof section establishes, that is the level at which a national outcome is decided. An adversary does not need fifty states. It needs the election management system of a small number of large counties.

What nobody has proven, in either direction

This is the point at which most documents on this subject overstate, and this one will not.

Neither of the two most-cited technical accounts of direct manipulation in an actual American election has been proven to have occurred. Both remain theories with reasonable competing explanations, and this memorandum treats them identically.

The Halderman account. J. Alex Halderman's examination of Georgia's Dominion ImageCast X, later published under academic peer review (USENIX Security 2022), and his court-ordered examination of the Antrim County system, are rigorous work. What they establish is **capability**: that specific exploits are feasible against certified equipment. Halderman himself has been explicit that he has **not** concluded that any American election result was altered by exploitation of those vulnerabilities. CISA's advisory records the same limitation: **"CISA has no evidence that these vulnerabilities have been exploited in any elections."** So: the vulnerabilities are demonstrated; the exploitation is not. Anyone citing Halderman for the proposition that votes were changed is citing him for something he did not find.

The Lenberg account, assessed on identical terms. Jeffrey Lenberg — retired Distinguished Member of the Technical Staff at Sandia National Laboratories, BS 1978 and MS 1980 in Electrical Engineering from the University of New Mexico, more than 31 years at Sandia, and previously an assistant to the FBI in a data analysis of potential election fraud in the 1994 Maryland gubernatorial election (motion filed September 30, 2024) — asserted in a report declared under penalty of perjury on May 9, 2021 that the Antrim County Dominion election management system "has been found to be subverted," with "numerous error conditions that are identified by the tabulator [that] are ignored by the EMS/RTR," which he asserted was "designed to mute such error reporting" (report). A May 15 report described a "logical bumper": "One of the specific subversions to the error handling in the EMS/RTR noted was the use of logical 'bumpers' that prevented the shifting of votes from one contest to another."

What supports it: the underlying phenomenon — an EMS reporting layer that suppresses or mishandles error conditions raised by the tabulator — is **exactly the failure mode Michigan's own Antrim finding confirms.** The state established that the tabulators counted correctly and that the reporting layer published a wrong county winner, four separate times. Whatever the correct mechanism, the general shape of the claim is consistent with the state's own conclusion, and that deserves to be said. His credentials are serious, and dismissing them by association rather than by analysis is not a rebuttal.

What it lacks: the "logical bumper" mechanism **has never been validated by any court, audit, or independent forensic body.** His own reports describe findings as preliminary and "consistent with" subversion rather than as proof and acknowledge that he did not obtain the source-code review his conclusions would require. The widely circulated May 3, 2021 demonstration was **not performed on in-situ certified live election equipment**: sworn testimony in the *Curling* record states the election management software in the video came from Antrim County, Michigan, not the Georgia county where the video was made, and the tabulator was supplied by third parties.

The symmetry is the point. One examiner demonstrated exploits in a laboratory and did not claim they were used. Another asserted subversion in a live system and could not validate the mechanism. **Neither established that any vote total in any American election was directly manipulated. Both had reasonable competing explanations available — laboratory conditions in the first case, documented reporting-layer defects and known error-handling behavior in the second.** Nothing in this memorandum's conclusion rests on either account, and no reader should take from this document the claim that direct manipulation of a tally has been proven.

Why it cannot be disproven either — and why that is the finding

Here the standard cuts hard against the assurance side, and it is the most important thing in this Area.

The identical evidentiary vacuum that prevents proof of manipulation prevents disproof of it. The claim "no votes were changed" requires the same class of evidence as the claim "votes were changed": a trustworthy record of what the system did. The mechanisms that would supply it are the ones CISA has documented as defeatable — the self-attesting hash display, the exportable audit log, the application export. A log that the potentially compromised software writes about itself is not evidence about that software. **This is not a rhetorical point; it is CVE-2022-1740.**

And the standard reply — "just look at the ballots" — presupposes a chain of custody that the record does not establish. Examining ballots resolves a dispute only if the ballots examined are, provably, all of the ballots cast and only the ballots cast, in the condition in which they were cast. That premise fails on the documented record in multiple jurisdictions:

- **Antrim County, Michigan** produced **four different ballot totals for the same election**, treated in detail below.
- **Fulton County, Georgia** produced **3,075 duplicate ballot images**, and state investigators stated they "were unable to determine how many of the 3,075 duplicate images represented ballots that were included in the results used to certify the 2020 election" (Georgia Recorder).
- **Coffee County, Georgia** ballots were scanned repeatedly by unauthorized parties over multiple days, documented below.
- **Print-on-demand production**, established in Area B, means a system-produced ballot is indistinguishable by inspection from a legitimate one, and the count of ballots issued is itself a software output.

So the honest state of the record is this: direct manipulation of vote tallies in an American election can be neither proven nor disproven, and the reason is the design of the system. The instrumentation that would settle the question does not exist, the logging that does exist is defeatable by the software it monitors, and the paper fallback depends on custody controls that have failed in documented cases. **Under the burden of proof stated at the outset — that those asserting an election is secure must produce the evidence — an unfalsifiable assurance is not an assurance. It is a request for trust.** No other component of national critical infrastructure is operated on that basis.

Antrim County: four counts of the same ballots

Antrim County, Michigan, is the single most instructive record in this document, and the reason is arithmetic rather than argument. **The same election, in a county of roughly 16,000 voters, produced four different presidential vote totals across four separate counts.**

The figures, as recited in the oral decision of the Honorable Kevin A. Elsenheimer, 13th Circuit Court, and in the state's own announcement (transcript supplied as Exhibit 16):

COUNT	DATE	PRESIDENTIAL VOTES COUNTED	TOTAL BALLOTS CAST (AS THEN REPORTED)	REPORTED RESULT
1. INITIAL PUBLISHED	Nov. 3–4, 2020	**12,423**	16,047	Biden 7,769 / Trump 4,809 / 145 third-party / 11 write-in
2. FIRST CORRECTION	Nov. 5, 2020	**17,327**	18,059	Biden 7,289 / Trump 9,783
3. PRE-CERTIFICATION REVISION	Nov. 21, 2020	**15,949**	16,044	Biden 5,960 / Trump 9,748
4. FULL HAND TALLY	Dec. 17, 2020	**15,718**	—	Trump 9,759 / Biden 5,959

The fourth figure is the state's own (Michigan Secretary of State), which characterized the hand tally as "a zero-limit risk-limiting audit" confirming the certified outcome "to absolute certainty," with a net difference of "only 12 votes out of 15,718."

Read the second column down. 12,423, then 17,327, then 15,949, then 15,718. The number of presidential votes counted moved by **4,904 upward, then 1,378 downward, then 231 downward.** The reported number of total ballots cast moved from 16,047 to 18,059 and back to 16,044 — a swing of **2,012 ballots** in the denominator, in a county where roughly 16,000 people voted.

The state's position, credited in full. The tabulators counted correctly; the initial published figures reflected an error in how results were configured and reported, not in how ballots were read; and the final hand tally confirmed the certified outcome within twelve votes. That position is documented, it was reached by counting every ballot by hand, and this report does not dispute it.

What the state's position does not explain is the denominator. A reporting or configuration error explains why *votes* were mis-tallied. It does not explain why the **count of ballots cast** was reported as 16,047, then 18,059, then 16,044. Nor does the record establish, for any of the four counts, a documented custody chain demonstrating that the ballot set counted on December 17 was identical to the ballot set that produced the 16,047 figure on November 4. **On the available record that identity is assumed, not proven** — and where a county has already demonstrated that it cannot state consistently how many ballots it holds, the assumption is doing heavy work. The submitting party's position is that four differing counts of a single ballot set are consistent with the absence of effective chain-of-custody control, and raise the possibility of ballot-set substitution producing closer adherence to reported figures. **No evidence in the record establishes that a substitution occurred, and none is asserted here.** What is asserted, and is established, is that **the record contains no custody documentation capable of excluding it** — which is the same finding, in a different form, as the one above: the system cannot answer the question put to it.

What the judge actually said

Bailey v. County of Antrim is routinely cited as judicial rejection of the Antrim technical claims. The transcript does not support that characterization, and the judge went out of his way to say so.

Judge Elsenheimer, dismissing the case, stated on the record:

> "**By deciding this motion, the Court is not saying that there were no problems in the way that Antrim County conducted its November 2020 elections.** The Clerk has admitted that there were challenges and problems in the elections."

And, directly on the technical question:

> "**Nor am I saying that the processing of election data here wasn't corrupted or corruptible. I don't have the facts to make that determination.**"

He identified the policy question and pointed it at the federal level:

> "The plaintiff's reports and the news of the day, including a computer hack recently of a main petrol fuel pipeline on the East Coast might well suggest that **this is something that policy**

> **makers should be looking into in the future. If election results were to be held for ransom in the future, one can only imagine what would happen.**"

And he framed the whole matter in terms that anticipate this report's recommendation:

> "At its core, this case has involved, from the beginning, something that we all learned to do in kindergarten, and that is count… **We've, over time, and perhaps with good reason, in the conduct of our elections, taken this very simple function and made it into a complex and often computerized exercise.**"

(All quotations: oral decision transcript, 13th Circuit Court, Antrim County, supplied as Exhibit 16.)

The ground of dismissal was stated plainly: "as pled, the plaintiff's request for an audit is not available." **That is a pleading holding, not a technical finding**, and the judge said as much in the sentences quoted above.

One further admission appears in the same proceeding and matters independently. At oral argument, counsel for the Secretary of State **acknowledged that the December 15/17 hand recount was not an audit conducted pursuant to MCL 168.31a(2)** — the statutory audit provision. The state's most-cited answer to Antrim is therefore an exercise the state itself declined to characterize, in court, as the statutory audit.

The appellate history confirms the procedural character of the disposition, and contains a holding adverse to the state. The Michigan Court of Appeals, in a published opinion of April 21, 2022, reviewed dismissal under MCR 2.116(C)(4) and (C)(8) and on mootness. It held that **the mootness determination was error** — "it is undisputed that plaintiff did not receive all the relief requested" — but affirmed on the alternative ground that the plaintiff was not entitled to the relief sought, holding that the constitutional audit right "does not permit an audit to be performed in the manner dictated by an individual voter." It **made no findings on the technical merits** (Michigan Court of Appeals No. 357838). The Michigan Supreme Court denied leave.

The correct summary of the case law generally is therefore not "courts rejected these claims." *Lake v. Hobbs*, also cited as judicial rejection, reached trial on **only 2 of 10 claims** (ruling). And *Curling v. Raffensperger*, the most technically searching of the election-systems cases, went the other way on the central question: **summary judgment was denied to the State Defendants on the ballot-marking-device claims**, because "material factual disputes required a bench trial." The court recorded plaintiffs' experts' opinion that the copying and distribution of Georgia's voting system software "materially

increased the risk that a future Georgia election would be attacked **because all 159 Georgia counties used the same voting system**" (order of November 10, 2023). Of the **64 post-2020 lawsuits** catalogued in Exhibit 14, 20 (31%) were dismissed on procedure or standing, 14 (22%) were voluntarily withdrawn, and only **three** — *Ward v. Jackson*, *Favorito v. Cooney* and *Bailey v. Antrim* — involved any discovery. **The technical merits have largely not been adjudicated, in either direction.**

Defects that were caught, reported because a document that reports only adverse findings cannot be trusted

Two cases are cited in both directions and both belong in the record honestly.

Williamson County, Tennessee. An EAC investigation into Dominion Democracy Suite 5.5-B confirmed a real software defect affecting result reporting, correctly identified and remediated through the federal process (EAC report). It is properly cited as evidence that certified systems ship with defects that alter reported results, and equally properly cited as evidence that the federal investigation process functions. Both are true.

Maricopa County, 2022. "A substantial number of ballot-on-demand (BOD) printers at vote centers… produced ballots that could not be tabulated" (Maricopa County report). An independent investigation led by a former Arizona Supreme Court Chief Justice found the cause was ballots too long and paper too heavy for the printers (Arizona Mirror). This is **not** evidence of tabulation fraud and is not offered as such. It is evidence of the reliability cost of print-on-demand ballot production at scale, in the largest jurisdiction using it, on election day.

4.4 Area D — Interoperability and Artificial Intelligence

The certification regime makes patching a decertifying act

The most consequential fact in this memorandum is not any individual vulnerability. It is the mechanism that keeps vulnerabilities in the field.

Maricopa County, responding to a claim that its systems had not been patched since August 2019, did not deny it. It explained it:

> "If the County were to implement a software or security update without it being tested and approved by the EAC, the County's tabulation equipment would lose its federal and state certification."

(Maricopa County response)

That is a jurisdiction stating on the record that **applying a security patch would strip its equipment of legal authorization to be used.** It is not an excuse; it is an accurate description of the regime. The consequence is that every certified system in the United States is frozen at the security posture of its certification date until a full recertification cycle completes.

The timeline for the nine CISA vulnerabilities demonstrates the cycle's length. The advisory issued June 3, 2022. Dominion produced Democracy Suite 5.17. "The patched software entered federal certification testing in October 2022 and was certified by the U.S. Election Assistance Commission on **March 16, 2023**." Georgia then announced it would not install the patch until after the 2024 presidential election. Halderman's assessment of that announcement: "Announcing this is worse than doing nothing at all, since it puts would-be adversaries on notice… giving them nearly 18 months to prepare and deploy attacks" (SF memo).

Nine publicly documented vulnerabilities, in a system designated critical infrastructure, remained deployed through a presidential election **by announced policy**, more than two years after federal disclosure. No adversary had to defeat a control to achieve that. The regime produced it.

Against that structural fact, CISA's own data — a **108-day median remediation time for critical vulnerabilities with known public exploits** — reads not as institutional laziness but as the arithmetic consequence of a certification regime that penalizes patching.

The national security consequence. The United States operates its election infrastructure under a rule that converts every disclosed vulnerability into a **published, dated, guaranteed-open window.** An adversary reading the CISA advisory of June 3, 2022 learned not only what the vulnerabilities were but that they would remain exploitable through the next presidential election. No other critical infrastructure sector operates under a regime that legally penalizes patching.

One mandated chain, three uncertified links

Interoperability is not an emergent property of these systems. In Michigan it is a **contract requirement**, as Area A establishes: registration data flows into the election management system, ballot definitions flow into election-night reporting using the registration file structure, and results flow out in a state-mandated format. The same pattern — a required, format-level chain joining registration, tabulation and reporting — recurs wherever a state has standardized its data formats.

The security consequence of a mandated chain is that its weakest link governs. And the weakest link is not certified.

There is no federal standard governing the layer the public watches. The EAC, on election-night reporting software:

> **"There are no federal standards governing the design, security, and setup of this critical aspect of the electoral process."**

(EAC)

Tabulators are certified. The election management system is certified. **The layer that transmits results to the public, and through which the entire country forms its understanding of the outcome, is subject to no design standard, no security requirement, and no setup requirement at the federal level.** Ballot-on-demand printing, as Area B establishes, is likewise outside certification. Electronic pollbooks are outside the voting system as VVSG defines it. **The certified core is surrounded on three sides by uncertified components that are required to interoperate with it.**

The unofficial feed and the official canvass come from the same machine

The standard dismissal of any anomaly in election-night reporting is that those were only unofficial numbers, separate from the official canvass. **As a matter of system architecture, that is not accurate.**

Dominion's *Results Tally & Reporting User Guide 5.17*, hosted by the Colorado Secretary of State, lists among the core functions of the election management system: **"Publishing the unofficial Election Results for further processing or reporting (i.e. by news and media feeds),"** and describes pushing XML output to configurable network "transfer points" (Colorado Secretary of State). ES&S states that modem transmission of unofficial results exists because "these early, unofficial results help the news media report results quickly on election night" (ES&S).

The official count and the media feed are **two outputs of one certified machine.** They diverge only in what happens downstream. An observer watching the unofficial feed is watching the certified system's own output, carried by an uncertified, unlogged, unaudited transport layer — which means that a defect or intrusion at the source appears in both, and a defect in transport is indistinguishable from a defect at the source by anyone outside the county office.

And this architecture is not an American afterthought. As Area A establishes, the Smartmatic–Sequoia product glossary defines **HAAT** as a precinct-level accumulator whose documented function includes

"transmission of unofficial results from all precinct voting devices." The unofficial reporting channel is in the product definition of the Venezuelan-shareholding product line from which the current American fleet's lineage descends.

Uniformity converts a local exploit into a national one

The *Curling* court recorded plaintiffs' experts' opinion that distribution of Georgia's voting system software "materially increased the risk that a future Georgia election would be attacked **because all 159 Georgia counties used the same voting system**" (order of November 10, 2023).

That is the interoperability risk in one sentence. Standardization is procured for good reasons — training, cost, comparability of results. Its security consequence is that **a single working exploit scales to every jurisdiction running the same build.** Combine that with the propagation path CISA confirmed in CVE-2022-1743 — malware spreading from a county election management system to every device in the jurisdiction — and with the patch freeze above, and the exposure is not "a vulnerability in a machine." It is a vulnerability in a fleet, held open by regulation.

Georgia's own procurement illustrates the scale: a **$107 million** contract for more than 30,000 ballot-marking devices and 3,500 scanners across all **159 counties**, on a ten-year term (StateScoop).

Artificial intelligence changes the economics of every finding above

No claim is made here that artificial intelligence has been used to manipulate an American election, and no evidence of that was located. The relevant point is different and is a matter of cost.

Every attack path documented in this memorandum has historically been rate-limited by scarce human expertise: someone had to read the code, find the path traversal, craft the election definition file, forge the smartcard protocol, or identify which county's margin was worth attacking. **Automated code analysis and code generation compress each of those tasks.** The specific compounding factors on this record are:

- **A published file manifest.** NIST's reference data set supplies file names, sizes and expected hash values for a certified build (Area A) — a structured, machine-readable starting point for automated analysis of exactly the kind that current tooling consumes most readily.
- **A frozen target.** The patch regime guarantees that a vulnerability found today remains present for a recertification cycle, often through the next federal election. Automated discovery is most valuable against targets that cannot move, and this target is legally prohibited from moving.

- **A uniform fleet.** One exploit, 159 counties.
- **A documented data chain.** Mandated interoperability means an entry point in the least-protected component — a pollbook, a ballot-on-demand station, a reporting feed — has a documented, format-level path toward the components that matter.
- **A quantified target list.** As the materiality analysis shows, the number of counties whose compromise would decide a national election is small, and their identities are public.

The national security consequence. Automated tooling does not create a new vulnerability class here. It collapses the cost of exploiting the existing one, at exactly the moment when federal defensive capacity is being reduced — CISA's fiscal 2026 budget justification proposes eliminating its election security base of **14 full-time positions and $39.61 million**, removing Election Security Advisors from all ten regions, and states that "the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) will be discontinued" (CISA FY2026 congressional budget justification). **The defensive posture is contracting while the offensive cost curve falls.**

Area E — No Evidence Capable of Confirming or Refuting a Result

This is the area that subsumes the other four. Each of the preceding areas describes an exposure. This one describes why none of them can be resolved — and therefore why the appropriate response is architectural rather than remedial.

Direct analysis of the archived 2020 national feed

The archived feed supplied as Exhibit 11 is an 11-megabyte JSON capture of the New York Times 2020 presidential results, `meta.version` 25064, captured **2021-01-06T01:19:29.800Z** — two months after election day and after every state had certified. It contains 51 races, 3,159 county reporting units, and **11,063 timestamped observations** of cumulative vote totals.

Its declared provenance is machine-readable and unambiguous: `county_data_source` = **edison** for all 51 races; `eevp_source` = **edison** for all 51 races and all 3,159 county units.

Two methodological corrections were applied and must be stated, because analyses that omit them produce false results. First, **the stored observation arrays are not in chronological order in any of the 51 races** — there are 110 out-of-order adjacent pairs — so every figure below was computed after sorting by timestamp. Second, **the feed does not store per-candidate vote counts.** It stores one integer total per race and candidate shares rounded to three decimals, so any per-candidate figure is a

reconstruction carrying up to ±0.0005 × total of quantization error. **Every finding below rests on the race-level integer total, which requires no such adjustment.**

Finding 1 — a nationwide reset discarding 134,998,591 votes. Sorted chronologically, the feed contains 56 events in which a race's cumulative total fell to exactly zero from a nonzero value. Fifty of them discarded more than 100,000 already-reported votes. Those fifty span **50 of the 51 races** and total **134,998,591 votes**. All fifty occur within a four-hour window on November 4, 2020, from 05:58:59Z to 10:02:44Z — **twenty-two of them inside the single clock hour beginning 10:00Z.**

RACE	VOTES ZEROED	PERCENT REPORTED, BEFORE → AFTER
CALIFORNIA	11,752,178	72 → 0
TEXAS	11,134,336	95 → 0
FLORIDA	11,031,440	96 → 0
NEW YORK	7,082,194	60 → 0
OHIO	5,701,651	94 → 0
NORTH CAROLINA	5,457,368	95 → 0
PENNSYLVANIA	5,323,770	76 → 0
GEORGIA	4,719,993	95 → 0
ILLINOIS	4,495,802	79 → 0
MICHIGAN	4,365,423	89 → 0

The honest interpretation, stated before anyone else states it. Fifty states resetting within four hours is not consistent with votes being deleted in fifty separate jurisdictions. It is consistent with a **feed-wide reset and re-baseline** — the reporting layer discarding its accumulated state and starting over. That is the most probable explanation and it is the one adopted here.

The finding survives that interpretation intact. The claim is not that votes were deleted. The claim is that **the layer of the pipeline the entire country watched discarded 135 million cumulative votes and re-baselined from zero, across fifty states, inside four hours — with no public log, no published explanation, no audit trail, and no requirement that any of the three exist.** Whether that reset was routine or hostile cannot be determined from outside, by anyone, ever. That is the finding, and it is a structural one that requires no allegation about intent.

Finding 2 — 416 decrements remain after every reset is excluded, and in three decisive states they equal or exceed the margin. Removing all 56 resets, the feed still contains **416 events in which a race's cumulative integer total fell**, across 45 races. The largest is **Pennsylvania, −586,189 votes**, at 02:22:45Z on November 4, with the reported percentage unchanged at 19. The median is 184. **Three**

hundred thirty of the 416 occurred at 99% or more reported — after the feed itself said counting was essentially complete — across 42 races.

STATE	DECREMENT EVENTS	VOTES DECREMENTED	CERTIFIED MARGIN	RATIO
PENNSYLVANIA	17	988,616	80,555	**12.3×**
GEORGIA	38	43,715	11,779	**3.7×**
WISCONSIN	18	20,581	20,682	**1.0×**
MICHIGAN	23	42,307	154,188	0.27×
ARIZONA	2	2,583	10,457	0.25×
NEVADA	0	0	33,596	—

In three of the six states that decided the 2020 presidential election, **the volume of unexplained downward revision in the feed that reported the result equals or exceeds the certified margin of victory.** In Wisconsin the two figures differ by 101 votes — the decremented volume falls just short of the margin, and is therefore reported as approximately equal rather than exceeding it.

This does not establish that any outcome was wrong, and it is not offered for that purpose. It establishes that **the reporting layer's own churn is larger than the quantity in dispute** — which means the reporting layer cannot be used to confirm the outcome either. A measurement whose noise exceeds the signal is not a measurement.

Finding 3 — "100% reporting" is not a terminal state. In 32 races the feed reported 100% of expected vote counted and then continued revising in both directions. New Jersey **gained 52,650 votes** after being reported complete. Kansas gained 37,973. Virginia **lost 15,544**. Georgia recorded **26 downward revisions and 10 upward** after the count was declared complete; Michigan, 19 down and 17 up.

Finding 4 — the feed silently changed its own declared source mid-count. In **49 of 51 races the eevp_source field flipped between edison and ap during the series**, typically twice in each direction. And the archive, captured January 6, 2021 after every state had certified, still flagged **edison_certified = false for 24 of 51 races.**

Finding 5 — what is clean, reported because a document that reports only adverse findings cannot be trusted on them. Of 3,159 county reporting units: **zero** with a zero vote total; **zero** with a major-party candidate at exactly zero; **zero** where candidate results fail to sum to the reported total; **zero** timestamps carrying conflicting totals; **zero** observations with a nonzero percentage reported but zero votes. The file is internally consistent at the county level. There are no "zero counties" and no arithmetic that fails to close. **Claims to the contrary sourced to this file are wrong**, and are not made here.

Two documented explanations, offered in both directions. The Associated Press concedes that its cumulative totals can fall: "in some cases, that can lead to a drop in the total number of votes counted when the problem is identified and fixed," and it "can have up to five or six potential sources of election results in each county" (AP). And a state government has documented a vendor-side decrement in its own words — the Nebraska Secretary of State: **"Edison Research misreported public data from the Secretary of State's website… Nebraska's public results website never reported a decrease in votes"** (Nebraska Secretary of State).

Both cut in two directions at once, and both are reported here for that reason. They are benign explanations for some decrements. They are also a wire service acknowledging that it aggregates up to six unreconciled sources per county with no published reconciliation, and a state government confirming that the national feed misreported vote counts that the state itself never reported.

There is no published reconciliation of the 2020 national feed against county canvass records. MIT's Election Data and Science Lab, which archived and studied the same feed, states that it "did not systematically gather election results directly from state and local election offices for comparison," and separately confirmed that errors in the feed persisted "several hours and even days."

The audit that the state declined to call an audit

The Antrim hand tally is the most frequently cited proof that these systems can be checked. As Area C records, **counsel for the Michigan Secretary of State acknowledged at oral argument that the December 2020 hand recount was not an audit conducted pursuant to MCL 168.31a(2)** (Exhibit 16). The state characterized it publicly as "a zero-limit risk-limiting audit" confirming the result "to absolute certainty" (Michigan Secretary of State) — and, in court, as not the statutory audit.

And what it verified was the count of a ballot set whose size the county had reported three different ways.

The general point. The exercises held out as verification are not, on inspection, instruments capable of confirming or refuting a result. A hand tally of the ballots in the room tests whether the tabulator read those ballots correctly. It does not test whether those are the ballots that were cast, whether ballots were produced by the system itself, whether the election management system was compromised before the count, or whether the figures the public saw bore any relation to the figures the county held. Those questions require records that do not exist.

Minnesota, August 11, 2026

One anomaly in the 2026 Minnesota primary is documented, and it is instructive about detection.

Blue Earth County uploaded approximately **17,000 test-deck records** — pre-election logic and accuracy test data, not votes — to the Minnesota Secretary of State's live results website during the August 11, 2026 primary. It was corrected by about 10:40 p.m. The detection mechanism is the important part: the error was caught because **"results were higher than voter turnout"** (WCCO).

Three features carry the argument.

Nothing in the pipeline flagged the upload. It was caught by arithmetic impossibility noticed by a human. A test deck smaller than the county's turnout would have produced no impossibility, and no documented mechanism would have caught it.

Minnesota's ingestion model is manual data entry, not system export. Minnesota documents that county election officials **enter** unofficial results on the state website, and treats transposition errors as routine. Compare Colorado Rule 11.9.1, which requires that the results file be **"exported from the voting system."** Two states, two entirely different trust models for the same public data product, and no federal standard reconciling them — exactly as the EAC states.

A Minnesota primary receives no post-election review. Minn. Stat. § 206.89 provides for post-election review of the **general** election. There is no statutory post-election review of a primary. The one after-the-fact check that might have caught a discrepancy **does not apply to the contest in which the anomaly occurred.**

The records that would settle these questions are unavailable by design

The pattern across every area of this memorandum is that the decisive evidence is held by the party whose conduct is in question, and is not producible.

- **Source code is sealed.** The software that counts American votes is proprietary and unavailable for independent examination as a condition of the vendor relationship.
- **Audit logs are self-attested.** CVE-2022-1740. The log is written by the software the log is supposed to police.
- **Hash verification is self-attested.** The published academic finding is that malware "can completely conceal itself from the kind of hash validation performed in Georgia, which relies on the running software to self-attest to its integrity" (SF memo) — and NIST published the expected hash values (Area A).

- **The reporting layer has no logging requirement at all.** No federal standard governs its design, security or setup (EAC).
- **Reconciliations are withheld.** Michigan never produced the query or script behind 125,428 excess records, and denied the request that sought them (Area B).
- **Custody documentation is absent where it matters most.** Four ballot counts in Antrim; 3,075 undeterminable duplicate images in Fulton.

A system in which every verification mechanism is either sealed, self-attesting, unregulated, or withheld is not an auditable system. It is a system that produces a number and asks to be believed.

What would change this conclusion

Because the burden of proof rests on those asserting that these systems are secure, the following is a specific, non-exhaustive list of evidence that would materially weaken this memorandum's conclusion. None of it was located in the preparation of this document. All of it is producible by the parties who possess it.

1. A published, independently verified reconciliation of the 2020 national election-night feed against county canvass records, accounting for the 416 non-reset decrements and the 135-million-vote re-baseline.
2. Documentation that the mitigations MITRE and other central assurances depend upon were actually implemented and verified in the jurisdictions relying on those assurances.
3. A federal standard governing the design, security, logging and setup of election-night reporting systems, with conformance testing.
4. Any mechanism by which a state can apply a security patch to certified equipment without decertifying it, and evidence of its use.
5. An audit and hash-verification architecture that does not rely on the audited software's self-attestation.
6. The Michigan script, query and reconciliation that produced 125,428 excess records in the state's own published report.
7. Chain-of-custody documentation sufficient to establish that the ballots hand-counted in Antrim County on December 17, 2020 were the same set that produced the totals published on November 4.

8. A federal requirement, with audit, disclosing where certified voting system software is written and where its components are manufactured.
9. Independent examination of the runtime configuration of third-party voter registration interfaces, establishing what read capability exists today.
10. Source code available for independent examination under conditions that permit publication of findings.

Item 4 is the one that matters most, and it is the one that cannot be produced, because the regime is designed the other way.

5 Loss of Integrity Is the Cost of Convenience

Every architectural decision documented in this memorandum was made for a defensible reason, and the reason was almost always convenience.

Modems exist so that results arrive quickly: ES&S states plainly that "these early, unofficial results help the news media report results quickly on election night" (ES&S). Print-on-demand exists so that any voter can be served at any location without pre-printing every style: "ballots when and where you want them." The voter-registration-to-EMS data path exists so officials need not re-enter data — and in Michigan it exists because the state required it. Barcode tabulation exists because barcodes are faster and cheaper to read than marks. Electronic pollbooks exist to shorten lines, and Michigan is moving them toward live network connections to shorten them further. Unified tabulator security keys exist because managing unique keys across hundreds of devices is laborious. Generic shared accounts exist, in Maricopa County's own account, because they are administratively simpler and physical controls were thought to compensate.

Each of those trades a property that can be independently verified for a property that must be trusted. A pre-printed ballot is verifiable by counting; a print-on-demand ballot must be trusted. A hand-marked mark is verifiable by any human; a barcode must be trusted. An air-gapped tabulator's isolation is verifiable by inspection; a modem's transmission integrity must be trusted. A unique key per device is verifiable by enumeration; a unified key must be trusted not to have leaked. A count performed in public by neighbors is verifiable by attendance; a count performed inside sealed proprietary software must be trusted.

That is the trade, stated in one sentence: convenience was purchased with verifiability, and verifiability is the thing that makes a result binding on the losing side.

The growth of these architectures is documented. Vote centers grew from 31% to 69.6% of states between 2018 and 2024. Electronic pollbooks are used in 41 states and 41.6% of jurisdictions, with a single vendor at 61% market share. **The first federally certified electronic pollbook was certified only in February 2025** — after two decades of deployment. Ballot-on-demand printing remains **outside EAC certification scope entirely** (EAC Election Administration and Voting Survey 2024).

The professional consensus on the resulting requirement is not new and is not contested by the researchers this memorandum has relied on throughout. The National Academies concluded that elections should be conducted with human-readable paper ballots and that every effort should be made to use human-readable marks, verified by the voter (National Academies). The principle underlying that recommendation is **software independence**: an undetected change or error in the software must not be capable of causing an undetectable change or error in the reported outcome. **The systems documented in this memorandum do not satisfy that principle**, and the findings in Areas C and E — self-attesting audit logs, EMS-to-device propagation, one-minute undetectable installation, an unregulated reporting layer — are precisely why not.

And the convenience was not even cheap. The section that follows establishes that the cost comparisons routinely used to reject hand counting compare an incomplete accounting of the machine regime against a complete accounting of the alternative.

6 Remedy

The primary recommendation: hand-marked paper ballots, counted by hand, in public

The primary recommendation of this memorandum is that federal elections be conducted on hand-marked paper ballots counted by hand, in public, at the precinct, with results posted at the precinct before the ballots leave the room.

This is stated first, and as the primary remedy rather than a fallback, because it is the only architecture on the record that satisfies the requirement every other option fails: **it produces a result that an ordinary citizen can verify with his own eyes, without trusting any institution, any vendor, any certification body, or any software.** Every finding in this document reduces to the same defect — the systems in use cannot demonstrate their own correctness and cannot be shown wrong. A public hand count of human-readable ballots does not have that defect. It is not a nostalgic preference for older technology. It is the only architecture yet devised in which the outcome of an election does not depend on trusting the people who administer it.

Four arguments support making it primary. The first three answer the cost objection; the fourth is the one that governs.

First: integrity is the requirement, and speed and cost are preferences

The purpose of an election is to produce a result the losing side accepts. Nothing else it does matters if that fails. **Cost and speed are properly traded against one another; neither is properly traded against the ability to demonstrate the result**, because a result that cannot be demonstrated does not accomplish the purpose for which the money was spent in the first place. Every dollar of savings and every hour of speed documented in favor of machine tabulation was purchased with the specific property that makes an election binding.

Judge Elsenheimer, dismissing *Bailey v. Antrim County*, put it more plainly than any advocate could:

> "At its core, this case has involved, from the beginning, something that we all learned to do in kindergarten, and that is count… **We've, over time, and perhaps with good reason, in the conduct of our elections, taken this very simple function and made it into a complex and often computerized exercise.**"

(Exhibit 16, oral decision transcript.)

Second: the cost comparisons omit most of the cost of the machine regime

The studies used to reject hand counting compare the marginal cost of hand counting against the marginal cost of running machines already purchased. **They do not price the regime the machines require.** A complete accounting must include at least the following, all of which are documented.

Federal regulatory apparatus. The Election Assistance Commission exists because voting machines exist. Its salaries and expenses grew from **$2.0 million in FY2003 to $26.5 million** in recent years; the FY2025 audited figure is **$27,720,000**, including **$1.25 million transferred to NIST** for voting-system standards work, against total budgetary resources of **$48,448,164** (CRS Report R45770; EAC FY2025 Agency Financial Report). None of that expense arises in a hand-count regime.

Federal cybersecurity apparatus. CISA's election security program — **14 full-time positions and $39.61 million** in the base being eliminated in the FY2026 justification, Election Security Advisors in all ten regions, and the Elections Infrastructure Information Sharing and Analysis Center (CISA FY2026 congressional budget justification) — together with a separate **$10 million** partnership with the Center

for Internet Security that was terminated in 2025 (Nextgov), exists to defend computerized election infrastructure. A paper ballot counted in public requires no threat intelligence sharing.

Certification and testing. A single federal certification campaign runs approximately **$1 million** in test-laboratory fees; Hart's Verity Vanguard consumed **more than 6,000 laboratory hours**; Texas charges **$3,000 per component** for state examination (Bipartisan Policy Center). The Presidential Commission on Election Administration put federal certification at "well over $1 million," and one vendor is documented as having spent **"over $12 million"** pursuing certification before withdrawing (Verified Voting, "The Price of Voting"). Those costs are recovered in the per-machine price paid by counties.

Acquisition, recurring fees, and replacement. Federal HAVA appropriations for election security ran **$380.0 million in 2018, $825.0 million in 2020, $75.0 million in 2022, $75.0 million in 2023 and $55.0 million in 2024**; the EAC reports **$955 million** in election-security funds to 56 grantees since 2018 and **more than $4.35 billion** in HAVA formula funds since 2003. State purchases at the retail end include Georgia at **$107 million**, Pennsylvania at a **$90 million** bond against a statewide cost of **$125–150 million** (StateScoop), Ohio at **$104.5 million**, and Michigan at **$40 million** — $30 million HAVA plus $10 million general fund, including five years of maintenance, across 1,012 jurisdictions in 49 counties (Michigan House Fiscal Agency). Recurring vendor fees are not trivial relative to acquisition: over a ten-year horizon they reach **90.31% of acquisition cost in Davis County, Iowa; 88.87% in Lyon County, Kansas; and 83.25% in Hernando County, Florida** (Verified Voting). And the cycle repeats: nationwide replacement to meet VVSG 2.0 is estimated at **$2.71 billion**, with an independent estimate of $1–3 billion.

A caution stated because the standard requires it: these categories overlap and must not be summed. HAVA grants fund a substantial share of the state and county purchases listed. The point is not a single total; it is that the machine regime carries a federal regulatory, certification and cybersecurity superstructure plus a perpetual replacement cycle, none of which appears in a marginal hand-count cost study.

The cost of the unresolved integrity problems. Every remedy that would make machine tabulation verifiable — mandatory risk-limiting audits before certification, cast vote record publication, an independent examination regime, decoupled security patching, federal standards and conformance testing for election-night reporting, isolation of registration systems from ballot production — is an additional recurring cost of the machine regime that no comparison prices, **and that no jurisdiction has yet paid.** The machine option as actually costed is the machine option without the controls that would make it trustworthy.

Third: a large majority of the world's democracies count paper by hand, and several adopted machines and reversed

International IDEA's global survey finds that only 19% of countries — 34 of 178 — use any form of e-voting, and that 11 countries, or 6% of the total, have abandoned it after use. IDEA identifies the principal reason for abandonment as **"concern about trust and security of the vote"** (International IDEA). The overwhelming majority of the world's elections are conducted on paper counted by people.

The reversals are the most instructive part of the record, because they were made by advanced states with the technical capacity to do otherwise.

COUNTRY	ACTION	DOCUMENTED BASIS
GERMANY	Federal Constitutional Court held the use of the computerized voting machines unconstitutional in principle, 2 BvC 3/07 (March 3, 2009)	The court required that "all key steps of an election be subject to public scrutiny," and that "it must be possible for citizens to reliably scrutinise the key steps of the polling process and the determination of the result **without any specialist knowledge**" (Bundesverfassungsgericht)
NETHERLANDS	Voting machines prohibited in 2007; pencil-and-paper voting reinstated in 2009	(Kiesraad, the Dutch Electoral Council)
IRELAND	Electronic voting programme abandoned; **€51 million** spent plus roughly **€3 million** in storage costs written off	(BBC)
FRANCE	Moratorium on new deployments of electronic voting machines in place since 2008 and repeatedly maintained	(French Senate)
NORWAY	Internet voting trials discontinued in 2014	(Government of Norway)
CANADA	Federal ballots hand-counted: "Ballots are counted by trained and paid election workers who **work in pairs in front of witnesses**"; Québec provincial ballots hand-counted	(Elections Canada)

The German holding is the one that bears most directly on this memorandum, because it states the constitutional principle that the American record has abandoned: **the citizen must be able to check the count himself, without expertise.** A barcode he cannot read, tabulated by software he may not examine, reported through a layer subject to no standard, fails that test at every stage.

Two limitations stated because the standard requires it. Practice is genuinely mixed, and this memorandum will not overstate it: IDEA's own inventories place some of the countries above in categories involving optical-scan or ballot-classification equipment for particular contests, and other advanced democracies — Japan among them, with optical ballot-classification machines in municipal use since 2001, and Scotland, with electronic counting in local elections — have moved toward more machine counting rather than less. The France entry is a moratorium on new machines, not a ban on existing ones, and the German court did not invalidate the election before it. The defensible claim is the one made here: ***the large majority of countries do not use electronic voting, a documented set of advanced democracies adopted it and reversed course, and the reason recorded for abandonment is trust and security — not cost.***

Fourth: hand counting is already the mandated fallback, precisely because machines fail

Hand-counted paper is not a hypothetical alternative. **It is already the legally required backstop in multiple states, and it is required precisely because electronic systems are known to fail.**

Georgia State Election Board Rule 183-1-12-.11(2)(c):

> "If an emergency situation makes utilizing the electronic ballot markers impossible or impracticable… the poll officer shall issue the voter an emergency paper ballot that is to be filled out with a pen… **For any primary or general election for which a state or federal candidate is on the ballot, a sufficient amount of emergency paper ballots shall be at least 10% of the number of registered voters to a polling place.**"

Rule 183-1-12-.11(2)(d) names the qualifying emergencies: "**power outages,** malfunctions causing a sufficient number of electronic ballot markers to be unavailable for use, or waiting times longer than 30 minutes" (Georgia State Election Board rules).

New York Election Law § 7-120 goes further, making paper mandatory after one hour: "It shall be the duty of each board of elections to cause a sufficient number of emergency ballots to be placed at each polling place… At any time during the hour succeeding a breakdown, the inspectors of election may use such emergency ballots, and **if such breakdown lasts more than one hour, such emergency ballots must be used**" (N.Y. Elec. Law § 7-120).

New Hampshire requires it for recounts outright: "**no mechanical, optical, or electronic device shall be used for the counting of ballots**" (CEIMN), and towns covering roughly 10% of that state's voters hand-count as their routine method.

Federal continuity guidance, by contrast, is voluntary. The EAC states that "election officials are expected to continue their work, even during a crisis," and defines continuity-of-operations planning by reference to NSPD-51/HSPD-20 — but its guidance contains **no mandatory paper-ballot backup requirement**, and the EAC states its guidelines "are solely designed to serve as a source of information for election officials and not as requirements by which they must abide" (EAC contingency planning).

The law of several states already concedes the argument. It holds that when the machines cannot be trusted to work, the count reverts to paper and people. This memorandum's position is that the record documented above establishes that condition permanently rather than episodically.

The cost and accuracy record for hand counting, stated openly

The evidence against full hand counting at scale is real, it will be raised immediately, and concealing it would forfeit the credibility on which everything else here depends. **It is therefore stated in full.**

JURISDICTION / STUDY	DOCUMENTED FINDING
SHASTA COUNTY, CA	Annual cost increase **$445,528**; one-time costs **$914,146**; per-presidential-election increase **$1.41M–$1.69M**; the 2024 presidential primary alone estimated at **$659,000** and **375 additional staff** (Shasta County; States United)
MOHAVE COUNTY, AZ	Hand count estimated at up to **$1.1M**; nearly **500** new workers; test deck of 850 ballots produced **46 errors, a 5.4% error rate** (Mohave study takeaways)
KERN COUNTY, CA	2022 midterm hand count estimated at **103,857 hours, 920 temporary staff, nearly $1.9M** (Verified Voting)
NYE COUNTY, NV, 2022	"Just one day into the count, they found a discrepancy of nearly **25%**" (Verified Voting)
MARICOPA COUNTY, AZ, 2021 AUDIT HAND COUNT	**Over 28% of hand count batch totals did not match** — 51 of 180 batches (Maricopa County)
WISCONSIN STATEWIDE RECOUNTS, 2011 & 2016	"vote counts originally conducted by computerized scanners were, on average, **more accurate** than votes that were originally tallied by hand" (Ansolabehere, Burden, Mayer & Stewart)
RICE UNIVERSITY CONTROLLED EXPERIMENTS	Error rates around **1.4%**, with the authors noting "if anything, we expect that our data **underestimate** both the time necessary for audits and error rates" (Goggin, Byrne & Gilbert)
ESMERALDA COUNTY, NV	Seven-plus hours for **317 ballots** in the June 2022 primary (Verified Voting)
OSAGE COUNTY, MO	The clerk expected savings; "unfortunately, that was not the case" — costs "were actually higher" (States United)

Shasta County's clerk, who conducted the analysis, concluded that "a selective manual tally — that is, hand counting some ballots to prove that machine counts are precise, accurate, and indicate the correct winner — is generally recognized as a **best practice**… However, in a county the size and complexity of Shasta,

hand counting every ballot — particularly without verification by another method — is not a best practice."

Three responses, none of which requires disputing a single figure above.

One: every error in that table is a known error, and that is the entire distinction. The 28% batch mismatch in Maricopa and the 25% first-day discrepancy in Nye County are **measurements of human error that were detected and corrected because the count was performed on a human-readable record that multiple independent parties could re-examine.** The comparable figure for the electronic systems documented in Areas A through E **does not exist and cannot be produced**, because the audit log self-attests, malicious code modifies "all records, logs, and counters," the reporting layer is governed by no standard, and no independent party may lawfully examine the software. **A 5.4% error rate you can see and fix is a better foundation for a republic than an unknown error rate you cannot measure.**

Two: these figures measure hand counting performed the wrong way — centrally, at county scale, on a compressed statutory deadline, by temporary staff hired for the purpose. The architecture recommended here is different in kind: counting at the precinct, by the precinct's own bipartisan board, of the several hundred to two thousand ballots cast in that precinct, immediately after the close of polls, in public, with the result posted on the door before the ballots move. That is the model Canada uses federally, with workers "in pairs in front of witnesses" (Elections Canada), and it is a fundamentally different task from tallying 400,000 centralized ballots against a deadline. **Precinct-scale counting also produces something no county-scale count produces: thousands of small, independently posted, publicly witnessed subtotals that anyone can add up.** The cost studies above price the centralized model. They do not price this one.

Three: the studies price hand counting against machines already bought, and against a machine regime whose integrity controls have not been funded. Once the certification apparatus, the federal cybersecurity apparatus, the perpetual replacement cycle, and the unpaid cost of the audit and transparency controls that would actually make machine counts verifiable are all included, the comparison is not the one the studies present.

The recommendation stands: hand-marked paper ballots, hand-counted at the precinct, in public, as the primary method of conducting federal elections.

Supporting Measures for the Transition Period

Where a jurisdiction cannot immediately transition, and during any transition period, the following should be directed for all federal elections. Each is independently justified by the record above, and each is a partial measure — none is a substitute for the primary recommendation.

1. Hand-marked paper ballots in every case. No ballot-marking device except as an accessibility accommodation, and where used, configured to produce ballots **without barcodes for tabulation** — an option CISA notes the equipment already provides. The counted portion of a ballot must be the portion a human can read.

2. Machine tabulation, where retained, is preliminary only. A scanned result has no official status until confirmed by manual examination of the human-readable ballots. Where the two disagree, **the paper governs**, and the disagreement is published.

3. Mandatory risk-limiting audits of the human-readable record before certification, with published methodology, published sample selection, and published results. This is what CISA itself recommends: "conduct rigorous post-election tabulation audits of the human-readable portions of physical ballots and paper records" (CISA). Audit-scale hand counts are documented as accurate — "less prone to error than election night hand counts because there are many fewer votes to count, and the ballots can carefully be examined under significantly less time pressure" (Verified Voting).

4. Prohibition on any network connectivity — wired, wireless, or modem — for any device that marks, scans, tabulates, or aggregates votes, at any time. This aligns federal practice with the existing federal standard: draft VVSG 2.1 "does not permit devices or components using external network connections to be part of the voting system." **The standard already says this. It is voluntary. Make it mandatory.**

5. Federal standards for election-night reporting, closing the gap the EAC has itself identified. At minimum: results files must be exported from the certified system rather than hand-entered, following Colorado Rule 11.9.1's model; **every revision to a published cumulative total must generate an immutable, publicly available log entry stating the reason**; and the source of every published figure must be attributable. Had this existed on November 4, 2020, the 135-million-vote re-baseline documented in Area E would be a closed question.

6. Mandatory publication of cast vote records and complete tabulator logs within a fixed period after certification, in machine-readable form. This is the highest-value transparency measure available and it costs almost nothing. It converts the disputes in this memorandum from arguments about access into arithmetic anyone can check.

7. Isolation of voter registration systems from ballot production and tabulation systems. Any data path between them must be subject to federal standard and audit — which requires revisiting state requirements of the kind documented in Michigan's contracts, where the interface is mandatory. External programmatic ingress into state voter registration systems must be federally governed, with published runtime configuration, so that questions of the kind raised in Area A about read capability can be answered by evidence rather than by the operator's assurance.

8. Independent examination as a right, not a crime. A lawful, credentialed process by which qualified independent examiners may inspect certified equipment and software and publish their findings. The current regime — proprietary source code shielded, forensic images destroyed by vendor updates, unauthorized examination drawing criminal referral — guarantees that the security question can never be settled.

9. Decoupling security patching from recertification. An expedited pathway for security updates so that applying a patch is no longer a decertifying act. On the record here this is the single change most likely to improve the security of any machinery that remains in service.

10. Disclosure and audit of software development locus and component origin for any system retained in federal elections, and of the data-residency obligations of every ancillary contractor handling election or election-worker data. The Konnech episode ended with a dismissal, a $5 million settlement, and **no authoritative finding about where the data went.** That should not be possible.

11. A tested continuity capability in every jurisdiction. Every jurisdiction conducting a federal election must maintain a continuity plan providing for the complete conduct of that election on hand-marked, hand-counted paper ballots, with sufficient ballot stock on hand, and the plan must be **exercised — not merely filed — before each federal election.** For jurisdictions transitioning to the primary recommendation, this exercise is the transition.

7 Conclusion

The case against electronic voting systems does not require proving that an election was stolen, and this memorandum has not attempted to prove it. The case rests instead on facts drawn almost entirely from the government's and the vendors' own records.

The federal cybersecurity agency has confirmed nine vulnerabilities in a certified system, including forged technician authentication, extraction of county-wide cryptographic secrets, propagation of malicious code from the central system to every device in a jurisdiction, an audit log that grades itself, and the

unauthorized printing of an unlimited number of ballots. The same agency's internal assessment found a third of assessed election entities running operating systems that receive no security patches, and a 108-day median remediation time for critical vulnerabilities with publicly known exploits. A state required, by contract, that every certified voting system interface with its statewide voter registration database. A federal standards body published a file-level manifest of a certified system's software, with expected hash values, on a public server — while hash verification on that system relies on the software's self-attestation. A county has stated on the record that applying a security patch would decertify its equipment, and a state announced it would run a presidential election on known-vulnerable software rather than break certification. The Election Assistance Commission has stated that the layer of the system through which the entire public learns the result is governed by no federal standard at all. The archived record of that layer shows 135 million cumulative votes discarded and re-baselined across fifty states in four hours, with no log, no explanation, and no requirement that either exist — and, in three of the six states that decided the 2020 election, downward revisions exceeding or equalling the certified margin. A county produced four different totals for the same ballots. A state published more than 125,000 excess records in its own ballots-cast report and denied the request that sought the reconciliation. Unauthorized parties obtained thirteen hours of administrative access to a county's central tabulator, changed its system clock twice without changing it back, and the fact of it had to be reconstructed afterward from surveillance footage. And the company at the head of the industry's technical lineage is a defendant in a federal indictment alleging that the price charged per voting machine was the instrument of a bribery scheme.

Set against that record is a body of assurance whose central technical document concluded that the attacks were operationally infeasible **on the assumption that mitigations were in place which the record indicates were not in place.** Under the standard applied throughout this memorandum — the same standard applied to every claim on the other side — that assurance has not been substantiated.

The question before the President is not whether these systems have been exploited. On the evidence available to anyone outside a county election office, that question cannot be answered, and the reason it cannot be answered is the design of the systems themselves. A tabulator whose audit log self-attests, a ballot whose counted portion no human can read, a results feed that can silently discard a national vote total, a registration database joined by mandate to the machinery that prints and counts ballots, and a software base that no independent party may lawfully examine, together constitute a system that is not merely insecure but **unfalsifiable** — incapable, by construction, of demonstrating its own correctness or of being shown wrong.

That is also why this is a national security matter and not merely an administrative one. An adversary does not need to defeat American elections to profit from them. It needs the roster of the electorate, the running state of the count, the identity of the small number of counties where a national margin is decided, and the knowledge that the vulnerabilities it finds will remain open by regulation through the next federal election. Every one of those is available on the present record, and the federal capacity assembled to contest it is being reduced.

The consent of the governed rests on a demonstrable count. Not a trusted one — a demonstrable one. A hand-marked paper ballot, counted by hand in public at the precinct where it was cast, with the subtotal posted before the ballots leave the room, produces a result that any citizen of ordinary competence can verify with his own eyes. Germany's constitutional court reached the same requirement from first principles: the key steps must be scrutinizable by the citizen **without any specialist knowledge.** Most of the world's democracies count this way, and several of the wealthiest abandoned machines to return to it.

The systems in use today cannot demonstrate their own results. That is sufficient grounds to stop using them in federal elections.

8 Appendix — Method and Limitations

8.1 The feed analysis

The findings in Area E derive from direct programmatic analysis of `results.json`, an 11-megabyte archived capture of the New York Times 2020 general election presidential results feed, `meta.version` 25064, `meta.timestamp` 2021-01-06T01:19:29.800Z. The file contains 51 races, 3,159 county reporting units, and 11,063 timestamped observations. Analysis scripts are reproducible and the intermediate outputs are preserved.

Two corrections were applied, and any analysis omitting them will produce false results.

Ordering. The stored observation arrays are **not** in chronological order in any of the 51 races; there are 110 out-of-order adjacent pairs. Walking the arrays as stored manufactures decrements that do not exist. All figures were computed after sorting each series by timestamp.

Quantization. The feed stores one integer cumulative total per race and per-candidate shares rounded to three decimal places. A per-candidate count must be reconstructed as total × share, carrying up to ±0.0005 × total of error — for a five-million-vote state, ±2,500 per candidate. **Every finding reported in**

Area E rests on the race-level integer total and is unaffected by this. Candidate-level figures are reported only where the drop exceeds the quantization bound; 195 such drops exist across all 51 races.

Independent corroboration of the limitation. MIT's Election Data and Science Lab, which archived and analyzed the same feed, separately confirmed that errors persisted "several hours and even days," and states that it "did not systematically gather election results directly from state and local election offices for comparison."

The Michigan multi-record analysis

The findings in Area B derive from direct programmatic analysis of the statewide daily-ballots-cast records captured by citizen observers during the 2024 Michigan general election, in the state's own export format. The analysis script and its full output are supplied as Exhibit 15; the underlying capture is in the possession of the submitting party and is available on request, being too large to append to this memorandum.

Stated limitations. The file is a citizen capture, not a state production, and its chain of custody rests on the capturing parties' account. The analysis establishes the arithmetic of the file — 208,075 rows, 82,647 distinct voter identifiers, an excess of exactly 125,428 — and the internal patterns reported. **It does not establish that any ballot was improperly cast, and no such claim is made.** Two of its findings are consistent with the state's export-defect explanation and are reported as such. The finding that an address-history join cannot readily explain is the 5,258 byte-identical duplicate rows across 4,554 voter identifiers. The state has not produced the query, script, or reconciliation that would resolve the matter, and no independent party has been permitted to compare the citizen capture against the state's own contemporaneous file.

Items that could not be verified and are not asserted

- No 50-state survey exists of whether election-night reporting data must be exported from the certified voting system or may be hand-entered.
- No independent audit of Dominion's "transfer point" network isolation control was located.
- No contract between Edison Research or SSRS and any state or county is publicly available, so the precise mechanism by which county data reaches the feed in each jurisdiction is not established.
- No documented instance was found in which an investigator attributed a feed decrement to actual alteration of votes.

- No peer-reviewed treatment of cumulative-count monotonicity in election reporting was located.
- No primary-source enumeration of open network ports on any certified voting system was located; no specific open ports are asserted anywhere in this memorandum.
- **No federal indictment of Konnech Inc. or Eugene Yu was located, and none is asserted.** The Los Angeles County charge was dismissed and the county paid $5 million and proclaimed Yu's innocence.
- **No documentation was located establishing offshore storage or transfer of United States ballot or tabulation data by Dominion, ES&S or Hart InterCivic.** What is documented is offshore development labor and foreign-manufactured components, on the vendors' own statements.
- **No source establishes the actual runtime configuration of the Rock the Vote registration interface at any point in time.** The read endpoints' removal from the published documentation is documented; their removal from the running system is not.
- **No published security rationale for that removal was located.**
- No EAC Testing and Certification program budget line item was located; certification cost figures are drawn from test-laboratory fee reporting and commission-level appropriations.
- No Government Accountability Office report addressing the total cost of the machine-based election regime was located.
- No separate accounting of per-election ballot-programming fees paid to vendors was located.
- A circulating claim that Scytl collects all state election-night reporting data and provides it to Edison Research traces only to a private citizen's county public comment and is not usable as evidence.
- The term "AP StaffEntry," which circulates in discussions of this pipeline, appears in no Associated Press source located.
- The Fifth Circuit's First Amendment holding concerning CISA, cited in some accounts of federal involvement in election-related speech, was **reversed on standing grounds** by the Supreme Court in *Murthy v. Missouri*, and is not relied upon here.

8.2 Exhibits

Sixteen documents were supplied in support of this memorandum and are indexed separately. Three notes on their handling:

Exhibit 9, the CISA *Election Infrastructure Subsector Cyber Risk Summary*, carries a **TLP:AMBER** marking, which by its own terms limits redistribution to participants' organizations and clients with a need to know. A copy is in circulation. Any public reproduction of this memorandum should display that marking and treat reproduction as a deliberate decision.

Exhibit 12, Michigan contract 071B7700128, Exhibit 2 to Schedule A, Hart InterCivic technical requirements, was **received in truncated form and could not be read**; the PDF's cross-reference table is unrecoverable. The Michigan voter-registration interface requirement discussed in Area A was therefore sourced from Exhibit 13 — the corresponding Dominion contract document, which was readable — and independently from the state-published Hart contract and the ES&S bid document.

Exhibit 14, the compiled 2020 critical-infrastructure analysis, contains citations bearing the signature of automated generation. Its arithmetic on certified margins and minimum single-county flips was therefore recomputed from primary-sourced certified results rather than accepted from the document, and only the recomputed figures appear in this memorandum.

Every factual assertion in this memorandum is cited to a primary document, or is explicitly labeled as an allegation, a limitation, or unresolved.