

LIBERTY LIONS LEAGUE

29 September 2023

The Honorable Senator Mike Thompson and
Members of the 2023 Special Committee on Elections
Kansas State Capitol
300 SW 10th St.
Topeka, KS 66612

RE: Election Voting Machines

Dear Senator Thompson and members of the Special Committee on Elections:

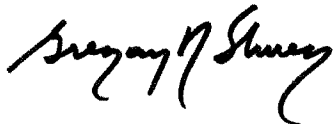
The question of vote integrity in the use of voting machines has long been a national issue raised by citizens and political figures of all persuasions. But today it has become a serious issue with the international threats and capabilities of foreign adversaries and others to interfere with our elections. Despite proclamations to the contrary, some 60% of the voting public do not believe our elections are secure.

The issue of machine integrity is a volatile one with adamant supporters on one side who declare that machines and the election system currently employed are adequately tested and proven to be safe, and ardent proponents on the other side who present reams of evidence and years of tests and testimony showing that machines are not secure and cannot be made secure by their very nature.

What must be done to resolve this problem and to ultimately provide an unquestionably fraud-proof system to ensure our most sacred right – the vote – is protected is to discard political rhetoric and obtain and evaluate hard facts. This is not a political issue. It is one of national and constitutional importance for it is not the voter who can determine an election, it is – as Joseph Stalin once noted – the person who counts the votes – if the system is corrupt. Our country cannot exist as a constitutional republic if we cannot guarantee that every vote counts as intended by the voter.

Attached is only a small sample of identified issues that support the call to eliminate machines and return to paper ballots. This is being accomplished in certain parts of this country and other countries as well. Kansas must follow.

Respectfully,



Greg Shuey, Founder
Liberty Lions League

Atch: Election Integrity Issues in Kansas

Election Integrity Issues in Kansas

A Citizens' Call for Insuring Election Integrity

**Presentation to the
Kansas Special Committee on Elections**

29 September 2023

Election Integrity Issues in Kansas

A Citizens' Call for Eliminating Voting Machines

INTRODUCTION

This document provides just a sample of the many issues discovered with voting machines and is intended to dispel the vast amount of disinformation being served to: 1) Suppress actual facts that dispute the widely proclaimed mantra that election machines are secure and can be trusted to deliver accurate votes as selected by the voter; and 2) Dissuade appropriate officials from eliminating at least one serious potential for manipulating elections, namely voting machines, and to replace them with high-tech paper ballots. Not only would eliminating voting machines remove the concern and potential source for vote manipulation, but would be cheaper, faster, free of foreign involvement in the election process, and would provide for hard evidence when recounts or audits were called.

EXECUTIVE SUMMARY

Despite a national coordinated disinformation campaign to deny such, the 2020 Presidential election revealed a great many problems with our election process and equipment to a greater or lesser extent in all 50 states. Fox News contributor and author Molly Hemmingway's investigation, documented in her book *Rigged*, revealed this has been going on as a well-orchestrated process for at least 40 years. Peter Navarro's national investigation exposed 30 different methods used to corrupt elections. Jovan Pulitzer's analysis of Arizona and other states' ballots confirmed violations of state laws that allowed large amounts of fraudulent ballots to be counted. Dr. Douglas Frank's analysis of counties across the U.S. proved there was an algorithmic process that illegally flipped or added ballots so as to cause a preferential outcome. Several forensic analyses by expert cyber groups exposed the fact that voting machines and Pollpad devices used across the country have Internet connections that are illegal; and that hacking into these devices was not only a trivial matter but was done routinely during elections. Bev Harris showed in 2002 that software in election machines use an algorithm that fractionalizes votes, retains and later releases them flipping enough of these fractional votes to the selected candidates to give them a late-night win. Seth Keshel's analysis of election trends showed that election outcomes (e.g., abnormal numbers of registrations, abnormal numbers of votes, and election outcomes) were so outside of historical patterns as to be statistically nearly impossible. Mike Lindell revealed cyber captures of large foreign vote insertions into state elections, enough to flip elections in some cases. Finally, massive numbers of reports of irregularities have been reported after recent elections that give strong evidence that our elections are not secure and may have resulted in flipping outcomes.

Despite the above reports and identified problems, it is not the intent of this report to relitigate any past election but rather to address one particular problem, voting machines. That is because more than a decade of analyses and tests, and highly suspicious and statistically nearly impossible outcomes have been recorded that suggest we cannot have assurance our elections are safe when our votes are digitized, encrypted and placed into a system where so many opportunities exist for bad actors to change or destroy them. Thus, our recommendation is to eliminate voting machines and return to paper ballots as some counties in the U.S. and some foreign countries are now doing.

ELECTION INTEGRITY ISSUES

National Investigations: A great deal of suspicion about election integrity began long ago from both parties as well as with many private citizens. Thousands of “irregularities” during the 2020 election not only caused serious concerns but prompted some investigations, all of which were opposed, attacked or even thwarted by officials from both parties. The question always left unanswered is why would anyone oppose an investigation into serious election “irregularities” if they were confident there was none? In nearly every case where investigations were conducted, serious violations of election laws or procedures and, in certain cases, outright fraud were discovered corroborating early suspicions.

Multiple investigations by independent parties and highly experienced technical teams have proven we do not have safe and secure national elections. It is currently unknown to what extent that problem exists in Kansas. However, to take a piecemeal approach and legislate election law changes here and there without conducting an extensive overview of our state’s entire election process, and without consideration of the many problems now being identified in other states, is imprudent at best. Furthermore, to believe that Kansas will not be a target for increased efforts to subvert and manipulate our elections is naïve. This document intends to give ample reasons to protect our elections by eliminating voting machines.

ELECTION MACHINES

History of Voting Machine Companies: Voting machines used in Kansas come from three major suppliers. Due to their tendency to launch egregious lawsuits on anyone daring to question their products, their names will not be used. However, public reports may be found identifying them or their equipment as the subject of the particular investigations or discoveries made.

There is a long, incestuous relationship with these companies since electronic voting was launched with the Help America Vote Act of 2002. Also, there is a history of buyouts and consolidations among several of these companies which raises the question of software collaboration. However, most concerning is that there are reports that 75% of voting machines used in this country are reportedly sold by companies owned by a Chinese government-owned company. In addition, much of the hardware inside the machines (including the microprocessors used for machine operation) is made overseas, much from Chinese companies. At the very least, this means that our elections are potentially compromised just by voting machines alone.

Complexity and Foreign Control: The U.S. election system is extremely complex and complicated, including problems with who owns what, who controls what, who validates what, and how it operates. It is easy to believe that some of this was intentional because such complexity lends itself to large numbers of vulnerabilities and opportunities for bad actors and organizations to exploit them. One indication that this is probably true is the clamor raised when objections are raised about outdated registration rolls, illegal voters, unmonitored ballot drop boxes, and violations of election laws and procedures.

Cursory investigations of the election system and its major players show potentially compromised instances and conditions. Just to name two, the encryption of a voter’s marked ballot into a QR code that the machine can read violates the legal requirement for the voter to know that his vote is properly recorded since he cannot read a QR code. Secondly, the fact that vote tallies are sent overseas to a foreign company that is recording votes nationally, offers the opportunity for intrusion into the final results. And it begs the question of why processing of our votes in a foreign country is necessary.

The bottom line is that it is very difficult to determine and compile all pertinent facets of our national election process because of its extreme complexity. This is not just a research problem. It is a serious integrity one because it lends itself to many opportunities to exploit vulnerabilities and for bad actors to control election outcomes. Hundreds if not thousands of articles, investigations and reports have been written detailing serious irregularities, many of which have been identified as major examples of probable election fraud. If compiled, there is little doubt the report would be larger than several major novels combined. The point is that if we are to ensure vote integrity, the system complexity must be reduced and returned to a

simple process of one-day direct voting, preferably by high-tech paper ballot only at controlled voting locations with vote aggregation being done exclusively at the state level and nationally aggregated in country.

Forensic Analyses vs. Contracts: Investigations of suspected sources of voting machine “irregularities” have been constantly thwarted by one principal reason: Voting machine suppliers all of whom have contracts that forbid any investigation or analysis of their equipment or software. While protective provisions of a contract are reasonable when trade secrets are involved, scanning, summing, recording and reporting accumulating votes are trivial software operations that a first-year computer science student could write. The egregious terms of these contracts seem to be designed to prevent the investigation of software that may go beyond mere accumulation and reporting votes. In fact, from forensic audits and test results performed to date by computer specialists and even from company confessions, it is all but certain these egregious contract covenants are intended to prevent discovery of software that could potentially manipulate votes.

Voting Machines Operation: Electronic voting generally involves voting (touchscreen) machines where the voter touches a screen to record his votes. After confirming the machine has recorded all votes correctly, the voter selects a record button after which the machine prints the votes on a strip of paper along with a QR code. The paper is then recorded by a second tabulating machine which reads and logs the votes defined in the QR code. There is no way to tell if any votes were encrypted accurately or were changed and recorded as such in the QR code. Likewise, as there are numerous servers involved in the national election system ranging from the tabulating machine all the way to the servers located in Secretaries of State offices, and servers in Barcelona, Spain, and Frankfurt, Germany, all of which are involved in our election, there is no way to know if or to what degree any votes have been destroyed, added or changed somewhere in that chain. This is because the whole process is deemed to be secure but without forensic investigations proving such. To suggest it is not secure brings massive condemnation from those defending the process, a signal that something not kosher is being protected.

The machine industry has created an electronic voting system sold as a convenience to the voter; yet the election process in which these machines are integral has many points of potential entry or sites of potential manipulation that make the entire system ripe for election manipulation. Extensive forensic analyses by computer experts such as Prof. A. J. Halderman, Ph.D., computer analyst James Thomas Penrose, and others have exposed numerous vulnerabilities in current voting machines. Halderman found no less than eight major vulnerabilities that could be exploited by a bad actor with limited computer skills in just one brand of machines alone. These could be accessed both through software additions during company system upgrades, wireless access via modems, or from firmware embedded in the machine’s microprocessors.

J.T. Penrose actually found two IP addresses in his testing of a particular machine, one of them being located in Taiwan, that essentially confirmed the machine had Internet connectivity. This capability potentially allowed a foreign actor to have direct access to anything internal to the machine, including the ability to change votes.

Great efforts by the manufacturers, the media and political players have been made to vociferously confirm these systems are safe. Yet numerous reports, forensic audits, and direct evidence from election results indicate exactly the opposite. A fundamental question is why expensive voting machines are needed when a paper ballot and pen can accomplish the same thing at much lower cost. The often-cited answer is that machines speed up the counting process. And yet, many states do not certify their results until days after the election. So is the use of vulnerable machines worth the risk when issues like frequent delayed outputs of results, high initial costs, and maintenance and overhead costs of using them are common downsides?

EXAMPLES OF MACHINE ISSUES

Hiding the Issues: It is commonly held by those who have little knowledge of or interest in investigating election machine issues that they do not exist or that, as a minimum, they are inconsequential. From just the last three years of investigation by many, many people who made objective analyses of machines, this has

been found to be not true. In fact, the opposite is actually the case. But there is great interest from various parties to ensure this false belief is maintained, all to ensure that machines are kept in place for various reasons, the most egregious being the ability to control election results. Since proponents of machines are quick to suggest, without proof to arguments to the contrary, that “election deniers” (as they like to discredit investigators and integrity skeptics) have no proof that machines are insecure, this paper includes just a few of many, many examples that prove otherwise.

INTERNET CONNECTIVITY

Internet Connectivity: In most states, election machines are not supposed to be connected to the Internet for obvious reasons. As with any computer that can be hacked so that its contents are accessed, stolen or changed, Internet connectivity would give a bad actor the ability to gain access to election results and easily change them if there were Internet connectivity. One might think that would be inconsequential for just one machine. But the problem is that malware can easily be introduced into one machine that could affect every machine with such connectivity. In other words, it is possible for one person, even of limited computer skills, to change the election outcome in a single precinct, a county and even a whole state with Internet connectivity merely by infecting one machine. Of course, the mantra is that “none of our machines are connected to the Internet.” Unfortunately, this hearsay is believed without supporting internal investigation by officials of what is inside the machines.

Evidence of Internet Connectivity: Voting machines used in Kansas have long been touted as being not connected to the Internet. Yet the supplier of one of those machines confirmed in congressional testimony that it has a modem on the motherboard of its machines. As confirmed in a document available upon request, this provides Internet capability between voting systems and election servers which is NOT authorized by Kansas law. While certain officials in Kansas are adamant that Kansas machines are not connected, if a modem is resident in these machines, there is no guarantee they have not nor will not be connected wirelessly to the Internet. And there is no way to confirm the existence of these modems without a forensic analysis even though a photo publicly available shows this modem on this particular motherboard.

Internet Vulnerability Examples: Various public demonstrations have proven that voting machines can be easily accessed by hackers via wireless connectivity. This could not happen if: 1) There was no Internet connection; and 2) The systems were ultra-secure. Numerous examples over recent years have shown how quick and simple hackers wireless access machines can be made. Here are just a few recent examples:

- At one hackers’ convention, teen boys successfully broke into a voting machine in only 15 minutes.
- At the Lindell Symposium in 2021, hackers were invited to electronically attack a machine intentionally setup as if it were ready for an election. The first hacker broke into the machine’s operating system and logged on as an administrator in merely five minutes using only his cellphone.
- During the 2020 Election, cyber experts reported logged intrusions from 68 different countries flipping a total of 13,405,062 votes. They reported that Kansas had 112,708 votes flipped. This would not be possible if somewhere in the system there was not a vulnerability via Internet connectivity.

MACHINE SOFTWARE ISSUES

Software Vulnerability: Many analyses have been reported citing a number of different malware programs that have been developed specifically to control the outcome of an election by vote manipulation in machines.

1. One of those was created in a foreign country specifically to ensure victory for a certain presidential candidate. It was so successful that it was repeatedly used and gave more than 90% of the votes to the presidential victor and his successor.

2. Fraction software was developed to change a vote into ten decimalized votes (i.e. ten 0.1 votes), store them, and allocate them throughout the election day to selected candidates who needed small increases to eventually win.
3. UC Berkley Professor of Statistics, Philip B. Stark, analyzed one system and determined it “could be maliciously programmed or hacked to create an entirely fraudulent machine-marked ‘paper ballot’ because the machine includes an option that allows the voter to automatically cast the ballot without first printing and inspecting it.” Princeton University Computer Science Professor Andrew Appel also corroborated this and dubbed it ‘Permission to Cheat.’ Appel found that a machine from a different supplier had the same defect. Appel said “these machines could still be programmed or hacked to fraudulently fill in undervotes (races that voters left blank) with no possibility of detection in a manual audit.” This additional defect is called a ‘Ballot Stuffing’ defect and has been confirmed by Professor Richard DeMillo, Georgia Tech’s former Dean of Computing and Director of its Information Security Center. These independent confirmations of this one vulnerability alone compromise the entire Kansas election system if it exists in Kansas election machines. The only way to confirm this is by forensic audit of the software and firmware by competent independent experts.

There are numerous other malware versions that have been used and employed on a global scale to control election outcomes. Why this is not widely known is because of two reasons: 1) Those employing such malware make great effort to hide it by proclaiming there is no election fraud and attacking anyone who claims otherwise; and 2) All of these malicious programs are quite small, are embedded within the machine code and either eliminate themselves upon command or at a specific time and date, or are protected from discovery by prohibitions to forensically investigate machine code. Since no one can see any malicious code much less get access to analyze it, even if it did not self-destruct after the election, claims that it exists are easily overwhelmed by official declarations it does not exist. And yet these defenders cannot prove their assertions because they too have not done forensic analyses and are merely taking the word of the suppliers.

Ballot-alternation by Adjudication: One major assumption too often relied upon is that election workers are all honest people. Unfortunately, that is not the case. Despite best efforts, and as criminal cases for election fraud have shown, some people will gain positions within the elections process specifically to commit violations of election laws in support of their preferred candidate or party. Adjudication is one favorite means to do that. And some software has been found to facilitate that whether by accident of intention. The process works this way. If a voter scribbles or marks his ballot so that the machine cannot easily read his intention, it rejects the ballot. Also, if scanning settings in the machine are set too restrictively*, whether by accident or intention, it may reject more ballots than is acceptable (which is 1 in 250,000 by federal standards). That rejected ballot is handed to a ballot adjudicator who fills out a new ballot with votes selected to match, to the best of the adjudicator’s knowledge, the intent of the voter. However, a bad acting adjudicator will select the candidates they want regardless of the voter’s intent. Since the newly adjudicated ballots may be separated from the original, the voter’s selections would be essentially zeroed out by votes for a different candidate in the new ballot. While adjudication logs are usually created to ensure proper adjudication, bad actors may find ways to circumvent the procedure to achieve their aims.

Abnormally High Adjudication Rates: One Michigan county’s very abnormal results led to investigations which revealed that the software had a 68% error rate (federal limits are .0008%). This resulted in a staggering number of adjudicated ballots. Investigators concluded the machines were intentionally designed to increase adjudication rates. Multiple states have reported adjudication rates of rejected ballots being much higher than normal and well over allowable limits. Considerable efforts have been made by voting machine companies and their supporters to excuse this as accidental or at least not intentional. But in a number of reports in recent elections, losing candidates had just enough votes come in at the last moment to flip elections and adjudicated ballots were often a suspicious source that all too often was not investigated.

Other Machine Issues: As previously stated, the amount of information concerning discoveries and analyses that raise serious questions about the use of machines in elections is massive. It should not be lost that these concerns have been publicly raised by both political parties for years. And it is not just a national

issue. Reports are that at least three European countries have abandoned machines and returned to paper ballots. One noted that France held a national election and counted more than 70 million paper ballots in one day. So arguments suggesting that paper ballots present too many problems are false or at least greatly overstated. Rather, paper ballots eliminate serious problems. But to continue, below are several other examples, of many, that involved machine software issues.

Data-deleting Software Updates: Reports have been made that voting machine companies were sending IT specialists or third-party contractors to install “system updates” after elections which were deleting all data records federally mandated to be retained for 22 months. This was formally documented by the clerk in one Colorado county. Since updates are frequent with voting machines and election officials seemingly never take screen shots of election files before or after elections, there is usually no indication and certainly no evidence of what has been deleted, if anything, that might contain malicious code or suspicious election results. Again, the constant mantra is that “everything is fine, there are no election issues; trust us.”

System Configuration Issues: Another reason to question the hardware and software configuration of voting machines is the following discoveries. In an Arizona audit, it was disclosed that those machines inspected had two hard drives installed. Also discovered was that both drives were bootable to different configurations, a decertifying configuration. The 2nd hard drive contained non-county data for some unexplained reason. While backup redundancy or other valid technical reasons may exist for a second drive, one consideration should be given: It is quite simple to have two operating systems in a voting machine. The first could be instructed to operate as the primary operating system up through midnight before Election Day. This system would perform exactly as required during any tests conducted to check for vote processing integrity. Then with a time/date stamp trigger, the operating system on the second drive could be instructed to takeover using vote-manipulating software (as those described below). After the election, a destruct code could then erase the 2nd software program leaving no trace of its operations. If such a system were installed, contractual requirements preventing forensic analysis would keep it hidden by denying forensic analysis. Also, post-election updates (as are now occurring around the country) could erase the second system deleting any chance of discovery if a self-destruct code was not integral to it. Though this is stated as a possibility and not a proven fact, in the absence of forensic analysis and discovery, there is no guarantee this situation does not exist in Kansas. Yet officials involved in the election process and others will quickly declare such possibility to be a conspiracy theory but yet will have no forensic evidence to disprove it.

ALGORITHM CONTROL ON ELECTION MACHINES

Voting creates a database lending itself to statistical analysis due to the extremely large population from which small-to-large data sets may be analyzed. Historically, voting patterns have very common characteristics even though there are variations in the number of voters and the popularity of candidates in any given race. In part, that means that as votes come in, the allocation between candidates usually results in relatively smooth curves because generally the percentage in favor of each candidate would relatively the same throughout the voting period. Sudden spikes for just one candidate at the beginning of the counting process can mean a large number of illegal ballots stuffed before election day while a sudden spike during the election would generally mean voting machine and election process manipulation by algorithm or other serious irregularities.

In recent elections, both of these have been witnessed and recorded from actual data (i.e., recorded votes). Were this an infrequent occurrence, it might be considered an election irregularity within a small population, perhaps in a one machine, or perhaps one precinct. But that it not the case. In fact, they have occurred in multiple states, especially at the same time as happened in early morning on post-election day in 2020. The probability of this being a coincidence in so many states at the same time is astronomically small. Rather, to the computer or software expert this is clear indication of an algorithm “managing” votes, an illegal violation of the Constitution, state and federal laws.

The following are just two examples (of many discovered) which indicate machine manipulation of votes by algorithm. The reason that the data below is not “proof” is that by legal standards actual forensic analysis of the original ballots compared to the digital output of voting machines and/or the electronic voting process would be necessary to show conclusively that votes made by a given voter did not match the votes outputted and counted by the election process. Still, statistical analysis indicates a near mathematical impossibility that the outcomes experienced happened without vote manipulation.

Texas Votes By % in 8 counties, 8 Nov 2022: Unusual results in eight Texas counties prompted an investigation of 2022 results in one election. Shown below are the interim results of this race, a snapshot of which was taken at 8:23 on election night. As may be seen in a number of pairings, the exact sample percentage of votes then counted was occurring between two candidates. This does not happen in any election and can only occur if an algorithm is preset to cause a given result by “managing” votes.

% Interm Results as of 8:23 with 75% of votes counted

(Note: Algorithm was storing and controlling allocation of votes to ensure wins)

Candidates:	Bexar	Brewster	Crane	Loving	Reagan	Sutton	Uvalde	Zavala
Gonzales (R)	38.5	37.3	81.4	74.5	80.5	76.6	44.9	39.9
Lire (D)	30.7	31.3	9.3	12.8	9.7	11.7	37.5	39.9
Lopez (I)	30.7	31.3	9.3	12.8	9.7	11.7	27.5	20.2

In the following chart, the final vote percentages were recorded. Note the significant changes which imply that the algorithm that may have been involved adjusted votes to ensure the selected candidate won apparently by reallocating some of the third-place candidate’s votes to the winner.

% Final Results provided by SecState (Algorithm adjusted results to hide manipulation)

Candidates:	Bexar	Brewster	Crane	Loving	Reagan	Sutton	Uvalde	Zavala
Gonzales (R)	54.8	52.3	84.3	85.1	75.9	83.3	60.2	34.2
Lire (D)	42.3	40.6	11.2	8.1	9.1	12.7	31.6	61.1
Lopez (I)	2.9	7.1	4.5	6.8	15.0	4.0	8.2	4.7

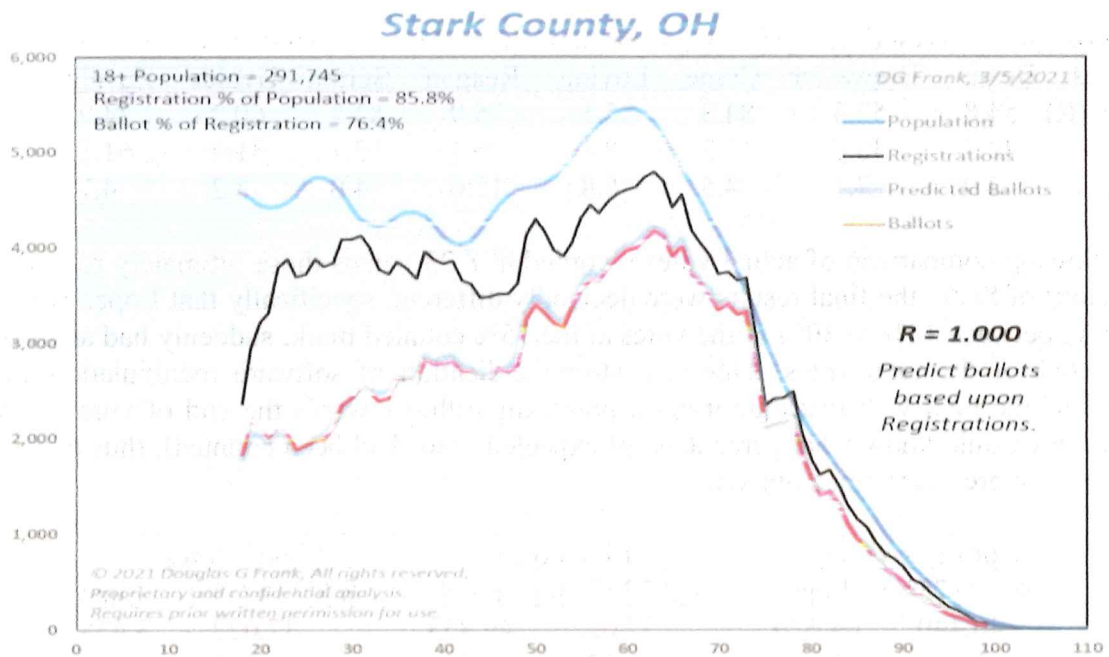
In the following comparison of actual votes recorded at 8:23 versus those ultimately reported by the Secretary of State, the final results were decidedly different, specifically that Lopez who was maintaining between 10% to 30% of the votes at the 75% counted mark, suddenly had an average of only 6.6% of the total votes. This is a strong indication of software manipulation which “adjudicates” the total vote distribution by a preset algorithm towards the end of vote counting (the algorithm would know what percentage of expected votes had been counted), thus managing the election to a pre-determined outcome.

County	Gonzales Votes		Lira Votes		Lopez Votes	
	@8:23 (75%)	Final	@8:23 (75%)	Final	@8:23 (75%)	Final
Bexar	46,440	64,620	37,022	49,853	37,022	3,458
Brewster	1,340	1,943	1,125	1,506	1,125	265
Crane	578	933	65	124	65	50
Loving	35	63	6	6	6	5
Reagan	538	538	65	65	65	106
Sutton	958	958	146	146	146	46
Uvalde	2,897	4,720	1,775	2,475	1,775	641
Zavala	808	773	808	1,381	409	107

(Note 1: The probability that any candidate would have any given percentage of votes (to one decimal place) is 1 on 1,000. The probability that two candidates would have that exact same percentage in a race is $(1/1,000)^2$ or 1 in 1,000,000. But the probability that three candidates would have identical percentages at a given time in eight counties is roughly $(1/1,000,000)^8$ or 1 in 10^{48} .)

(Note 2: Voting machines from two different companies were used in this election yet both had the same early voting results. There are only two potential ways two machines from two different companies can exhibit the same output results indicative of algorithmic manipulation: 1) The companies either collaborated or were using the same algorithm-based software; or 2) Vote manipulation was being done at a higher level in the vote processing chain.)

Stark County, Ohio: One last example is the voting data in Stark County, OH which revealed a result that is essentially statistically all but impossible to occur in a normal election. The data (shown below) shows a 1.00 correlation between registered voters and actual voters, meaning that as the actual voters (by age) were plotted versus the number of registered voters, there was a direct mathematical correlation. In other words, starting around age 40, the percentage of actual voters was mathematically fixed as a percentage of registered voters (though the actual percent changed with increasing age). In short, one could predict how many people in each certain age group would vote out of a given population by knowing (or setting) the algorithm value. Another way of saying this is that the number of voters (and their votes) were manipulated based upon the number of registered voters of each age. This is not what historically happens in voting but is precisely what can (and probably did) happen with an algorithm managing voting. The fact that this occurred in all other Ohio counties and was shown to occur across the country statistically indicates that algorithmic manipulation controlled the election.

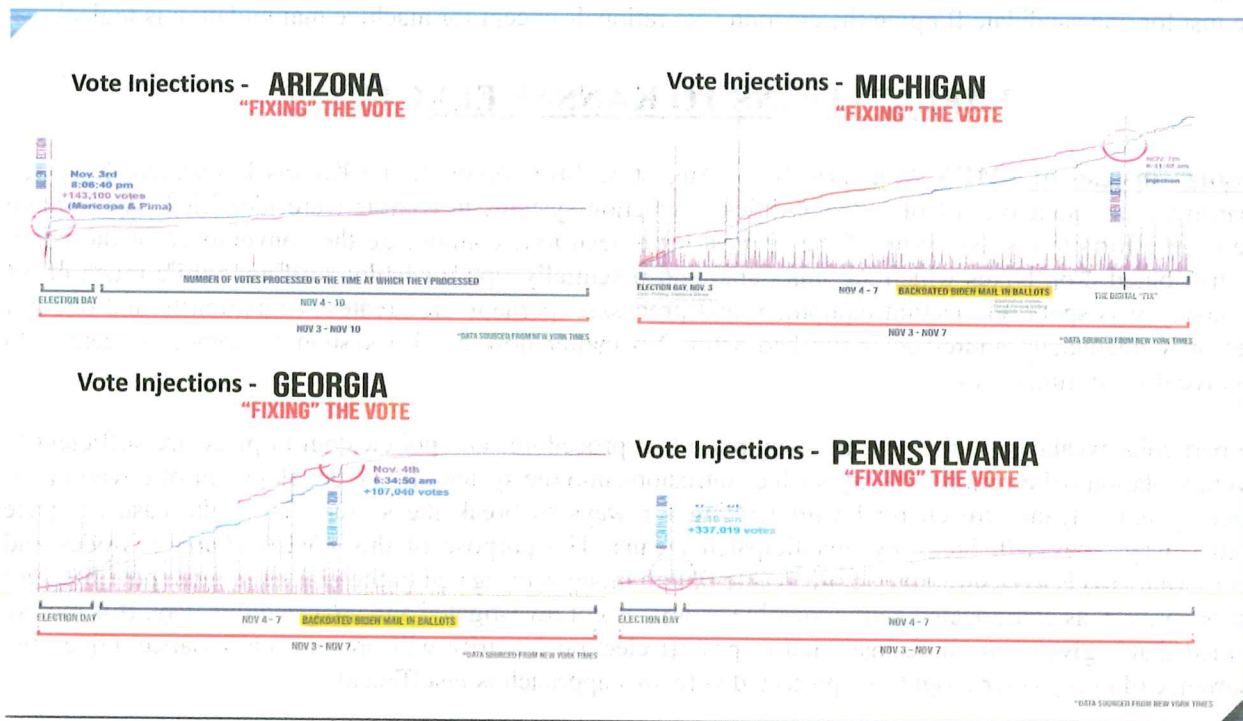


(Source: Statistical analyses of Dr. Douglas Frank who charted election results in 88 Ohio Counties and those in 45 other states and found the same pattern.)

Statistical Improbability in Five Battleground States: The above examples are only two of many that have been recorded but prevented from being presented both in the media and in court cases, generally under the judicial decision of denial because of lack of standing. Without

presentation of hard evidence, the media has taken the incorrect stance that there is no evidence of serious problems with election machines. Actually, the opposite is true. Courts have just not allowed it to be presented.

Another very prominent example of probable manipulation was evident on election eve across the country. At 11 p.m. on 4 Nov 2020, all five battleground states strangely stopped counting votes and sent poll watchers home with little explanation. This had never happened before and because states conduct their elections independently and without national coordination, except to report results, there was significant question as to what prompted this. Investigations and graphing of election data revealed that a number of states (4 are shown below) had statistically impossible spikes in new votes for just one candidate with as many as 75% to as much as 100% of the new votes being tallied being for just that candidate. This sudden and massive influx of votes flipped the election by 6 a.m. the next morning. The fact that a large number of votes would come in at one time with the large highly suspect majority being for one candidate is statistically unheard of. In fact, the probability that this would occur in multiple states in one election is again astronomically small. The fact that this occurred specifically in critical battleground states which subsequent flipped the election is essentially hard evidence of probable machine manipulation. The graphs of actual voting data of four of those key states are shown below.



CERTIFICATIONS

EAC Certifications: Federal law requires certification of voting machines. However, significant questions and lack of required documentation suggests that Kansas election machines may not have been certified in past elections. Lack of certification means that an election that uses uncertified machines cannot be certified. Numerous similar situations have been found in other states. For instance, Texas found that one machine supplier was conducting its own testing and that its hash-validation testing had not been validated as required by EAC (Election Assistance Commission). In an April 17, 2020 letter from that company to the EAC, it admitted that the EAC had not certified its machine with a modem. The bottom line is that failure by EAC to arduously ensure compliance provided a number of opportunities within the system for intrusion and

manipulation by insider threats. Instead of ensuring testing and compliance with federal laws, the EAC was taking the manufacturer at its word, that is, letting the fox confirm all the hens were safe in the hen house.

State Certifications: County election offices go through a logic and accuracy testing process to validate the security of voting machines before elections. Cases have been reported where manufacturers or their contractors provided updates to machine software after these tests were run, and without subsequent retesting. Though no evidence has been found that this created a problem or involved any malicious wrongdoing, specifically because no investigations have been conducted, if malware were to be introduced via software updates, this would logically be done after logic and accuracy testing of machines was completed.

NATIONAL INVESTIGATIONS

Independent Analyses: Many privately funded investigations have been conducted for a number of years, particularly in the last three. Their results have been statistically well beyond significant in suggesting serious problems exist with voting machines as seen in past elections and undoubtedly will be seen in future ones. As might be expected, their results were consistently met with adamant denials of any problems often without any credible evidence to prove otherwise. In some cases, the analyses were so overwhelmingly demonstrative of serious problems that no reasonable objection to the probable cause could be levied. For instance, how do you explain sudden dramatic inputs of hundreds of thousands of votes at 3 a.m. in all five battleground states which all shut down at the same time for no obvious reason, and nearly all new votes were just for one candidate flipping the election? No rationale except for machine manipulation is logical.

IMPLICATIONS TO KANSAS ELECTIONS

Blessings Instead of FMEA Analyses: In an August 8, 2018 report by the Kansas Legislative Research Department, an extensive list of vulnerabilities to election systems in Kansas were identified. While there have been efforts to resolve some of these, most have been to accommodate the convenience of the voter, like distributed drop boxes which are unsecured and potentially ripe for ballot stuffing. While much effort and money was spent on election equipment and processes, perhaps the greatest vulnerability and one not necessarily adequately addressed is the bad actor. No matter how good a system is, someone seeking to circumvent it can find a way.

One particular weakness is the official assumption that procedures and policies put in place are sufficient to prevent violations of election integrity such as intrusions into the system. In the development of government-funded systems, teams are charged with looking for ways to break the system or, in the case of space systems, ways they will break by unanticipated means. The purpose of this FMEA (Failure Modes and Effects Analysis) is to ensure every conceivable failure mode is mitigated to the greatest degree possible. Our election system, as complicated and vulnerable as it is, is not investigated and analyzed this way. It is merely assumed that a given procedure instituted to protect election integrity will prevent malfeasance. Given the importance of every voter's right to a protected vote, this approach is insufficient.

SUMMARY

Independent and objective analyses by numerous technical experts over the years and particular in the last several have shown numerous, significant vulnerabilities in election machines. As with any computer, it is nearly impossible to prevent bad actors from gaining access and corrupting these systems. In addition, our national election system is complex, involves foreign actors, and offers a wealth of opportunities for election results manipulation. The simple and cost-effective solution to this untenable problem is to eliminate the primary source – voting machines – and replace them with high-tech, paper ballots as is now being done in other countries.