The 2020 Election:

An Attack Upon U.S. Critical Infrastructure

June 2026

V2.0

EXECUTIVE SUMMARY

LINDELL OFFENSE FUND

LindellPlan.com

Made possible by funding from the Lindell Offense Fund

THE 2020 ELECTION

An Attack Upon U.S. Critical Infrastructure

This Executive Summary provides brief overview of the evidentiary record compiled in the full report, The 2020 Election: An Attack Upon U.S. Critical Infrastructure. All assertions in the report are drawn from forensic analyses, sworn legislative testimony, court filings, inspector general investigations, vendor invoices, reasonable inference based upon open-source intelligence, and government communications obtained through litigation and FOIA.

CORE FINDING

The 2020 General Election produced a convergence of ten distinct attack vectors that — individually — each constitute a predicate for federal grand jury action and — collectively — represent the most serious documented assault on democratic infrastructure in modern American history. The threat is constitutional, institutional, and national security in character. Adversarial foreign powers exploited vulnerabilities deliberately created or maintained by domestic actors. Independent oversight was blocked at every institutional layer — judicial, executive, and informational — before forensic verification could occur. No federal agency has conducted a comprehensive, independent investigation of the convergent record.

The full report documents 824 findings across 10 attack vectors, including 553 established facts, 155 disputed facts, and 116 reasonable, analytically supported inferences. It is supported by 2,527 numbered citations and spans approximately 800 pages. In other words, anyone who asserts that there is no evidence of 2020 election malfeasance is not credible. The report is organized by 10 distinct "attack vectors" against our election system which has been designated as "critical infrastructure". These 10 "attack vectors" are depicted in Figure 1.

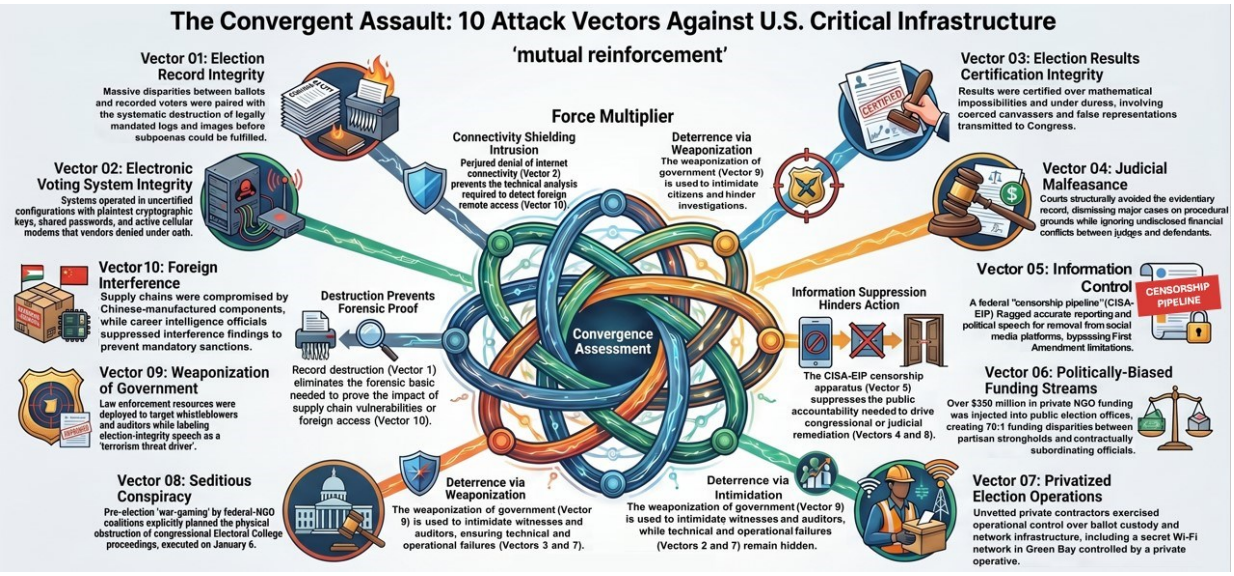

Figure 1 10 Attack Vectors Against U.S. Election System

Table 1 provides a summary of the findings for each of the 10 attack vectors documented in the full report.

Table 1 2020 Election Findings by Attack Vector

ATTACK VECTOR	FINDINGS SUMMARY	CRITICAL-INFRASTRUCTURE IMPACT
ELECTION RECORD INTEGRITY	Records needed to validate or invalidate the election were compromised across battleground jurisdictions: voter rolls, voter histories, ballot images, tabulation tapes, adjudication records, and system logs were missing, destroyed, inconsistent, or withheld.	Loss or destruction of records eliminated independent forensic layers and shifted public debate from proof to trust.
ELECTRONIC VOTING SYSTEM INTEGRITY	Systems were operated in configurations that deviated from certified baselines, including last-minute database changes, deleted logs, plaintext credentials, remote-access pathways, and modem or connectivity indicators.	Unverified configurations and connectivity risks created exploitable attack surfaces in designated critical infrastructure.
ELECTION RESULTS CERTIFICATION INTEGRITY	Certification was treated as final despite unresolved mathematical, procedural, and evidentiary issues, including duress against canvassers, incomplete statutory signatures, open investigations, and disputed reconciliation.	The last institutional checkpoint before electoral votes were cast was neutralized without full evidentiary review.
JUDICIAL MALFEASANCE	The courts largely failed to reach the evidentiary record because many cases were dismissed on procedural grounds, discovery was denied, conflicts were alleged, and attorneys faced sanctions or professional destruction.	The legal system provided no functional forum for retrospective adjudication of the forensic record.
INFORMATION CONTROL	Federal and federally aligned entities used private or academic intermediaries to flag election-related speech, suppress competing narratives, and shape public perception while withholding contrary vulnerability information.	Public accountability and congressional action were blunted by censorship-by-proxy and selective disclosure.
FINANCIAL INFLUENCE	Private funding was injected into election administration with contract terms and distribution patterns that favored key	Core public election functions were influenced through private financial

ATTACK VECTOR	FINDINGS SUMMARY	CRITICAL-INFRASTRUCTURE IMPACT
	jurisdictions and subordinated public officials to private grant conditions.	leverage outside ordinary public accountability.
PRIVATIZED ELECTION OPERATIONS	Private contractors and NGO-linked actors exercised operational control over ballot facilities, network infrastructure, election-night decisions, and system access without statutory authority or public vetting.	Unvetted private actors became gatekeepers over physical, digital, and procedural components of election infrastructure.
SEDITIOUS CONSPIRACY	Pre-election planning, simulation exercises, and disruption scenarios contemplated preventing or obstructing congressional Electoral College proceedings, later aligning with the constitutional effect of January 6.	The report frames the obstruction of congressional review as a national-security question requiring formal investigation.
WEAPONIZATION OF GOVERNMENT	Law-enforcement, prosecutorial, administrative, and counterterrorism tools were used to deter witnesses, punish auditors, target attorneys and citizens, and shield election administration from scrutiny.	Those who sought transparency bore consequences while officials accused of record destruction or obstruction often faced none.
FOREIGN INTERFERENCE	The report identifies foreign exposure through supply chains, software lineage, network communications, voter-data access, Chinese-manufactured components, and alleged suppression of E.O. 13848-related intelligence.	Foreign-interference review mechanisms were disabled or delayed before Congress and the public could evaluate the threat.

A cross-jurisdiction analysis of the findings throughout these 10 attack vectors is provided and reveals eight irrefutable patterns evident in multiple states (See Table 2). These multi-state patterns reinforce the need for federal government investigation into these findings. They indicate that these attacks upon our election system were conducted in a coordinated manner.

Table 2 Cross-Jurisdiction Patterns

PATTERN	DESCRIPTION
Synchronized Record Destruction Preceding Oversight Events	Across multiple battleground states, destruction or deletion of election records occurred before legislative subpoenas, FOIA requests, and forensic audits. The analysis highlights missing ballot images, eliminated cryptographic files, absent adjudication logs, and vendor-directed trusted-build updates that deleted log files across county lines, suggesting a coordinated obstruction pattern rather than routine local administration.

PATTERN	DESCRIPTION
Uniform Voting System Configuration Deviations	Voting systems in separate jurisdictions exhibited similar deviations from certified baselines, including plaintext credentials, shared passwords, active cellular connectivity, uncertified updates, and common vendor-level configuration weaknesses. The recurrence of the same vulnerabilities across counties and states suggests a supply-chain or vendor-management source rather than independent local error.
Coordinated Coercion of Certification Officials	Certification officials in multiple jurisdictions faced pressure, harassment, or procedural disregard after raising unresolved anomalies. The pattern described is certification proceeding despite mathematical discrepancies, duress, missing statutory requirements, or rescinded objections, indicating that the final checkpoint before electoral votes were cast was neutralized across jurisdictions.
Procedural Foreclosure of Judicial Merits Review	Post-election legal challenges across jurisdictions were blocked through similar procedural mechanisms, including standing, laches, mootness, denial of discovery, and coordinated professional sanctions against counsel. The analysis characterizes this as a cross-jurisdictional denial of evidentiary access that prevented courts from reaching the underlying forensic record.
Geographically Targeted Private Funding with Operational Control	Private election-administration funding flowed through a common NGO apparatus with non-neutral geographic distribution and grant terms requiring public officials to obtain private approval for operational changes. The analysis identifies uniform contractual subordination, partisan geographic targeting, and operational influence as evidence of centralized private control across jurisdictions.
Unvetted Private Actors Controlling Critical Election Infrastructure	Private contractors and NGO-linked actors, controlled ballot custody, election-night facilities, network infrastructure, tabulation hardware, and system access without statutory authority or public vetting. Similar patterns of configuration-data destruction and blocked forensic access followed, indicating private operational control over critical election infrastructure across jurisdictions.
Selective Prosecution of Witnesses and Suppression of Oversight	The analysis demonstrates a repeated inversion of law-enforcement priorities: witnesses, auditors, attorneys, and local officials who sought election review faced investigation or retaliation, while officials accused of record destruction or obstruction faced little accountability. Complaints were routed to conflicted officials, deterring independent federal or state review.
Suppression of Foreign Interference Intelligence Across Agencies	Foreign supply-chain vulnerabilities, network communications, voter-data exposure, and foreign-manufactured components appeared across multiple jurisdictions while related intelligence was suppressed within federal agencies. The analysis argues that this prevented full activation of E.O. 13848 foreign-interference review and delayed congressional or public assessment of the threat.

The report's most important analytical claim is convergence. The 10 attack vectors are not independent events but mutually reinforcing failures. Record destruction removed the forensic basis for detecting intrusion. Denials of connectivity prevented technical analysis. Judicial foreclosure blocked discovery and merits review. Information suppression prevented public accountability and congressional action. Intelligence suppression disabled the foreign-interference response. Weaponized government action deterred witnesses, auditors, attorneys, public officials, and citizens from coming forward. Taken together, every institutional layer capable of detecting, adjudicating, or reporting election misconduct was neutralized before full forensic verification could occur. That cross-jurisdictional pattern is the basis for treating the matter as a national-security and critical-infrastructure event requiring compulsory investigation, not merely as a political controversy. The national security implications of such findings are significant as there are indications that domestic and foreign actors were involved in subverting the lawful execution of the 2020 election. Such findings warrant criminal investigations and legislative reforms.

The full report provides recommendations for such efforts. These recommendations include a prioritized list of 18 recommended investigations along with 8 search warrants. The recommended investigations are summarized in Table 3.

Table 3 Recommended Investigations

ID	INVESTIGATION TITLE	PRIORITY
INV-01	Vote Tally Chain of Custody: Results Transmission, ENR, Media Feed, and Vendor-Held Records	**IMMEDIATE**
INV-02	Ballot Chain of Custody	**IMMEDIATE**
INV-03	Voter History Chain of Custody	**IMMEDIATE**
INV-04	Voter Roll Chain of Custody	**IMMEDIATE**
INV-05	Election Interference Planning and Execution	**IMMEDIATE**
INV-06	FEC-Enabled Money Laundering	**HIGH**
INV-07	Perjury — Voting System CEO's False Sworn Denial of Internet Connectivity	**IMMEDIATE**
INV-08	Post-Election Destruction of Federally Mandated Election Records — Michigan	**IMMEDIATE**
INV-09	Post-Election Destruction of Federally Mandated Election Records — Georgia	**IMMEDIATE**
INV-10	Post-Election Destruction of Federally Mandated Election Records — Pennsylvania & Arizona	**IMMEDIATE**
INV-11	Perjury — Voting System CEO's False Sworn Denial of Internet Connectivity	**IMMEDIATE**
INV-12	False Statements to Congress — Georgia Secretary of State's January 6, 2021 Letter	**HIGH**
INV-13	Remote Access to Electronic Voting Systems – Center for Internet Security	**IMMEDIATE**
INV-14	Electronic Voting System Subcontractors – Election Source, Runbeck	**IMMEDIATE**
INV-15	CISA / Election Integrity Partnership — Unconstitutional Censorship Architecture	**HIGH**
INV-16	CTCL/CEIR Private Election Funding — Election Bribery and Subordination of Public Officials	**HIGH**
INV-17	"Delivered Just the Margin"— Milwaukee Elections Group Contractor	**HIGH**
INV-18	CFIUS Evasion — Voting System Foreign Ownership and Chinese-Manufactured Components	**IMMEDIATE**

The search warrants delineated in Table 4 are recommended in support of these investigations. To date, most investigations into the integrity of the 2020 election have been constrained to information obtained using Open-Source Intelligence (OSINT). Search warrants enable access to election records heretofore denied to the public which are essential to discerning the extent to which our election systems have been compromised and to what degree the public trust in such systems is currently merited.

Table 4 Recommended Search Warrants

ID	SEARCH WARRANT TITLE	TARGET / SUBJECT
SW-01	Center for Internet Security / EI-ISAC 2020 Election Infrastructure Records	CIS, MS-ISAC,EI-ISAC
SW-02	Electronic Voting System Subcontractors – EMS Project Files, Configuration Records, Access Logs, and Maintenance Directives	Election Source, Runbeck
SW-03	Milwaukee Elections Group Contractor — Election Night Network Control	Ryan Arey; Elections Group LLC
SW-04	Georgia Secretary of State's Office — January 6 Letter and Internal Investigation Records	Office of the Georgia Secretary of State; Brad Raffensperger (official capacity)
SW-05	CTCL/CEIR Grant Agreements, Compliance Reports, and Operational Communications	Center for Tech and Civic Life (CTCL); Center for Election Innovation and Research (CEIR)
SW-06	CISA / Election Integrity Partnership — Internal Communications and Content-Flagging Records	CISA; Stanford Internet Observatory; Election Integrity Partnership
SW-07	Voting System Vendor Cellular Modem Billing Records	Dominion Voting Systems, Inc.; AT&T, Verizon, T-Mobile (cellular carriers)
SW-08	Search Warrant for Vote Tally Chain-of-Custody Records, Results Transmission Logs, Election Night Reporting Data, Media Feed Records, and Vendor-Held Election Result Artifacts	SCYTL/SOE; Edison Research; Tyler Technologies; Associated Press

In addition to investigations, the report recommends the adoption of 13 federal legislative reforms (See Table 5) and 15 state legislative reforms (See Table 6). A key tenet of these legislative reforms is the need to shift the burden of proof from the backs of citizen investigators to prove election fraud to the need for election officials to prove that the elections were conducted in a lawful, transparent manner.

Table 5 Recommended Federal Legislation

ID	TITLE	DESCRIPTION
F-01	**Election Records Transparency and Preservation Act**	Requires comprehensive preservation, public availability, and forensic protection of physical and digital election records necessary to reconstruct federal elections.

ID	TITLE	DESCRIPTION
F-02	**Election Certification Burden of Proof Act**	Prohibits certification of federal election results unless election officials first produce a public evidentiary record proving lawful compliance.
F-03	**Federal Election Digital Evidence Act**	Establishes national digital-evidence standards for systems and records used to administer, tabulate, adjudicate, and audit federal elections.
F-04	**Voting System Certification Integrity Act**	Requires the system actually deployed in an election to match the certified system and be retested after material changes.
F-05	**Election System Connectivity Prohibition Act**	Bans unauthorized connectivity and requires sworn, independently verified proof that election systems are not connected to prohibited networks.
F-06	**Election Vendor Accountability and Supply Chain Security Act**	Regulates election vendors as critical-infrastructure contractors and requires transparency over ownership, software, components, and foreign exposure.
F-07	**Public Election Administration Act**	Prevents private entities from exercising operational control over public election functions or election infrastructure.
F-08	**Election Data Access and Voter File Security Act**	Regulates third-party access to voter files and election databases and requires auditable logs of voter-file changes.
F-09	**Federal Election Audit Rights Act**	Creates enforceable audit rights for candidates, parties, voters, legislatures, and courts before federal results are finalized.
F-10	**Election Whistleblower Protection Act**	Protects election workers, public officials, contractors, vendors, and citizens who make good-faith reports of election irregularities.
F-11	**Election Censorship and Government Speech Neutrality Act**	Prohibits federal agencies from suppressing lawful domestic speech about election administration directly or through third parties.
F-12	**Foreign Election Interference Disclosure and Sanctions Act**	Strengthens congressional notification, public reporting, and sanctions review for foreign threats to U.S. election infrastructure.
F-13	**SAVE Act / Save America Act Eligibility Model**	Uses proof-of-citizenship, voter-identification, and voter-roll maintenance reforms as one component of a broader election-integrity framework.

Table 6 Recommended State Legislation

ID	TITLE	DESCRIPTION
S-01	**State Election Record Transparency Act**	Requires preservation and prompt public disclosure of physical and digital election records at the state and local levels.

ID	TITLE	DESCRIPTION
S-02	**State Election Certification Proof Act**	Requires state and local election officials to prove statutory compliance before certifying results.
S-03	**State Burden-Shifting Election Contest Act**	Revises election-contest procedures so officials bear the burden once challengers identify material irregularities.
S-04	**State Ballot Image and Digital Audit Act**	Requires creation, preservation, hashing, and controlled public release of ballot images and digital audit records.
S-05	**State Chain-of-Custody Act**	Codifies strict custody requirements for every ballot, election device, memory card, seal, and transfer point.
S-06	**State Voting System Configuration Act**	Requires public testing, disclosure, and forensic preservation of the actual voting-system configuration used in each election.
S-07	**State No-Connectivity Election System Act**	Prohibits unauthorized network connectivity in voting and tabulation systems and requires sworn verification.
S-08	**State Election Vendor Licensing Act**	Licenses and regulates election vendors, subcontractors, and service providers as entities serving critical public infrastructure.
S-09	**State Private Election Funding Prohibition Act**	Prohibits private money, staffing, software, consulting, or operational support from controlling public election administration.
S-10	**State Voter Roll Integrity Act**	Requires continuous, auditable voter-roll maintenance and eligibility verification, including proof-of-citizenship reforms where legally permissible.
S-11	**State Canvasser Independence Act**	Protects canvassers and election boards from coercion and guarantees access to records necessary for certification decisions.
S-12	**State Election Audit Independence Act**	Creates independent audit authority outside the control of the officials and vendors whose conduct is being audited.
S-13	**State Election Public Records Fast-Track Act**	Creates expedited public-records procedures, preservation duties, and penalties for delayed election-record production.
S-14	**State Legislative Election Oversight Act**	Reaffirms the legislature's constitutional role by requiring election officials to produce records and comply with subpoenas.
S-15	**State Election Official Accountability Act**	Creates meaningful civil, administrative, and criminal consequences for intentional or reckless violations of election law.

The report's conclusion emphasizes that election systems are critical infrastructure and that an attack upon election infrastructure is an attack upon the country's constitutional order. It argues that the sheer volume of findings, their recurrence across jurisdictions, and the neutralization of oversight mechanisms require a formal institutional response. The report further stresses the human cost borne by patriotic Americans who attempted to investigate the 2020 election and were threatened, censored, defamed, prosecuted, professionally punished, or otherwise targeted by government actors and their partners. The conclusion frames accountability as necessary for two inseparable reasons: justice for those targeted by weaponized institutions, and deterrence against future election misconduct. It calls on federal and state authorities to preserve evidence, compel testimony, examine surviving digital artifacts, investigate potential crimes and civil-rights violations, protect whistleblowers, and reform election systems so future contests are transparent, lawful, auditable, and worthy of public confidence.

BOTTOM LINE

The report does not ask officials to accept a political conclusion. It asks them to investigate evidence. If election officials, vendors, private actors, or government agencies violated the law, destroyed records, concealed vulnerabilities, obstructed review, or retaliated against investigators, accountability is required not as vengeance, but as deterrence and restoration of public confidence.