

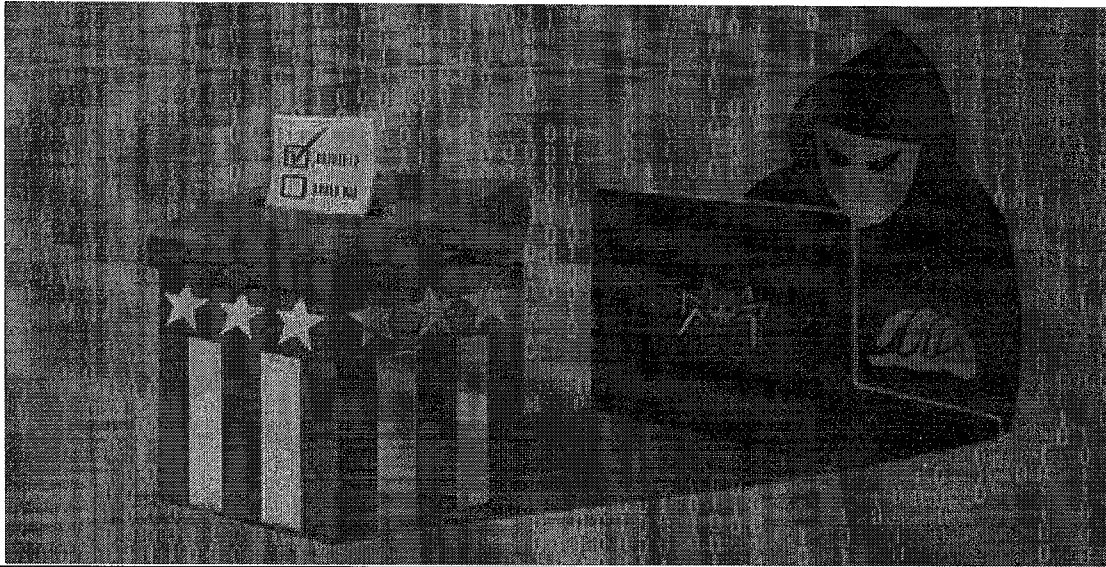
2024-03-12 Bill Wiesner to LC-BOC regarding Safety Net

#1.



Ban All Voting Machines-Hand Count Elections!

Take Action Now



3,490,831
Actions Taken

The Voting Machines Must Go! Secure One Man, One Vote by 2024!

Most local election officials at the county level have the power to opt for hand-count elections and set aside all voting machines and electronic devices before the 2024 election!

Hand Count Elections Are Simple, Reliable, Affordable, and Within Reach! Let's Restore Conventional Elections with hand-count, paper ballot, in-person, at precinct elections, county by county.

Americans deserve security, accountability, transparency, and accuracy in elections.

-Every voting machine and tabulator can be hacked within 1-7 minutes, in person or remotely, altering vote tallies without detection, if a machine plugs into a wall, regardless of internet connectivity, an intrusion is easy.

-State and Government websites have been accessed by domestic and foreign hacking including the central tally of votes and, intrusions like this, are often not discovered for a year or more with most virtually undetectable.

It's a disgrace for lawmakers to continue to defend the impossible and blatantly false claims that voting machines are safe and secure!

Time to end the reign of machines and put elections back into the hands of We the People today!

"America will never be destroyed from the outside. If we falter and lose our freedoms, it will be because we destroyed ourselves."

-Abraham Lincoln

#2. Professor Alex Halderman hacks Dominion Computer in seconds with a ballpoint pen.

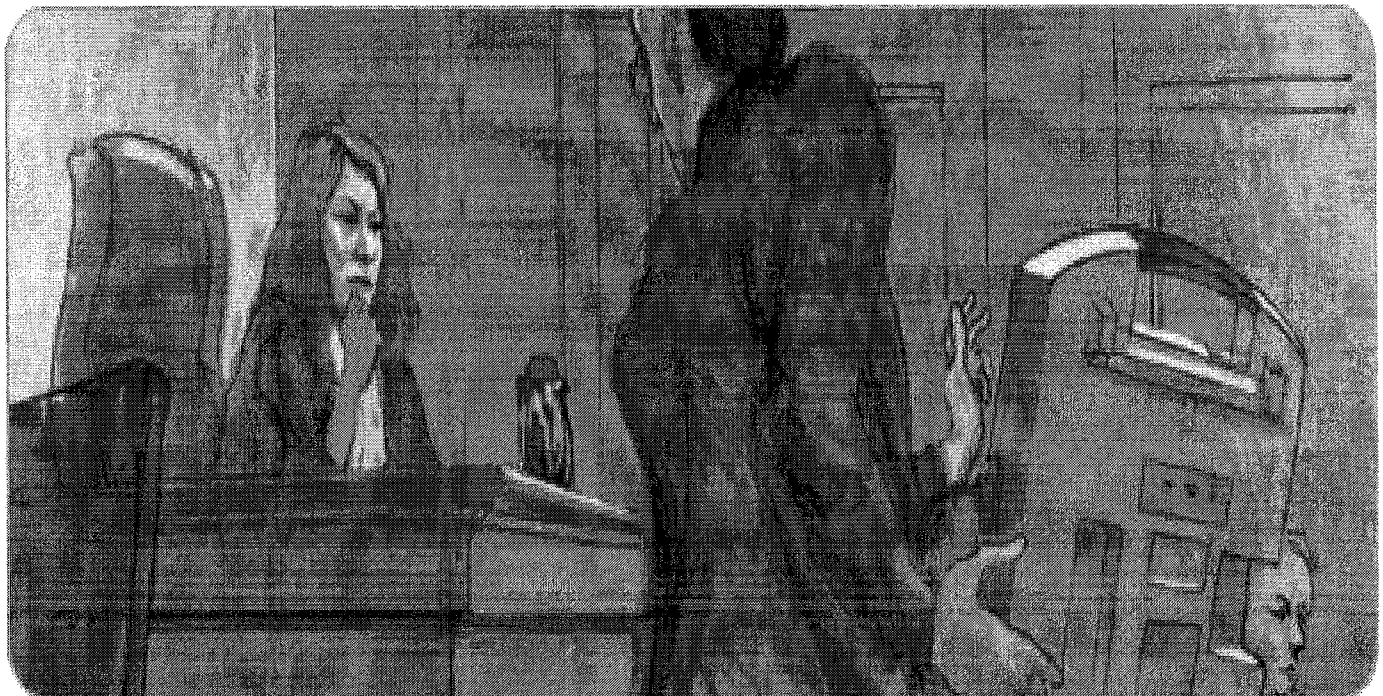


John Basham

@JohnBasham



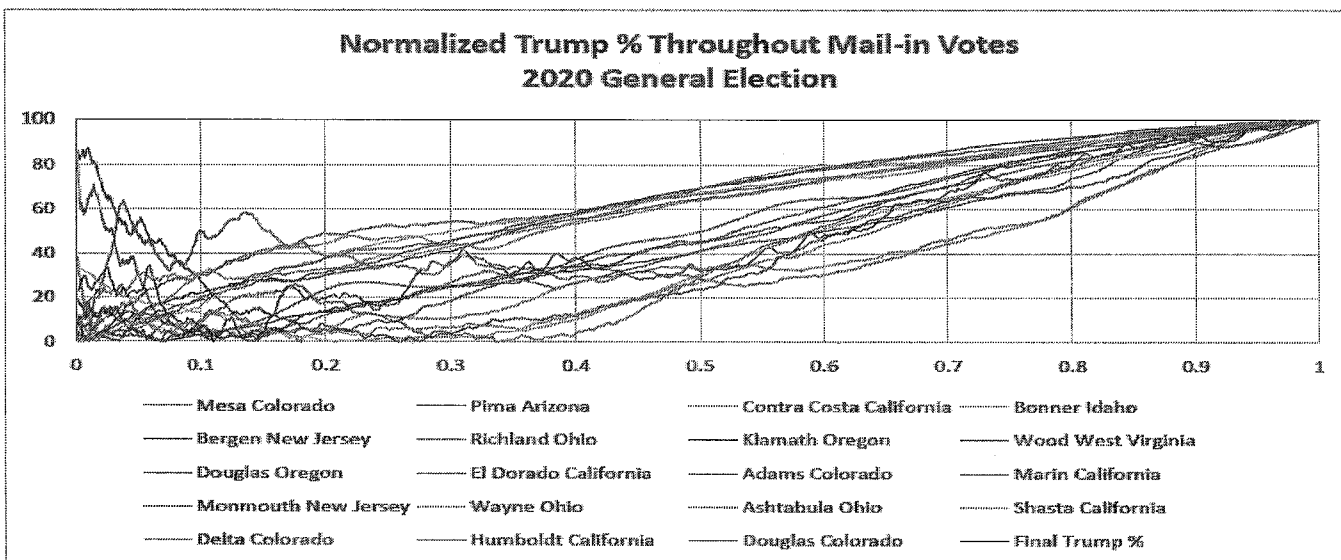
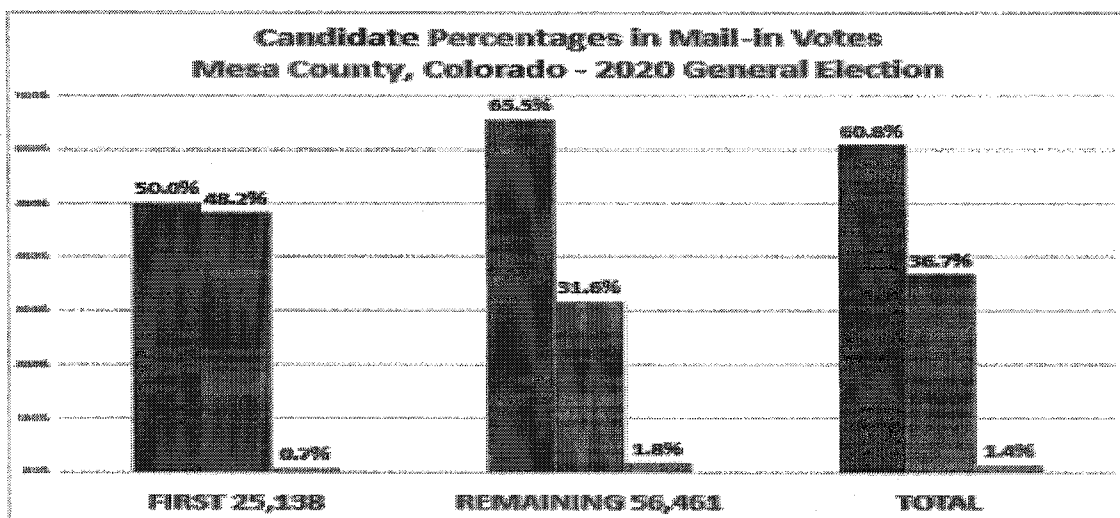
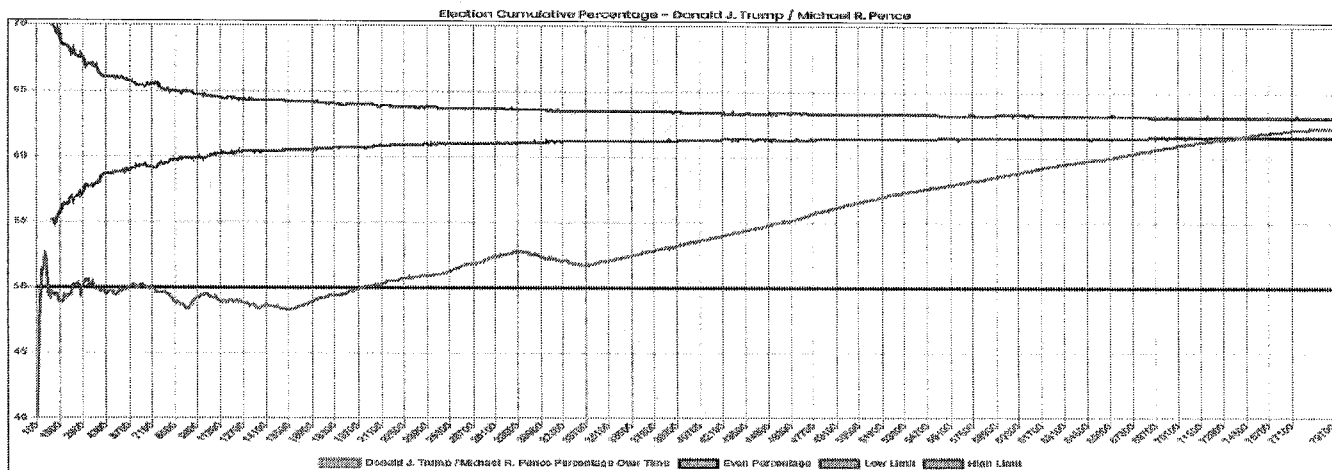
BREAKING: In A Federal Court In Atlanta Georgia On Friday J. Alex Halderman (@jhalderm) Was Able To HACK A DOMINION VOTING TABULATOR In Front Of U.S. District Judge Amy Totenberg USING ONLY A PEN TO CHANGE VOTE TOTALS! This Is Part Of A Long Running Lawsuit By Election Integrity Activista Set As A Bench Trial. Plaintiff's Seek To Remove What They Say Are Insecure Voting Machines In Georgia In Favor Of Secure Paper Ballots.



5:57 PM · Jan 20, 2024 · 3.1M Views

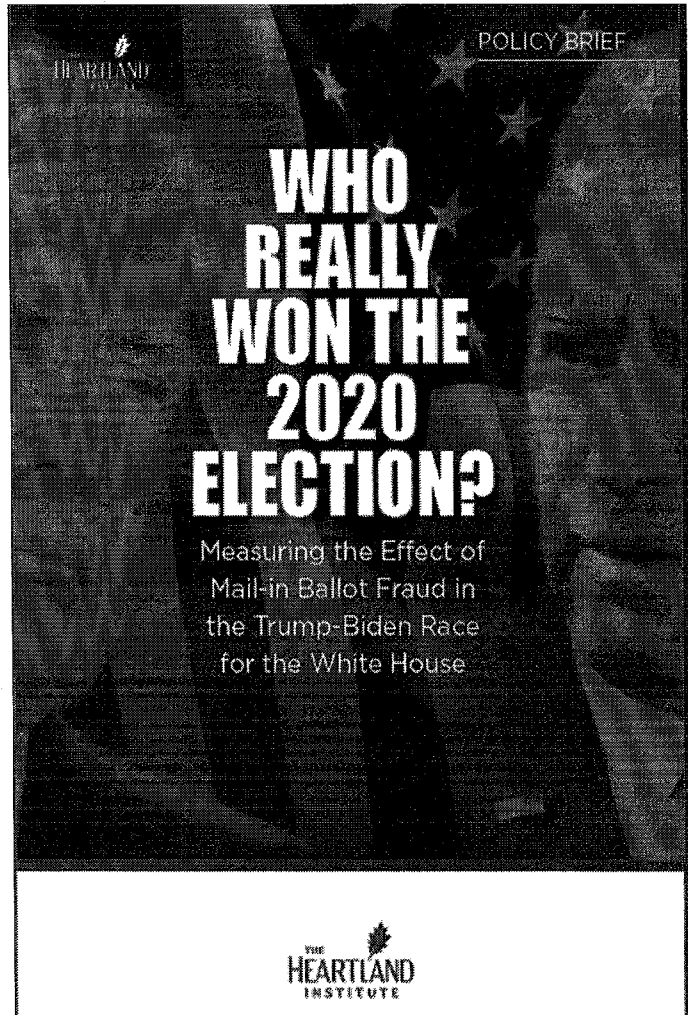
#3. Cast Vote Records prove machine fraud: The Mesa Pattern – Mesa County Colorado – Tina Peters County Clerk

Below is the percentage plot of President Trump's mail-in votes in Mesa County, CO during the 2020 General Election.



#4 ~61% of Leelanau County votes cast in the February 27, 2024 election were Mail in Ballots.

- 21 percent of mail-in voters admitted that they filled out a ballot for a friend or family member
- 17 percent of mail-in voters said they signed a ballot for a friend or family member “with or without his or her permission.”
- 19 percent of mail-in voters said that a friend or family member filled out their ballot, in part or in full, on their behalf.



<https://heartland.org/who-really-won-the-2020-election/>

#5 Linda Rantz in Missouri

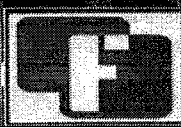
TPACTION.COM/DONATE

Common Myths

Costs too much
 Less Accurate
 Takes too Long
 Not Enough People
 Only Works for Small Counties



Help Save Our Country Go To Lindellplan.com
 Donate At LindellOffenseFund.org or 800-598-6747
FRANKSPEECH.COM Roku Apple TV androidtv



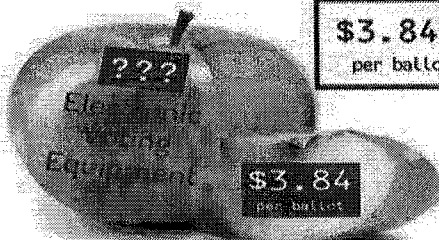
TPACTION.COM/DONATE

Apple-to-Slice Comparison

Osage County MO • <10,000 Voters • 4-year Cycle



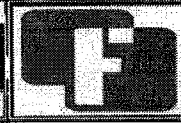
\$2.71
per ballot



\$3.84+
per ballot

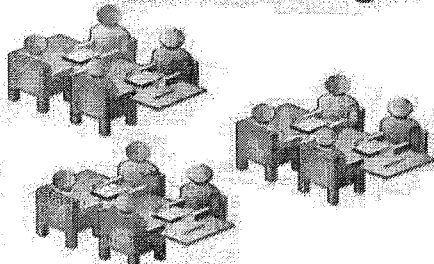


Help Save Our Country Go To Lindellplan.com
 Donate At LindellOffenseFund.org or 800-598-6747
FRANKSPEECH.COM Roku Apple TV androidtv



TPACTION.COM/DONATE

Counting Team 4 Election Judges



Team Scheduling

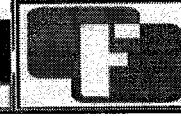
600 ballots/poll place
= 1 Team

Up to 1,200 ballots/poll place
= 2 Teams




Up to 1,800 ballots/poll place
= 3 Teams







Help Save Our Country Go To Lindellplan.com
 Donate At LindellOffenseFund.org or 800-598-6747
FRANKSPEECH.COM Roku Apple TV androidtv



TPACTION.COM/DONATE

 APRIL 2023 ELECTION 	
Osage County, MO <10,000 Registered Voters Westphalia Polling Place 481 Ballots Cast 1 Team Counted in 5 hours	St. Charles County, MO ~292,000 Registered Voters 115 Polling Places (PP) 83 PP <481 ballots / 1 Team 32 PP <1K ballots / 2 Teams Could count in 5 hours
 Help Save Our Country Go To Lindellplan.com Donate At LindellOffenseFund.org or 800-598-6747 FRANKSPEECH.COM Roku Apple TV androidtv	

TPACTION.COM/DONATE

Continuity of Government 	 PLANT A VICTORY GARDEN 
 Help Save Our Country Go To Lindellplan.com Donate At LindellOffenseFund.org or 800-598-6747 FRANKSPEECH.COM Roku Apple TV androidtv	

#6 – www.FrankSpeech.com/LetMyPeopleGo -- 2hour 17 minute DVD proving Election Machine Fraud:



Watch it FREE Online on RUMBLE by simply typing: "Let My People Go". Watch the 2-hour 18-minute version.

(Ask me for a free DVD copy if you can't watch it online.)

#7 Dr. Douglas G. Frank

Nine Michigan Counties

Collected Demographics for
Populations, Registrations, & Ballots

with Statistical Confirmation of Algorithm Use

November 2020 United States General Election

Douglas G Frank, PhD
4/6/2021

General Conclusions

- Voter registration is consistently near, or exceeding county population demographics.
- There are over 66,000 ballots recorded that are not associated with a registered voter in the October database.
- The ability to predict ballot demographics with such remarkable precision (average correlation coefficient of $R = 0.997$) demonstrates the activity of a regulating algorithm.
- This confirms, as seen in several other states, that ballots are being harvested at the precinct level, regulated at the county level, and determined at the state level.
- The degree of precision observed confirms that algorithms had access to voting databases and voting activity before, during, and following the November 3, 2020 election.

"Correlation Coefficient, R"

A statistical value that indicates how well a set of values predicts a target set of data.

$R = 1.000$ The target set is precisely correlated

$R = 0.000$ The target set is not correlated at all (random)

$R = -1.000$ The target set predicts the opposite result

Correlations involving human behavior rarely have R values greater than 0.8

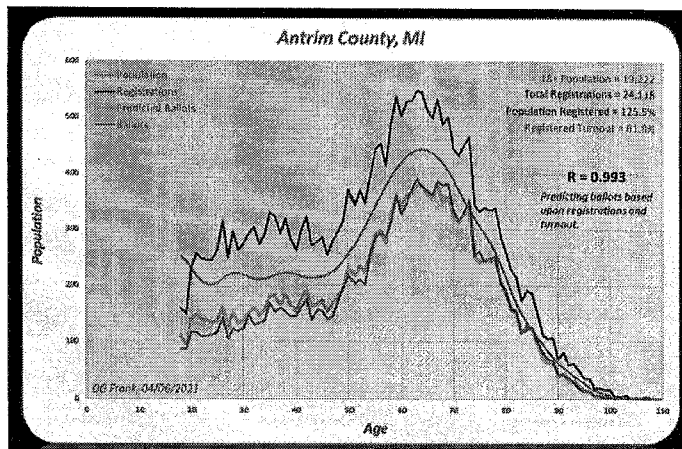
Predicting Ballots with the Registration Key

(In decreasing order by population)

R	County Name
0.999	Wayne County
0.999	Oakland County
1.000	Macomb County
0.999	Kent County
0.999	Livingston County
0.996	Grand Traverse County
0.996	Barry County
0.995	Charlevoix County
0.993	Antrim County

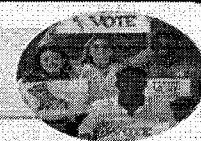
"That ain't natural, buddy."

0.997 Average Correlation



Follow the Data with Dr Frank

Proposal 2 Of 2022



In November 2022, Michigan voters overwhelmingly passed Prop 2. This Constitutional Amendment enhances the security of our elections and safeguards the voting rights of all Michiganders. The provisions outlined in Prop 2 are now in effect. These provisions include:

"The State with the Worst Elections"

I'm often asked which states are making the most progress toward election integrity. Most of the progress I've seen is at the grassroots level. There are a few states making small, incremental legislative improvements... some tinkering at the edges, but nothing substantial.

But Michigan elections are probably the WORST in the country. Not only are their courts corrupt and their grassroots efforts diverted and ineffective, but with the passage of Prop 2 (2022) their legislature has basically guaranteed that every future election will be teeming with election fraud.

Michigan clerks are mostly hypnotized, unqualified, and unaware, and their citizens are ignorant and compliant.

I say again: the key to fixing our elections is not legal nor legislative. Instead, the fix is local. Citizens need to awake to their spiritual and constitutional duties and reclaim their local elections.

Until then, without miraculous intervention, we are lost.

👍 55 🗳️ 22 🗳️ 14 🗳️ 4 ❤️ 2

👁️ 3382 Dr Frank, 1:40 PM

11 comments

#8. www.TinaPeters.USA Mesa County Colorado Forensic Reports: Report #1a:

EXECUTIVE SUMMARY

This report documents initial findings in an ongoing forensic examination of the voting systems of Mesa County, Colorado, used in the November, 2020 General Election. These voting systems represent a portion of overall election systems infrastructure, and this report is limited to the findings of an ongoing investigation. The findings in this report were prepared by the cyber forensic expert retained to advise the County Clerk pursuant to her duties as the county's Chief Election Official as part of the impacted parties' legal team.

Federal law requires the preservation of election records – which includes records in electronic or digital form – for twenty-two months after an election. Colorado law requires the preservation of election records for an additional three months beyond the Federal requirement. The obligation to ensure the integrity of elections and that all election records are preserved pursuant to federal and state law falls to the elected Clerk & Recorder. This report, the first of several, is based on examination of the data obtained from forensic images of the Dominion Voting System EMS server last used in Mesa County for the November, 2020, election, images taken in furtherance of the preservation requirements of federal and state law. Based upon information received by the Clerk's office from various sources in early 2021, the Clerk became concerned that the voting system modifications might jeopardize these preservation and other legal requirements under the responsibility of the County Clerk. For this reason the Clerk ensured a full backup of election records from the County voting systems, both before and after the software modification performed by the vendor and the Secretary of State on May 25-26, 2021, just six months after the November, 2020, election.

Forensic examination¹ found that election records, including data described in the Federal Election Commission's 2002 Voting System Standards (VSS) mandated by Colorado law as certification requirements for Colorado voting systems, have been destroyed on Mesa County's voting system, by the system vendor and the Colorado Secretary of State's office. Because similar system modifications were reportedly performed upon county election servers across the state, it is possible, if not likely, that such data destruction in violation of state and federal law has occurred in numerous other counties.

The extent and manner of destruction of the data comprising these election records is consequential, precluding the possibility of any comprehensive forensic audit of the conduct of any involved election. This documented destruction also undermines the conclusion that these Colorado voting systems and accompanying vendor and Colorado Secretary of State-issued procedures could meet the requirements of Colorado and Federal law, and consequently vitiates the premise of the Colorado Secretary of State certification of these systems for use in Colorado.

Two backup images, using forensic imaging methods, were obtained from the Dominion Voting Systems (DVS) Democracy Suite (D-Suite) Election Management System (EMS) Standard Server in Mesa County, Colorado. The first image was made of that EMS Standard Server in the D-Suite 5.11-CO version configuration, as used in the November, 2020 election. The second image was of the configuration of the EMS Standard Server in the D-Suite 5.13 version configuration, following the modification of the EMS Standard Server by a combined team of DVS vendor personnel and Colorado Secretary of State staff. The forensic information provided in this report is presented using screenshots from forensic analysts' systems running industry-standard forensics software tools. The report includes "before" and "after" screenshots from the forensic tool that shows the differences between the two backup images.

The forensic examination found that numerous logfiles had been deleted or overwritten. These logfiles are required to reconstruct the function of and events taking place on the the voting systems, and based upon information

¹ Many individuals and organizations, some public officials, have made recent claims that no audit performed nor examination conducted on elections or computer-based election systems can be legitimate or credible unless the examiners are "election experts" or accredited election auditors. There is no such thing as an "accredited election auditor," nor are there Federal standards or procedures to credential election auditors.

Report #1b:

provided by legal counsel, must, by law, be preserved. By comparing filenames in the two images (before and after the Dominion update on May 25-26, 2021), examination and analysis identified a total of 28,989 files that were deleted. During a software update, some replacement of program files and their related content is normally expected. However the examination found that 695 log and event log files necessary for the determination of election integrity were deleted.

Based upon information provided by legal counsel, Colorado law (Colorado Revised Statute (CRS) § 1-5-601.5) requires that, prior to use in Colorado elections, electronic and computer-based voting systems be certified by the Colorado Secretary of State. This certification is based on the systems' compliance with the requirements of the Federal Election Commission's 2002 Voting System Standards (VSS), verified by their testing by a Federally-accredited (by vote of the U.S. Election Assistance Commission (EAC)) Voting System Testing Lab (VSTL). While several iterations of newer Voluntary Voting System Guidelines (VVSG) have been issued by the EAC, Colorado's statutory requirement is for compliance with 2002 VSS, which states:

"Election audit trails provide the supporting documentation for verifying the accuracy of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation."

The relevant sections of the VSS are cited in Appendix E.

These statutory requirements establish that voting systems are required to generate and preserve, as critical to the ability to determine and reproduce the conditions and details of election conduct using these systems, logfiles of all system functions, including normal activity, connectivity, file and data access, operator- and automated-processes, and errors. Logfiles are critical to the ability to detect improper operation, including the ability to detect malicious intrusions as well as other improper activities and conditions, and configuration changes that could enable alteration of the actual vote count.

Assuming this information to be correct, this forensic examination found that a substantially large number of these requirements have not been met. This examination also found that destruction of critical logfiles has occurred. This destruction is not incidental or minor but is extensive.

The purpose of this initial report is to document these findings and present preliminary evidence demonstrating unacceptable conduct and system defects revealed by the examined images, as necessary for the Chief Election Official to discharge her statutory obligations. The facts and resultant findings support the conclusions that:

- 1) Election-related data explicitly required to be preserved, as stated in the 2002 VSS criteria referenced in this section, have been destroyed in violation of Federal and State law, and
- 2) Due to non-compliance with the 2002 VSS requirements, these voting systems and accompanying vendor-provided, Colorado Secretary of state-approved procedures cannot meet the certification requirements of the State of Colorado, and should not have been certified for use in the state.

Comprehensive investigation is required to determine whether these critical failures are the result of malicious intent or negligence, and to what extent the systems may have been compromised or subjected to unauthorized access or operation prior to, during, and after election use. That comprehensive investigation is *beyond the scope of this report*. Subsequent reports will address these issues in detail.

Evidence supporting all of these findings is documented in this report.

Report #1c:

Introduction

Election officials, including Secretaries of State, are obligated by law to ensure the integrity of all elections, including the transparency required for citizens to verify that integrity themselves. Modern electronic voting systems are marketed as an efficient solution to streamline the voting process and allow for automated collection, tabulation, and reporting of election results, but the efficiency they promise comes at a cost.

The necessary measures and safeguards to ensure the integrity of the systems and their operation against a severe, mounting and ever-evolving threat from sophisticated nation-state and non-nation-state actors are so complex and dynamic as to outpace the limited capabilities and resources of our government, at all levels. While minimal security safeguards may be within government capacity, modern computer-based voting systems are extremely complex and difficult to secure, even for cybersecurity experts, and since voting systems are not under the direct control of the Federal government's top security experts, any government assurances about the sufficiency of those safeguards can serve only to mislead citizens and policy-makers. Even critical defense systems, relentlessly monitored and defended by highly-trained teams using costly, sophisticated tools, are at risk and are frequently compromised, sometimes before procurement. Earlier generations of voting systems relied on simple, human-scale safeguards, for example "air gaps"—that is—to have no wired network connection to the system. But miniaturized wireless communication technologies and networks have proliferated, with billions of wireless devices installed or in use, and malicious actors have developed sophisticated attacks to bypass air gaps, compromise every kind of hardware, firmware, and software, often before they even come into customer or user possession, and to move laterally through networked systems, often undetected. Supply-chains for these systems, from the initiation of the design of integrated circuits and electronic components, most manufactured overseas with little U.S. insight or oversight, through the fabrication, testing, assembly, integration, and operation of these complex composite systems, are vulnerable and untrustworthy for critical functions of government and lucrative economic and national security targets. For all these reasons logfiles, such as those that have been deleted by the Dominion "Trusted Build" update must be preserved to document the complete operation of the computer system and voting applications, and to be able to verify the authenticity, integrity and accuracy of the vote.

The feature size of individual circuits in the chipsets and components of our voting system computers is at the nanoscale, smaller than the smallest known virus particle, and less than 3/10,000ths of the width of a human hair. So we have lost the ability, if we ever had it, to visually verify what is really happening, even at the physical level, in our computer-based voting system. Regardless of how the systems appear to be configured to authorized users and poll-watchers, the functionality and connectivity in these computers can be enabled and modified remotely and wirelessly, or by the introduction of embedded codes on scanned paper, or triggered by specific unforeseeable and indiscernible predetermined software and hardware conditions, or by specific timing events, or by geographic location, or by the proximity of other devices or combinations of any of these means.

Report #2:

Critical Discoveries

This report details the following critical discoveries regarding Mesa County's voting system:

- Uncertified software installed, rendering the voting system unlawful for use in elections.
- Does not meet statutorily mandated Voting System Standards (VSS) and could not have been lawfully certified for purchase or use.
- Suffered systematic deletion of election records (audit log files required by Federal and State law to be generated and maintained), which, in combination with other issues revealed in this report, creates an un-auditable "back door" into the election system.
- Violates Voting Systems Standards ("VSS") which expressly mandate prevention of the ability to "change calculated vote totals." This report documents this non-compliance from the logged-in EMS server, from a non-DVS computer with network access, and from a cell phone (which may be possible if any of the 36 internal wireless devices in voting system components are deliberately or accidentally enabled and a password is obtained).
- Mandatory VSS "System Auditability" required features are disabled.
- Is configured with 36 wireless devices, which represent an extreme and unnecessary vulnerability, and which may be exploited to obtain unauthorized access from external devices, networks, and the Internet.
- Is configured through firewall settings to allow any computer in the world to connect to the Election Management System (EMS) server.
- Uses only a Windows password with generic userIDs to restrict and control access.
- Contains user accounts with administrative access that share passwords, subverting VSS-required user accountability and action traceability controls.
- Uses a self-signed encryption certificate which exposes the system to the risk of undetected compromise or alteration.

Report #3a:

EXECUTIVE SUMMARY

This report documents the findings of an examination of tabulated vote databases based on forensic analysis of the drive image of Mesa County, Colorado's Dominion Voting Systems (DVS) Election Management System (EMS) server. The findings in this report were prepared by the authors as consultants to the legal team representing Tina Peters, the Mesa County Clerk and Recorder, pursuant to her statutory duties as Mesa County's Chief Election Official. The findings provide evidence of potentially unauthorized and illegal manipulation of tabulated vote data during the 2020 General Election and 2021 Grand Junction Municipal Election. Because of this evidence, which led to the vote totals for those elections being impossible to verify, the results and integrity of Mesa County's 2020 General Election and the 2021 Grand Junction Municipal Election are in question.

This analysis was performed using the forensic image of the EMS server, which was backed up before Colorado Secretary of State and DVS overwrote the hard drive with D-Suite version 5.13.

Findings and Implications:

- 1) There was an unauthorized creation of new election databases during early voting in the 2020 General Election on October 21, 2020, followed by the digital reloading of 20,346 ballot records into the new election databases, making the original voter intent recorded from the ballots unknown. In addition, 5,567 ballots in 58 batches did not have their digital records copied to the new database, although the votes from the ballots in those batches were recorded in the Main election database.
- 2) The same unauthorized creation of new election databases occurred during the 2021 Grand Junction Municipal Election on March 30, 2021, followed by the digital reloading of 2,974 ballot records, making the original voter intent recorded on those ballots unknown. In addition, 4,458 ballots in 46 batches did not have their digital records copied to the

Report #3b:

new database, although the votes from the ballots in those batches were recorded in the Main election database.

- 3) The absence of secure hash algorithm (.sha) files for each digital ballot image makes the authenticity of each digital ballot image, and the ballot-level record for those ballots, impossible to verify.
- 4) The true total vote count in Mesa County, Colorado cannot be accurately calculated for the 2020 General Election or the 2021 Grand Junction Municipal Election from records in the databases of the county's voting system.
- 5) There is 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 to occur, especially within the time frame that these events occurred. Given the complex sequence of data manipulations and deletions necessary to produce the digital evidence described in this report, this combination of events could not have been the result of either deliberate or inadvertent actions by those officials.
- 6) 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, including the batch and ballot records that evidenced the creation of new databases and reprocessing of ballot records described in Findings 1 and 2 above. This destruction of all data by the trusted build is described in the "Mesa County, Colorado Voting Systems Forensic Examination and Analysis Report".
- 7) The fact that such ballot record manipulation has been shown demonstrates a critical security failure with the DVS EMS wherever it is used. The manipulation would not be identifiable to an election official using the voting systems, nor to an observer or judge overseeing the election conduct, much less to citizens with no access to the voting systems; without both cyber and database management system expertise, and

Page 4 of 87

unfettered access to database records and computer log files (many of which were destroyed by the actions of the Secretary of State) from the EMS server, the manipulation would be undetectable.



