Mesa County Security Breach: An Examination of the Claims – Full Explanation

The Mesa Reports, a set of documents authored by individuals conducting what they described as a "forensic examination" of Mesa County's voting systems, claim to show evidence of illegality and vulnerabilities. However, official investigations and professional analyses by actual election experts found no such evidence. They determined that the authors either fundamentally misunderstood or deliberately misrepresented election procedures, system functionality, and the law, producing half-truths, falsehoods, and fundamentally flawed conclusions.

Executive Summary

The Mesa Reports attempt to undermine confidence in Colorado elections by making false or misleading claims about election technology and procedures. A thorough review reveals:

- Report #1: Falsely claims the Trusted Build deleted election records that were not otherwise retained. In reality, all legally required records were preserved.
- Report #2: Falsely claims Colorado systems were uncertified, that Wi-Fi connectivity existed, and that unauthorized software was installed. In reality, the lab Colorado uses for testing was EAC-accredited, Wi-Fi was permanently disabled, SQL Server/SQL Server Management Studio (SSMS) was a part of the certified suite, and the Colorado Department of State approved the use of LibreOffice.
- Report #3: Falsely claims "unauthorized databases" existed in adjudication. In reality, the databases were normal, authorized election management system (EMS) functions. The issue stemmed from staff error troubleshooting, not malicious code, and all ballots were accounted for.
- Report #4: Falsely claims election records were destroyed, reports were created illegally and misrepresents voting patterns as fraud. In reality, all legally required records were preserved. Generating reports before Election Day is not illegal unless results are released. Claims of "unusual patterns" overlook Colorado's nonpartisan local elections and its demonstrated history of ticket splitting, e.g., voters supporting liberal candidates while opposing tax increases.

Why the Mesa Reports Gained Traction

The Mesa Reports did not emerge in a vacuum. They surfaced in a national climate of skepticism about election integrity, fueled by baseless fraud claims following the 2020 presidential election. This environment, amplified by social media and other on-line platforms, created a receptive audience for distorted narratives about voting systems.

The reports' authors, with no background in election administration, demonstrated a fundamental misunderstanding of how certified election systems and laws operate. Lacking both expertise and context, they misinterpreted normal procedures as irregularities and misrepresented lawful system behavior as evidence of wrongdoing. Rather than allowing facts to shape their analysis, they selectively highlighted isolated data points to fit a preconceived narrative of fraud.

Former Mesa County Clerk Tina Peters further amplified these false claims. By portraying herself as a whistleblower, she lent the reports a veneer of insider credibility that was later disproven by subsequent investigations, analysis, and actual election experts. Her actions, including disabling security cameras and allowing unauthorized access to voting equipment, were found by a Mesa County jury to violate multiple state laws. The reality is Tina was not a certified Colorado elections administrator, in violation of Colorado election rule, lacked the understanding of basic law and system operations, and failed to recognize that her staff had preserved all records required for retention for both the 2020 Presidential Election and the 2021 Grand Junction Municipal Election.

Social media accelerated the spread of the reports' falsehoods. Sensationalized excerpts were widely shared without context, reaching audiences unfamiliar with Colorado's rigorous election safeguards. Public distrust, often rooted in the complexity of election technology, was exploited by those seeking to erode confidence in legitimate outcomes. This narrative later gained additional public traction when Peters used the reports as central evidence in her 2022 campaign for Secretary of State, giving them political amplification they would not have achieved otherwise.

Colorado's election officials continue to counter these false narratives through transparency and education, inviting public observation of logic and accuracy testing and other election processes, while highlighting the many layers of security throughout the election process. These ongoing efforts ensure that voters can see for themselves the professionalism, accountability, and accuracy that define Colorado's elections.

Summary of Mesa Reports

The Mesa Reports misrepresent routine, lawful election procedures as evidence of crimes that never occurred.

Report #1: Data Deletion

Mesa Report Claim	Facts & Official Findings
Trusted Build deleted election records.	The Trusted Build is a controlled, state-supervised procedure in which new voting system software and firmware, certified by the State of Colorado after testing by a federally accredited Voting System Testing Laboratory (VSTL), are installed, ensuring only approved versions of software are present. These updates are necessary to improve system functionality and security and are a routine, standard process in election administration. All required election records are preserved before the process begins, and every step is logged and witnessed by authorized personnel. The files cited in Mesa Report #1 were routine Windows operating-system event logs that are automatically overwritten by the system. This normal computer behavior is not evidence of deletion or tampering. Operating system logs are not election records. Under federal law (52 U.S.C. §20701), state law (C.R.S. §1-7-802), and election rule (Colo. Election Rule 20.10.2), election records include ballots, CVRs, chain of custody documentation, audit logs, etc., not operating system files. Election records are preserved every election and again before the Trusted Build takes place.
Conclusion	Report #1's central claim is incorrect. There was no fraud, no destruction of election records, only incorrect legal interpretation.

COLORADO COUNTY CLERKS ASSOCIATION

Report #2: Certification, Wi-Fi, LibreOffice & SQL Server

Mesa Report Claim	Facts & Official Findings
Systems not certified because VSTL accreditation expired.	Only the Election Assistance Commission (EAC) can revoke accreditation (52 U.S.C. § 20971). Accreditation does not expire automatically. C.R.S. §1-5-608.5 and Colo. Election Rule 21 require accredited labs and standards. EAC never voted to revoke accreditation of PRO V & V, the VSTL Colorado uses. The EAC has confirmed this.
Wi-Fi components present. Systems connected to internet.	C.R.S. §1-5-616 and Colo. Election Rule 20.5.3(a)(1) prohibits voting systems from being connected to the internet. The Wi-Fi capability was disabled and verified in BIOS/firmware during the Trusted Build.
Microsoft SQL Server/SSMS unauthorized software	SQL Server/SSMS is a critical component for the Dominion EMS, especially for the adjudication process. It was disclosed, tested, and certified under Colo. Election Rule 20.2.
LibreOffice unauthorized software.	Under Colo. Election Rule 20.5.3 (d), a clerk may install software on the voting system if directed to or approved by the Secretary of State. Mesa County had Secretary of State approval to install LibreOffice
Conclusion	Report #2's claims are baseless. The VSTL was accredited, no WI-FI was functional, SQL was certified. LibreOffice was approved.

Report #3: Adjudication & Databases

Mesa Report Claim	Facts & Official Findings
Unauthorized databases created; not caused by human action.	The "unauthorized databases" were not unauthorized at all. They were routine functions of the certified Election Management System. The Mesa County District Attorney's opened a separate investigation into the claims made in this report. Backed by video evidence, staff interviews, and a recreation of events, they confirmed the extra databases were created by human action when the Elections Manager attempted troubleshooting during adjudication. This was a user mistake, not a hidden algorithm or malicious software. This new database was a normal function of the voting system. Importantly, Mesa County staff verified that all ballots were fully accounted for using system backups required pursuant to federal law (52 U.S.C. §20701), state law (C.R.S. §1-7-802), and election rule (Colo. Election Rule 20.10.2).
Database anomalies indicated possible vote flipping or adjudication bias. Changes in adjudication not logged.	Adjudication is the process used to resolve questions about voter intent on paper ballots that the scanner could not read automatically, for example, when a voter crosses out a choice or makes stray marks. Bipartisan election judges review the original ballot image and determine voter intent, with all actions logged and audited. Mesa Report #3 misrepresented this routine, transparent process as evidence of vote manipulation, when in fact every adjudication action was recorded, auditable, and reviewed by bipartisan judges. All adjudication records were present and fully accounted for when cross-checked against system backups and corresponding ballot images.
Conclusion	Report #3's claims are incorrect. There was no fraud, no malicious code, no unauthorized databases. Only staff error. Report shows willful misrepresentation or lack of understanding of election systems by report authors.

Report #4: Logs & Record Retention

Mesa Report Claim	Facts & Official Findings
Cast Vote Record and Election Night Reporting files were generated six days before Election Day, proving a violation of law and an indicator of fraud.	The mere generation of Cast Vote Record (CVR) or Election Night Reporting (ENR) files within the voting system is not a violation of law. What matters is whether any results were prematurely disclosed to the public. Colorado law (C.R.S. § 1-7.5-107.5) permits counties to begin ballot processing before Election Day, provided that no information concerning the count is released before 7:00 p.m. on Election Day. The distinction is clear: generating internal reports for administrative or technical purposes is lawful; releasing results early is not.
Trusted Build destroyed election records (logs).	Operating system logs are not election records. Under federal (52 U.S.C. §20701) and Colorado law (Colo. Election Rule 20.10.2), election records include ballots, CVRs, chain of custody documentation, audit logs, etc., not operating system files. Election records are preserved and retained before the Trusted Build takes place.
Unusual voting patterns	Unusual voting patterns are not fraud. The report's so-called "Voter Defection Analysis" ignores that Colorado municipal elections are nonpartisan and voter behavior in local races often diverges from partisan patterns. Audits confirmed the results. Furthermore, Colorado voters often support liberal candidates statewide and federal contests and yet vote against tax increases. This claim continues to demonstrate how little the authors understand elections and voting tends/behaviors
Conclusion	Report #4's claim is misleading. No destruction of election records, no illegal activity, no early release of results.

Defense-in-Depth Safeguards

The Mesa Reports present isolated technical claims while ignoring the broader defense-in-depth security ecosystem that protects Colorado elections. By focusing on isolated technical details, the authors miss the point: Colorado's safeguards operate as a layered, interlocking system. No single safeguard stands alone. Our election system is secured by multiple, overlapping layers of protection designed to detect and deter problems at every stage. These checks work together to create transparency, accountability, and resilience, none of which the Mesa Reports even acknowledge. Worse, the authors repeatedly misstate basic election law and misunderstand how certified voting systems function, leading them to draw false and misleading conclusions. Colorado's defense-in-depth safeguards include, but are not limited to:

- **Air-gapped Infrastructure** – The Election Management System (EMS) is physically isolated from the internet and external networks. Any data transfer (e.g., results uploads) occurs via secure, removable media under strict chain of custody.
- **Ballot Cure Process** – Colorado voters are notified if their ballot envelope signature is missing or does not match their voter registration record. Voters can "cure" their ballot by providing identification or confirming their signature through multiple methods, including online, by mail, or in person, up to eight days after Election Day. This process ensures every eligible voter has the opportunity to have their ballot counted while preventing fraudulent ballots from being accepted. Any signatures that remain unresolved after the cure period are referred to the district attorney for investigation.
- **Ballot Tracking** – Voters can track their ballot from mailing to acceptance, providing transparency and confidence.

COLORADO COUNTY CLERKS ASSOCIATION

- **Bipartisan and Multipartisan Election Judges** – Citizens from both major parties, and in some counties, minor parties as well, serve as judges to process ballots, verify signatures, conduct ballot adjudication, and oversee every step of the election, ensuring transparency and shared accountability.
- **Canvass Board**s – Bipartisan boards, with political party appointees, certify the accuracy of every county's results.
- **Chain of custody** – Every ballot and piece of equipment is tracked, with bipartisan verification.
- **Continuous Video Monitoring** – Cameras record election facilities, 24-hour ballot boxes, and ballot processing areas 24/7.
- **Criminal Background Checks for Election Personnel** – Colorado law mandates criminal history checks for election judges and staff who handle voting systems, ballots, or voter data; clerks must verify that workers have not been convicted of election offenses or fraud before granting access.
- **Cybersecurity Partnerships and Testing** – Colorado election officials partner with the respected third parties to conduct vulnerability scans, phishing-resistance testing, and cyber-hygiene assessments that help identify and mitigate threats before each election.
- **Election Official Education and Training** – Colorado requires all election officials to be certified by the Department of State before conducting their first election, ensuring they understand election law, security, and procedures. The state also conducts annual trainings and tabletop exercises to help officials prepare for potential issues and maintain readiness across all aspects of election administration.
- **Incident Response and Continuity Planning** – Each county maintains written plans to ensure elections continue in the event of a cyber incident, physical security incident, natural disaster, or power outage.
- **Logic & Accuracy Testing** – Before every election, counties test each voting system component to ensure ballots are read correctly and that the equipment accurately records and reports every possible vote combination.
- **No QR code-based tabulation** – Colorado prohibits the use of QR codes for tabulating ballots and instead requires that all ballots be counted using only the human-verifiable marks (ovals), enhancing transparency and auditability.
- **Open Records and Transparency** – Colorado's open records laws ensure that ballots, ballot images, cast vote records, and other election materials are available for public inspection after each election. Many counties go a step further by posting ballot images and cast vote records online at no charge after each election.
- **Physical Security Assessments** – Colorado requires every county election office to undergo regular third-party physical security assessments to identify and mitigate potential risks to election facilities. These independent reviews help ensure that ballot processing areas, storage rooms, and voter service centers meet rigorous security standards and best practices.
- **Political Party/Public Observation** – Political party-appointed watchers and media may observe election processes, including ballot counting and audits.
- **Public Logic and Accuracy Test** – A public event that allows citizens and parties to see the equipment function correctly before the election. Political party appointees serve on testing board.
- **Restricted Access to Secure Facilities** – Only credentialed staff, election judges, and watchers may enter under strict controls. Access to different areas strictly controlled by roles.
- **Risk-Limiting Audits** – Paper ballots are checked against results to guarantee accuracy. Political party appointees participate in this process in every county.
- **Separation of Duties** – No single person has control over critical processes; tasks are distributed among bipartisan teams.
- **Signature Verification** – Bipartisan election judges verify every mail ballot envelope signature against the voter's registration record.
- **State Oversight** – The Secretary of State's office enforces uniform standards, monitors compliance, and conducts audits.
- **Trusted Build** – Ensures only certified software/firmware is installed and verified on every voting system.

- **Voting Systems Are Tested and Certified –** Colorado certifies all voting systems used in the state through Voting System Test Laboratories (VSTLs) accredited by the U.S. Election Assistance Commission (EAC). These systems are tested to rigorous federal standards and must also meet additional state-specific requirements established under Colorado law.
- **Voter List Maintenance and Data Matching** – Colorado conducts continuous voter list maintenance. Data comes from the Department of Motor Vehicles, the U.S. Postal Service's National Change of Address (NCOA) system, Department of Corrections felon status records, state vital records for deaths, Social Security Administration data, and voter-initiated changes. Counties also use undeliverable election mail and returned ballots to identify voters who may have moved, ensuring timely updates and confirmations.
- **Voter-verified Paper Ballots** – Every voter marks a paper ballot that can be audited and recounted, independent of electronic systems.

These layers demonstrate that Colorado's defense-in-depth model extends across technology, personnel, and planning, ensuring that even if one safeguard fails, others prevent, detect and help recover from any compromise. By disregarding these systemic protections, the Mesa Reports misrepresent isolated procedures as vulnerabilities, while ignoring the redundant safeguards that make Colorado's elections among the most secure and transparent in the country.

Tina Peters' Conviction

Former Mesa County Clerk Tina Peters was not a whistleblower or a defender of election integrity. She was convicted in 2024 of multiple felonies and misdemeanors for her role in a deliberate security breach of Mesa County's election equipment. A jury of her peers in conservative Mesa County found her guilty after hearing the evidence, proving that the only criminal conduct tied to Mesa County elections at that time came from Peters herself, not from the election systems or processes.

Specifically, Peters was convicted of:

- Three felony counts of attempting to influence a public servant.
- One felony count of conspiracy to commit criminal impersonation.
- One misdemeanor count for official misconduct—abuse of her office to violate election security protocols.
- One misdemeanor count for violation of duty—failing to uphold the laws and responsibilities of her office.
- One misdemeanor count for failure to comply with Secretary of State rules and directives.

At the same time, it is critical to note what Peters was not convicted of:

- She was not charged with preserving or backing up election records or making an image of her voting system. Her election team had already retained election records.
- She was not acting under any legal duty or authority to copy the system. No statute, rule, or court order required or authorized her actions. Her conviction was for violating security controls and falsifying access, not for preserving evidence that her staff had already lawfully retained or performing any duty required of a clerk.

Peters' actions went far beyond mistakes or misunderstandings. She actively deceived her staff, the public, state officials, and her fellow clerks by:

- Turning off cameras monitoring secure election areas.
- Falsifying government documents to give access to an imposter.
- Sneaking that imposter in on a weekend to image the voting system equipment.
- Failing to require the imposter to sign a contract protecting voters' personal identifiable information and confidential records.

None of these acts had to be done under the cover of deception. That same year, at approximately the same time, Larimer County worked openly with the Secretary of State to back up non-required Windows operating system logs. They followed the law and demonstrated that transparency and cooperation were always available options.

The defining contrast: 63 other Colorado clerks understood their systems, upheld their oaths, and complied with state and federal law. Tina Peters was the only clerk who chose to break the law to pursue an unnecessary and unlawful course of action.

It is also essential to understand where her accountability lies: Peters was prosecuted and convicted in Mesa County District Court under Colorado state law.

- Her convictions were for state, not federal crimes.
- Only the Governor of Colorado has the authority to pardon or commute a state sentence.
- The President of the United States has no power to pardon or alter her sentence.

Peters' case underscores a simple but vital truth: the Mesa Reports did not expose systemic fraud or misconduct. The only criminal conduct in Mesa County at that time was led by Tina Peters. Colorado's election systems and processes have consistently been proven secure, transparent, and accurate.

Conclusion

The Mesa Reports present a distorted and incomplete picture of Colorado's elections. By focusing on misrepresented technical details and presenting them in a deceptive way, the authors attempt to manufacture doubt where none exists. These reports are not evidence of fraud or misconduct, but examples of misunderstanding ordinary processes and mischaracterizing lawful procedures.

Colorado elections are built on a foundation of accountability and transparency, with multiple, overlapping safeguards that prevent, detect, and correct errors at every stage of the process. The Mesa Reports never acknowledge these protections, but the facts are clear:

- No election records were destroyed.
- No uncertified systems were used.
- No part of the voting system was connected to the internet.
- No unauthorized databases were created.
- All ballots were properly accounted for.
- No election results reports were created illegally
- Elections in Mesa County are accurate and secure.

The only proven criminal activity in Mesa County elections during this time was committed not by the election systems or staff following the law, but by former Clerk Tina Peters, as determined by a jury of her peers.

By contrast, Colorado's election officials continue to conduct elections with transparency, accountability, and the highest professional standards. The defense-in-depth model, ranging from restricted access and chain of custody to risk-limiting audits and canvass board certifications, ensures that every eligible voter can have confidence that their ballot is counted as cast.

In short, the Mesa Reports are not evidence of wrongdoing. They are evidence of malinformation, information that is based on fact but is deliberately presented out of context, distorted, or used in a misleading way to cause harm to people, institutions, and/or public trust. These documents misrepresent technical details, present them deceptively, and ignore the broader safeguards that make Colorado's elections among the most secure and trusted in the nation.