FOR IMMEDIATE RELEASE

JUNE 24th, 2026

Election Crime Bureau Releases Landmark Evidence Dossier: "The 2020 Election – An Attack Upon U.S. Critical Infrastructure"

The Election Crime Bureau today released a comprehensive, fully cited investigative report, "The 2020 Election – An Attack Upon U.S. Critical Infrastructure," documenting ten coordinated attack vectors against America's election infrastructure in the 2020 general election. The report compiles more than **824 distinct findings** supported by over **2,517 citations** drawn from court records, government documents, sworn testimony, and technical forensics. Full documentation is available at **ElectionCrimeBureau.com/Evidence**.

"People have been told for years there is 'no evidence,'" said Patrick Colbeck with Mike Lindell's Election Crime Bureau. "This report does not ask you to trust us. It asks you to read the evidence, check the citations, and decide for yourself."

A national-security framing, not just politics

The report treats U.S. elections as what federal law already says they are: **designated critical infrastructure** on par with the power grid and financial systems. It concludes that in the jurisdictions that decided the 2020 presidential outcome, the evidentiary backbone of the election—ballot images, logs, tapes, surveillance video, and voter-history records—was so badly compromised that key outcomes are now "functionally unauditable and therefore unreliable as a matter of national security."

"As this record shows, you cannot call an election 'secure' if you cannot reconstruct what the machines did, who changed which ballots, or where hundreds of thousands of ballots came from," the report states.

Readers can download the full report and its detailed appendices at **ElectionCrimeBureau.com/Evidence**, where each finding is organized, classified, and backed by primary-source references.

Ten distinct attack vectors

The report identifies **ten interlocking attack vectors** through which the 2020 election infrastructure has been manipulated, shielded from scrutiny, or both.

1. Election Record Integrity (Attack Vector 01)

The report catalogs dozens of instances where voter rolls, ballot images, adjudication logs, memory cards, tally tapes, drop-box videos, and voter-history records were missing, destroyed, wiped, or never produced in key jurisdictions. It highlights that federal law requires preservation of federal election records for 22 months and documents large-scale non-compliance.

"Michigan counted 499,850 more ballots than voters. Pennsylvania counted 155,053 more. In Fulton County alone, 22,534 more ballots were counted than voters recorded. Each discrepancy independently exceeds its state's margin of victory."

2. Electronic Voting System Integrity (Attack Vector 02)

The report shows that voting systems in multiple states were operated outside their certified configurations, including uncertified software updates, extreme error rates, weak or shared passwords, plaintext encryption keys stored next to votes, and auto-overwriting logs.

"319 classified-severity vulnerabilities. Suppressed for 22 months. Those machines are still certified. They will be used in 2026. The question is not whether they were vulnerable in 2020. The question is whether they are vulnerable today."

3. Election Results Certification Integrity (Attack Vector 03)

The report details irregularities in certification, including certifications under duress, over unresolved discrepancies, and in some cases contrary to statutory requirements and canvassers' written objections.

"Certification was not a checkpoint — it was a closing mechanism. In every decisive battleground state, officials certified results over missing records, statutory violations, mathematical impossibilities, and canvassers operating under duress. The last institutional brake on a defective election was never applied; it was bypassed, coerced, or falsified out of the way."

4. Judicial Malfeasance (Attack Vector 04)

The report dissects the "64 cases lost" narrative, separating procedural dismissals, voluntary withdrawals under sanction threats, and a small number of cases that reached limited discovery.

"They didn't need to rig the count. They needed the pre-election challenge to be too early, the post-election challenge to be too late, the discovery request to be denied, the forensic sample to be too small, the protocol order to never arrive, and the attorney who kept filing to lose her license. By the time the public was told the courts found no evidence, the courts had made certain they never would."

5. Information Control (Attack Vector 05)

The document outlines how officials, agencies, and platforms coordinated a unified “most secure election in history” narrative even as internal risk reports (e.g., CISA’s TLP-AMBER summaries) showed hundreds of critical vulnerabilities and active exploitation.

"A federally certified critical-infrastructure system is resilient only if its public so that its courts and its Congress can see and debate its actual performance. When the government classifies the vulnerability data, suppresses the opposition research, censors the witnesses, and designates the questioners as terrorism threats — it has not secured the election. It has secured the narrative."

6. Financial Influence (Attack Vector 06)

The report describes how targeted private funding streams skewed resources toward select counties and operations, creating asymmetric leverage over how elections were run in key metros.

"Treasury OFAC has designated Cartel de los Soles as a Specially Designated Global Terrorist organization. If any dollar attributable to a designated foreign terrorist organization reached U.S. election infrastructure through the unverified online donation channels documented in this report, the legal exposure is not a campaign finance violation. It is material support for terrorism — up to life imprisonment."

7. Privatized Election Operations (Attack Vector 07)

Investigators show that critical election functions—data handling, network access, even control of Wi-Fi at central count locations—were handed to private vendors and NGOs, sometimes with foreign linkages.

"The voter saw a governmental election. The record shows a private organization deciding whom to hire, where to place the drop boxes, how to process the absentee ballots, who sat in the counting room on Election Night, and which records would later be available for inspection. The public paid for it. The public didn't run it. The public couldn't audit it. And the public still can't see the records."

8. Seditious Conspiracy / Congress Obstruction (Attack Vector 08)

The report argues that pre-planned disruption and security failures around January 6 effectively shut down the only remaining constitutional forum for airing election objections and evidence: the joint session of Congress.

"They war-gamed a scenario in which Congress could not count the electoral votes. They pre-mapped the Capitol. They trained activists to block the National Guard. They excluded credentialed observers from the counting rooms. They destroyed the records afterward. And then they told the country the election was the most secure in history."

9. Weaponization of Government (Attack Vector 09)

The dossier documents how whistleblowers, attorneys, cyber experts, and local officials who tried to preserve evidence or raise alarms were threatened with sanctions, targeted for prosecution, or stripped of credentials.

"The subpoenas were defied. The logs were cleared. The whistleblowers were interrogated. The auditors were threatened. The lawyers were indicted. The clerk who saved the server image was prosecuted. The officials who deleted the files were not. At every level, the power of government was not directed at the question of what happened — it was directed at the people asking it."

10. Foreign Interference (Attack Vector 10)

The report assembles findings of foreign-linked access, infrastructure, or influence: foreign IP artifacts on election devices, foreign-hosted vendor infrastructure, and statutory frameworks that were never invoked despite credible risk.

"The machines contained Chinese components. The data center ran on Huawei. The code was maintained in Serbia. The poll-worker files lived on a server in Beijing. The CIA analysts declined to report Chinese interference — in writing, on the record, for political reasons. By every measurable layer of the system, a foreign adversary had access. The only layer that didn't function was the one designed to detect it."

Key message for skeptics

This report does not ask you to agree with every conclusion. It asks you to look at the records that were deleted, the logs that are missing, the statutes that were ignored, and the national-security standards that were violated—and to decide whether ‘no evidence’ is an honest description of that record.

Direct all press inquiries to media@electioncrimebureau.com