

PLAINTIFFS' COMPLAINT EXHIBIT CORRELATION TABLE

DOCKET No.	EXHIBIT No.	EXHIBIT TITLE
1-1	EXH 1	Redacted - Venezuela Smartmatic Affidavit 11.116.2020
1-2	EXH 2	Absentee Survey Analysis - Briggs Rpt.
1-3	EXH 2 A	Absentee Survey Wisconsin Analysis – Briggs Rpt. re Attachment AZ
1-4	EXH 2 B	Briggs - attachment GA re 5 state Rpt. Absentee Live ID Topline
1-5	EXH 2 C	Briggs - attachment PA re 5 state Rpt. Absentee Live ID Topline
1-6	EXH 2 D	Briggs - Attachment WI Unreturned Live Agent Topline [26655]
1-7	EXH 2 E	Briggs - Attachment MI Unreturned Live Agent Topline
1-8	EXH 2 F	Briggs CV
1-9	EXH 3	Re Braynard
1-11	EXH 4	Redacted Expert affidavit - Statistician
1-12	EXH 5	Diane Serra Declaration (3 sep pdfs for pages 1-3)
1-13	EXH 6	Joseph Oltmann Affidavit
1-14	EXH 7	Harri Hursti Declaration Doc 809 US DIST CT 3 8-24-20
1-15	EXH 8	Affidavit of Anna Mercedes Diaz Cardozo in ENGLISH
1-16	EXH 9	Keshel Expert Affidavit
1-17	EXH 9 A&B	Keshel Expert attachment

1-18	EXH 10	Andrew W. Appel, <i>et al.</i> , “Ballot Marking Devices (BMDs) Cannot Assure the Will of the Voters” at (Dec. 27, 2019)
1-19	EXH 11	State of Texas Secretary of State Report of Review 20 //and 11B
1-20	EXH 12	Spider Affidavit Redacted
1-21	EXH 13	Redacted Declaration TPM 11 30 20 Redacted
1-22	EXH 14	Declaration of Ronald Watkins 11 26 20
1-23	EXH 15	Congresswoman Maloney letter re Smartmatica
1-24	EXH 16	Senators Warren etc. letter re Dominion Voting Systems
1-25	EXH 17	Ramsland Declaration
1-26	EXH 18	Joint FBI CISSA Cyber Security Advisory Exhibit [2305843009225631231]
1-27	EXH 19	MCB Redacted Fraud Declaration 11 30 20 Redacted
EXH 20		Mark Low Declaration
EXH 21		Burns Decl Declaration
EXH 22		Greg Wodynski Declaration
EXH 23		Linda Brickman Declaration

Dated December 2, 2020

Attorneys for Plaintiffs

SIDNEY POWELL P.C.

/s Sidney Powell

Sidney Powell
Sidney Powell P.C.
2911 Turtle Creek Blvd.
#300
Dallas, TX 75219-4480
(214) 707-1775
sidney@federalappeals.com
Attorneys for Plaintiff

EXHIBIT 1

DECLARATION OF [REDACTED]

I, [REDACTED], hereby state the following:

1. [REDACTED]
[REDACTED]
[REDACTED]
2. I am an adult of sound mind. All statements in this declaration are based on my personal knowledge and are true and correct.
3. I am making this statement voluntarily and on my own initiative. I have not been promised, nor do I expect to receive, anything in exchange for my testimony and giving this statement. I have no expectation of any profit or reward and understand that there are those who may seek to harm me for what I say in this statement. I have not participated in any political process in the United States, have not supported any candidate for office in the United States, am not legally permitted to vote in the United States, and have never attempted to vote in the United States.
4. I want to alert the public and let the world know the truth about the corruption, manipulation, and lies being committed by a conspiracy of people and companies intent upon betraying the honest people of the United States and their legally constituted institutions and fundamental rights as citizens. This conspiracy began more than a decade ago in Venezuela and has spread to countries all over the world. It is a conspiracy to wrongfully gain and keep power and wealth. It involves political leaders, powerful companies, and other persons whose purpose is to gain and keep power by changing the free will of the people and subverting the proper course of governing.
5. [REDACTED]
[REDACTED] Over the course of my career, I specialized in the marines [REDACTED]
[REDACTED]
[REDACTED]
6. Due to my training in special operations and my extensive military and academic formations, I was selected for the national security guard detail of the President of Venezuela. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

7. [REDACTED]

[REDACTED] Señor Cabello was a long-time confederate of President Chavez and instrumental in his gaining power. In 2002, Señor Cabello had very briefly taken over the duties of the presidency while Hugo Chavez was imprisoned. Within hours of Señor Cabello taking over the presidency, Hugo Chavez was released from prison and regained the office of President. On December 11, 2011, Cabello was installed as the Vice-President of the United Socialist Party – the party of President Chávez and became the second most powerful figure in the party after Hugo Chávez. Cabello was appointed president of the National Assembly in early 2012 and was re-elected to that post in January 2013. After Hugo Chávez’s death, Cabello was next in line for the presidency of the country, but he remained president of the National Assembly and yielded to Nicolás Maduro holding the position of President of Venezuela.

8. [REDACTED]

[REDACTED] President Chavez was very precise and exacting in his instructions in the details about meetings he wanted, where the meeting was to occur, who was to attend, what was to be done. [REDACTED]

[REDACTED]

9. [REDACTED] I was witness to the creation and operation of a

sophisticated electronic voting system that permitted the leaders of the Venezuelan government to manipulate the tabulation of votes for national and local elections and select the winner of those elections in order to gain and maintain their power.

10. Importantly, I was a direct witness to the creation and operation of an electronic voting system in a conspiracy between a company known as Smartmatic and the leaders of conspiracy with the Venezuelan government. This conspiracy specifically involved President Hugo Chavez Frias, the person in charge of the National Electoral Council named Jorge Rodriguez, and principals, representatives, and personnel from Smartmatic which included [REDACTED]. The purpose of this conspiracy was to create and operate a voting system that could change the votes in elections from votes *against* persons running the Venezuelan government to votes *in their favor* in order to maintain control of the government.
11. In mid-February of 2009, there was a national referendum to change the Constitution of Venezuela to end term limits for elected officials, including the President of Venezuela. The referendum passed. This permitted Hugo Chavez to be re-elected an unlimited number of times.
12. After passage of the referendum, President Chavez instructed me to make arrangements for him to meet with Jorge Rodriguez, then President of the National Electoral Council, and three executives from Smartmatic. Among the three Smartmatic representatives were [REDACTED]
[REDACTED] President Chavez had multiple meetings with Rodriguez and the Smartmatic team at which I was present. In the first of four meetings, Jorge Rodriguez promoted the idea to create software that would manipulate elections. Chavez was very excited and made it clear that he would provide whatever Smartmatic needed. He wanted them immediately to create a voting system which would ensure that any time anything was going to be voted on the voting system would guarantee results that Chavez wanted. Chavez offered Smartmatic many inducements, including large sums of money, for Smartmatic to create or modify the voting system so that it would guarantee Chavez would win every election cycle. Smartmatic's team agreed to create such a system and did so.
13. I arranged and attended three more meetings between President Chavez and the representatives from Smartmatic at which details of the new

voting system were discussed and agreed upon. For each of these meetings, I communicated directly with [REDACTED] on details of where and when to meet, where the participants would be picked up and delivered to the meetings, and what was to be accomplished. At these meetings, the participants called their project the “Chavez revolution.” From that point on, Chavez never lost any election. In fact, he was able to ensure wins for himself, his party, Congress persons and mayors from townships.

14. Smartmatic’s electoral technology was called “Sistema de Gestión Electoral” (the “Electoral Management System”). Smartmatic was a pioneer in this area of computing systems. Their system provided for transmission of voting data over the internet to a computerized central tabulating center. The voting machines themselves had a digital display, fingerprint recognition feature to identify the voter, and printed out the voter’s ballot. The voter’s thumbprint was linked to a computerized record of that voter’s identity. Smartmatic created and operated the entire system.
15. Chavez was most insistent that Smartmatic design the system in a way that the system could change the vote of each voter without being detected. He wanted the software itself to function in such a manner that if the voter were to place their thumb print or fingerprint on a scanner, then the thumbprint would be tied to a record of the voter’s name and identity as having voted, but that voter would not tracked to the changed vote. He made it clear that the system would have to be setup to not leave any evidence of the changed vote for a specific voter and that there would be no evidence to show and nothing to contradict that the name or the fingerprint or thumb print was going with a changed vote. Smartmatic agreed to create such a system and produced the software and hardware that accomplished that result for President Chavez.
16. After the Smartmatic Electoral Management System was put in place, I closely observed several elections where the results were manipulated using Smartmatic software. One such election was in December 2006 when Chavez was running against Rosales. Chavez won with a landslide over Manuel Rosales - a margin of nearly 6 million votes for Chavez versus 3.7 million for Rosales.
17. On April 14, 2013, I witnessed another Venezuelan national election in which the Smartmatic Electoral Management System was used to manipulate and change the results for the person to succeed Hugo Chávez

as President. In that election, Nicolás Maduro ran against Capriles Radonsky. [REDACTED]

[REDACTED] Inside that location was a control room in which there were multiple digital display screens – TV screens – for results of voting in each state in Venezuela. The actual voting results were fed into that room and onto the displays over an internet feed, which was connected to a sophisticated computer system created by Smartmatic. People in that room were able to see in “real time” whether the vote that came through the electronic voting system was in their favor or against them. If one looked at any particular screen, they could determine that the vote from any specific area or as a national total was going against either candidate. Persons controlling the vote tabulation computer had the ability to change the reporting of votes by moving votes from one candidate to another by using the Smartmatic software.

18. By two o'clock in the afternoon on that election day Capriles Radonsky was ahead of Nicolás Maduro by two million votes. When Maduro and his supporters realized the size of Radonsky's lead they were worried that they were in a crisis mode and would lose the election. The Smartmatic machines used for voting in each state were connected to the internet and reported their information over the internet to the Caracas control center in real-time. So, the decision was made to reset the entire system. Maduro's and his supporters ordered the network controllers to take the internet itself offline in practically all parts in Venezuela and to change the results.
19. It took the voting system operators approximately two hours to make the adjustments in the vote from Radonsky to Maduro. Then, when they turned the internet back on and the on-line reporting was up and running again, they checked each screen state by state to be certain where they could see that each vote was changed in favor of Nicholas Maduro. At that moment the Smartmatic system changed votes that were for Capriles Radonsky to Maduro. By the time the system operators finish, they had achieved a convincing, but narrow victory of 200,000 votes for Maduro.
20. After Smartmatic created the voting system President Chavez wanted, he exported the software and system all over Latin America. It was sent to Bolivia, Nicaragua, Argentina, Ecuador, and Chile – countries that were in alliance with President Chavez. This was a group of leaders who wanted to be able to guarantee they maintained power in their countries. When Chavez died, Smartmatic was in a position of being the only

company that could guarantee results in Venezuelan elections for the party in power.

21. I want to point out that the software and fundamental design of the electronic electoral system and software of Dominion and other election tabulating companies relies upon software that is a descendant of the Smartmatic Electoral Management System. In short, the Smartmatic software is in the DNA of every vote tabulating company's software and system.
22. Dominion is one of three major companies that tabulates votes in the United States. Dominion uses the same methods and fundamentally same software design for the storage, transfer and computation of voter identification data and voting data. Dominion and Smartmatic did business together. The software, hardware and system have the same fundamental flaws which allow multiple opportunities to corrupt the data and mask the process in a way that the average person cannot detect any fraud or manipulation. The fact that the voting machine displays a voting result that the voter intends and then prints out a paper ballot which reflects that change does not matter. It is the software that counts the digitized vote and reports the results. The software itself is the one that changes the information electronically to the result that the operator of the software and vote counting system intends to produce that counts. That's how it is done. So the software, the software itself configures the vote and voting result -- changing the selection made by the voter. The software decides the result regardless of what the voter votes.
23. All of the computer controlled voting tabulation is done in a closed environment so that the voter and any observer cannot detect what is taking place unless there is a malfunction or other event which causes the observer to question the process. I saw first-hand that the manipulation and changing of votes can be done in real-time at the secret counting center which existed in Caracas, Venezuela. For me it was something very surprising and disturbing. I was in awe because I had never been present to actually see it occur and I saw it happen. So, I learned first-hand that it doesn't matter what the voter decides or what the paper ballot says. It's the software operator and the software that decides what counts -- not the voter.
24. If one questions the reliability of my observations, they only have to read the words of [REDACTED] [REDACTED] [REDACTED] a time period in [REDACTED]

which Smartmatic had possession of all the votes and the voting, the votes themselves and the voting information at their disposition in Venezuela.

██████████ he was assuring that the voting system implemented or used by Smartmatic was completely secure, that it could not be compromised, was not able to be altered.

25. But later, in 2017 when there were elections where Maduro was running and elections for legislators in Venezuela, ██████████ and Smartmatic broke their secrecy pact with the government of Venezuela. He made a public announcement through the media in which he stated that all the Smartmatic voting machines used during those elections were totally manipulated and they were manipulated by the electoral council of Venezuela back then. ██████████ stated that all of the votes for Nicholas Maduro and the other persons running for the legislature were manipulated and they actually had lost. So I think that's the greatest proof that the fraud can be carried out and will be denied by the software company that ██████████ admitted publicly that Smartmatic had created, used and still uses vote counting software that can be manipulated or altered.
26. I am alarmed because of what is occurring in plain sight during this 2020 election for President of the United States. The circumstances and events are eerily reminiscent of what happened with Smartmatic software electronically changing votes in the 2013 presidential election in Venezuela. What happened in the United States was that the vote counting was abruptly stopped in five states using Dominion software. At the time that vote counting was stopped, Donald Trump was significantly ahead in the votes. Then during the wee hours of the morning, when there was no voting occurring and the vote count reporting was off-line, something significantly changed. When the vote reporting resumed the very next morning there was a very pronounced change in voting in favor of the opposing candidate, Joe Biden.
27. ██████████ I have worked in gathering information, researching, and working with information technology. That's what I know how to do and the special knowledge that I have. Due to these recent election events, I contacted a number of reliable and intelligent ex-co-workers of mine that are still informants and work with the intelligence community. I asked for them to give me information that was up-to-date information in as far as how all these businesses are acting, what actions they are taking.

I declare under penalty of perjury that the foregoing is true and correct and that this Declaration was prepared in Dallas County, State of Texas, and executed on November 15, 2020.

EXHIBIT 2

An Analysis of Surveys Regarding Absentee Ballots Across Several States

William M. Briggs

November 23, 2020

1 Summary

Survey data was collected from individuals in several states, sampling those who the states listed as not returning absentee ballots. The data was provided by Matt Braynard.

The survey asked respondents whether they (a) had ever requested an absentee ballot, and, if so, (b) whether they had in fact returned this ballot. From this sample I produce predictions of the total numbers of: **Error #1**, those who were recorded as receiving absentee ballots *without* requesting them; and **Error #2**, those who returned absentee ballots but whose votes went missing (i.e. marked as unreturned).

The sizes of both errors were large in each state. The states were Georgia, Michigan, Wisconsin, and Arizona where ballots were across parties. Pennsylvania data was for Republicans only.

2 Analysis Description

Each analysis was carried out separately for each state. The analysis used (a) the number of absentee ballots recorded as unreturned, (b) the total responding to the survey, (c) the total of those saying they did not request a ballot, (d) the total of those saying they did request a ballot, and of these (e) the number saying they returned their ballots. I assume survey respondents are representative and the data is accurate.

From these data a simple parameter-free predictive model was used to calculate the probability of all possible outcomes. Pictures of these probabilities were derived, and the 95% prediction interval of the relevant numbers was calculated. The pictures appear in the Appendix at the end. They are summarized here with their 95% prediction intervals.

Error #1: being recorded as sent an absentee ballot without requesting one.

Error #2: sending back an absentee ballot and having it recorded as not returned.

State	Unreturned ballots	Error #1	Error #2
Georgia	138,029	16,938–22,771	31,559–38,866
Michigan	139,190	29,611–36,529	27,928–34,710
Pennsylvania*	165,412	32,414–37,444	26,954–31,643
Wisconsin	96,771	16,316–19,273	13,991–16,757
Arizona	518,560	208,333–229,937	78,714–94,975

*Number for Pennsylvania represent Republican ballots only.

Ballots that were not requested, and ballots returned and marked as not returned were classed as *troublesome*. The estimated average number of troublesome ballots for each state were then calculated using the table above and are presented next.

State	Unreturned ballots	Estimated average troublesome ballots	Percent
Georgia	138,029	53,489	39%
Michigan	139,190	62,517	45%
Pennsylvania*	165,412	61,780	37%
Wisconsin	96,771	29,594	31%
Arizona	518,560	303,305	58%

*Number for Pennsylvania represent Republican ballots only.

3 Conclusion

There are clearly a large number of troublesome ballots in each state investigated. Ballots marked as not returned that were never requested are clearly an error of some kind. The error is not small as a percent of the total recorded unreturned ballots.

Ballots sent back and unrecorded is a separate error. These represent votes that have gone missing, a serious mistake. The number of these missing ballots is also large in each state.

Survey respondents were not asked if they received an unrequested ballot whether they sent these ballots back. This is clearly a lively possibility, and represents a third possible source of error, including the potential of voting twice (once by absentee and once at the polls). No estimates or likelihood can be calculated for this potential error due to absence of data.

4 Declaration of William M. Briggs, PhD

1. My name is William M. Briggs. I am over 18 years of age and am competent to testify in this action. All of the facts stated herein are true and based on my personal knowledge.
2. I received a Ph.D of Statistics from Cornell University in 2004.
3. I am currently a statistical consultant. I make this declaration in my personal capacity.
4. I have analyzed data regarding responses to questions relating to mail ballot requests, returns and related issues.
5. I attest to a reasonable degree of professional certainty that the resulting analysis are accurate.

I declare under the penalty of perjury that the foregoing is true and correct.



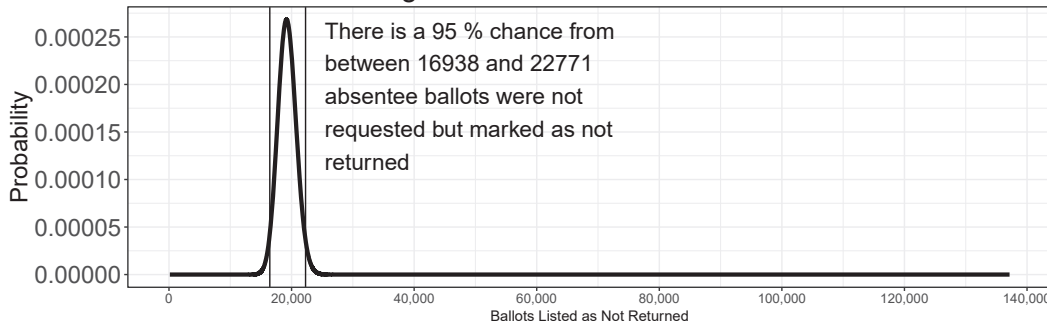
23 November 2020

William M. Briggs

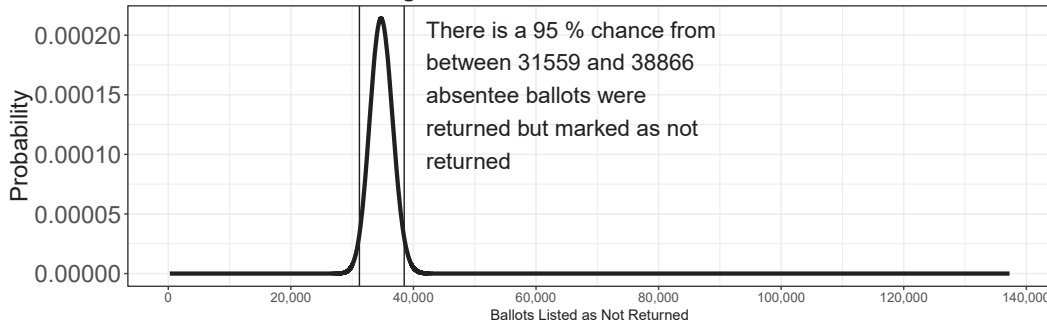
5 Appendix

The probability pictures for each state for each outcome as mentioned above.

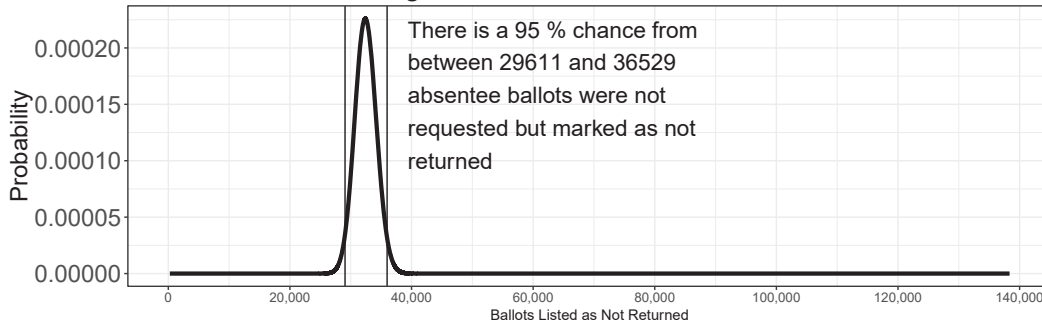
Probability of numbers of un-requested absentee ballots listed as not returned for Georgia



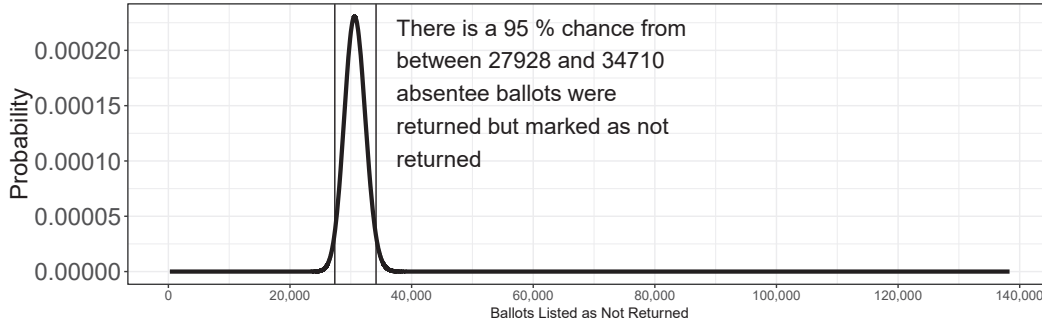
Probability of numbers of absentee ballots returned but listed as not returned for Georgia



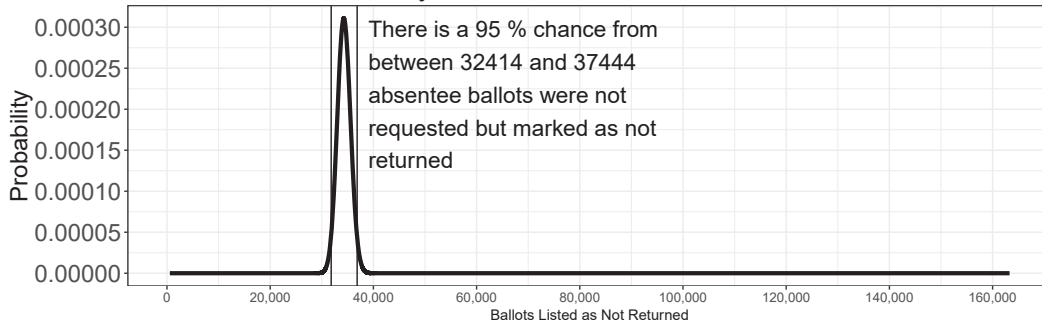
Probability of numbers of un-requested absentee ballots listed as not returned for Michigan



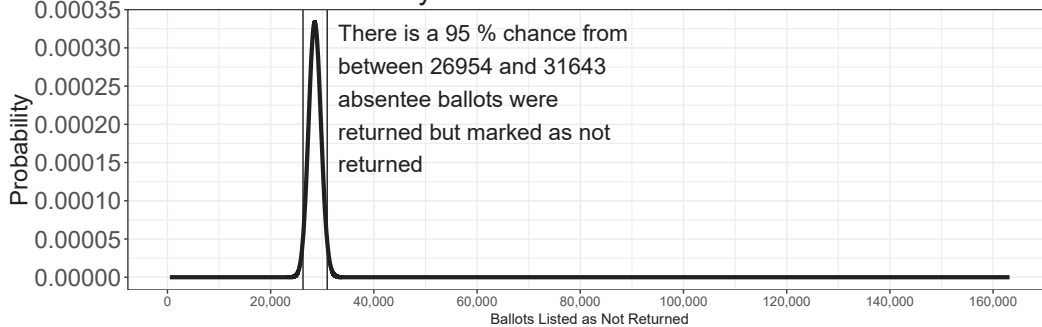
Probability of numbers of absentee ballots returned but listed as not returned for Michigan



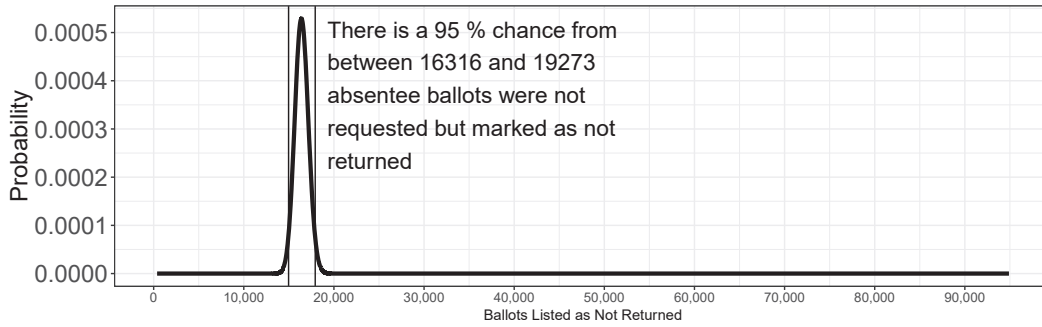
Probability of numbers of un-requested absentee ballots listed as not returned for Pennsylvania



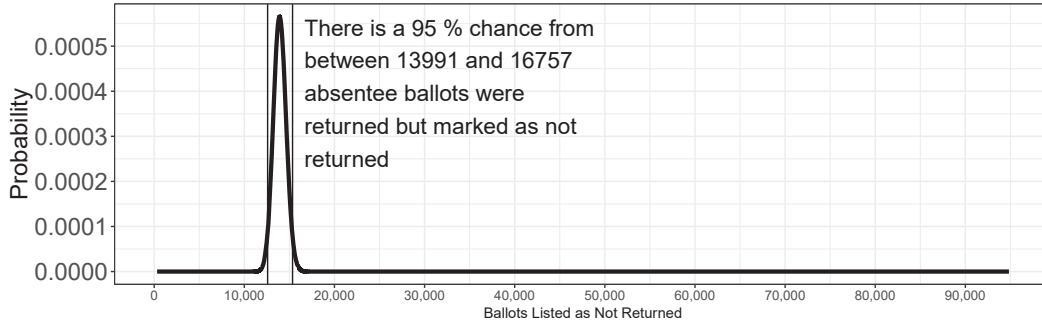
Probability of numbers of absentee ballots returned but listed as not returned for Pennsylvania



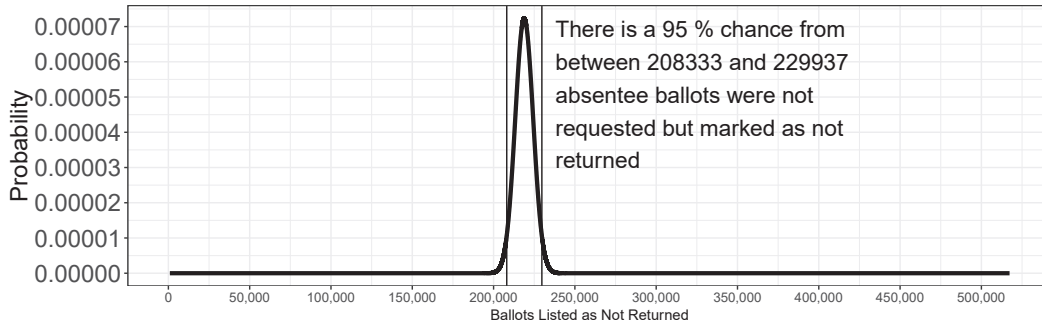
Probability of numbers of un-requested absentee ballots listed as not returned for Wisconsin



Probability of numbers of absentee ballots returned but listed as not returned for Wisconsin



Probability of numbers of un-requested absentee ballots listed as not returned for Arizona



Probability of numbers of absentee ballots returned but listed as not returned for Arizona

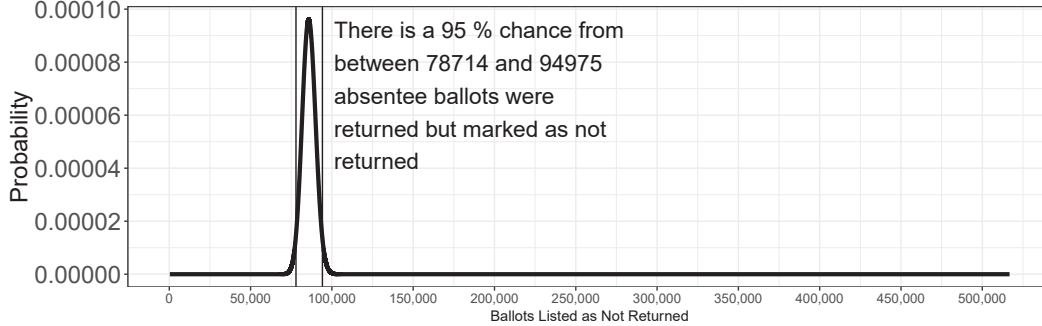


EXHIBIT 2 A

AZ Unreturned Live Agent - Mass Markets

	11/15/2020	11/16/2020	11/17/2020
5,604 Completes	745	1,881	2,978
684 Q4=01	116	212	356
1,945 VM Message Left	90	657	1,198
2,975 up/RC	539	1,012	1,424
74,437 No Answer	6,764	25,056	42,617
1,663 Numbers/Language	245	384	1,034
100.00% List Penetration			
81,708 Data Loads			

	11/15/2020	11/16/2020	11/17/2020
Q1 - May I please speak to <lead on screen>?	Response	11/15/2020	11/16/2020
1,812	40.05% A-Reached Target	307	554
335	7.40% Uncertain	80	124
2,377	52.54% X = Refused	382	854
0	0.00%		
4,524	100.00% Sum of All Responses	769	1,532
			2,223

	11/15/2020	11/16/2020	11/17/2020
Q2 - Did you request Absentee Ballot in state of AZ?	Response	11/15/2020	11/16/2020
1,120	45.00% A-Yes [Go to Q3]	210	361
			549

885	35.56%	B-No [Go to Q4]	162	286	437
24	0.96%	Member) [Go to Q3]	5	9	10
21	0.84%	Member) [Go to Q4]	3	10	8
72	2.89%	E-Unsure [Go to Close A]	10	18	44
7	0.28%	[Go to Close A]	-	1	6
360	14.46%	X = Refused	45	69	246
2,489	100.00%	Sum of All Responses	435	754	1,300

		Response	11/15/2020	11/16/2020	11/17/2020
344	16.16%	A-Yes [Go to Q4]	67	112	165
696	32.69%	B-No [Go to Close A]	116	237	343
11	0.52%	Member) [Go to Q4]	2	2	7
9	0.42%	Member) [Go to Close A]	1	4	4
14	0.66%	Close A]	3	4	7
1,055	49.55%	X = Refused	201	326	528
2,129	100.00%	Sum of All Responses	390	685	1,054

		Response	11/15/2020	11/16/2020	11/17/2020
678	82.48%	Q5]	116	212	350
144	17.52%	B-Refused [Go to Q5]	38	50	56

0	0.00%				
0	0.00%				
822	100.00%	Sum of All Responses	154	262	406

Q5 - Can you provide us your email address?		Response	11/15/2020	11/16/2020	11/17/2020
127	18.57%	01-Yes [Go to Close B]	24	36	67
557	81.43%	02-No [Go to Close B]	92	176	289
0	0.00%				
684	100.00%	Sum of All Responses	116	212	356

EXHIBIT 2 B

AZ Unreturned Live Agent - Mass Markets

	11/15/2020	11/16/2020	11/17/2020
5,604 Completes	745	1,881	2,978
684 Q4=01	116	212	356
1,945 VM Message Left	90	657	1,198
2,975 up/RC	539	1,012	1,424
74,437 No Answer	6,764	25,056	42,617
1,663 Numbers/Language	245	384	1,034
100.00% List Penetration			
81,708 Data Loads			

	11/15/2020	11/16/2020	11/17/2020
Q1 - May I please speak to <lead on screen>?			
1,812	307	554	951
40.05% A-Reached Target			
335	80	124	131
7.40% Uncertain			
2,377	382	854	1,141
52.54% X = Refused			
0			
0.00%			
4,524	769	1,532	2,223
100.00% Sum of All Responses			

	11/15/2020	11/16/2020	11/17/2020
Q2 - Did you request Absentee Ballot in state of AZ?			
1,120	210	361	549
45.00% A-Yes [Go to Q3]			

885	35.56%	B-No [Go to Q4]	162	286	437
24	0.96%	Member) [Go to Q3]	5	9	10
21	0.84%	Member) [Go to Q4]	3	10	8
72	2.89%	E-Unsure [Go to Close A]	10	18	44
7	0.28%	[Go to Close A]	-	1	6
360	14.46%	X = Refused	45	69	246
2,489	100.00%	Sum of All Responses	435	754	1,300

Q3 - Did you mail your ballot		Response	11/15/2020	11/16/2020	11/17/2020
344	16.16%	A-Yes [Go to Q4]	67	112	165
696	32.69%	B-No [Go to Close A]	116	237	343
11	0.52%	Member) [Go to Q4]	2	2	7
9	0.42%	Member) [Go to Close A]	1	4	4
14	0.66%	Close A]	3	4	7
1,055	49.55%	X = Refused	201	326	528
2,129	100.00%	Sum of All Responses	390	685	1,054

Q4 - Can you please give us the best phone number to reach you at?		Response	11/15/2020	11/16/2020	11/17/2020
678	82.48%	Q5]	116	212	350
144	17.52%	B-Refused [Go to Q5]	38	50	56

0	0.00%				
0	0.00%				
822	100.00%	Sum of All Responses	154	262	406

Q5 - Can you provide us your email address?		Response	11/15/2020	11/16/2020	11/17/2020
127	18.57%	01-Yes [Go to Close B]	24	36	67
557	81.43%	02-No [Go to Close B]	92	176	289
0	0.00%				
684	100.00%	Sum of All Responses	116	212	356

EXHIBIT 2 C

MI Unreturned Live Agent - Mass Markets

	11/15/2020	11/16/2020	11/17/2020
3,815 Completes	-	990	2,825
248 Q4=01	-	36	212
1,257 VM Message Left	-	388	869
2,310 up/RC	-	566	1,744
62,569 No Answer	-	15,482	47,087
3,644 Numbers/Language	-	570	3,074
100.00% List Penetration			
70,030 Data Loads			

	11/15/2020	11/16/2020	11/17/2020
Q1 - May I please speak to <lead on screen>?			
958 23.65% A-Reached Target	-	158	800
142 3.51% Uncertain	-	57	85
2,950 72.84% X = Refused	-	883	2,067
0 0.00%			
4,050 100.00% Sum of All Responses	-	1,098	2,952

	11/15/2020	11/16/2020	11/17/2020
Q2 - Did you request Absentee Ballot in state of MI?			
752 49.64% A-Yes [Go to Q3]	-	167	585

239	15.78%	B-No [Go to Q4]	-	39	200
50	3.30%	Member) [Go to Q3]	-	5	45
17	1.12%	Member) [Go to Q4]	-	2	15
37	2.44%	E-Unsure [Go to Close A]	-	4	33
11	0.73%	Moment [Go to Close A]	-	2	9
409	27.00%	X = Refused	-	63	346
1,515	100.00%	Sum of All Responses	-	282	1,233

			11/15/2020	11/16/2020	11/17/2020
Q3 - Did you mail your ballot back?	Response				
232	21.28%	A-Yes [Go to Q4]	-	41	191
472	43.30%	B-No [Go to Close A]	-	109	363
10	0.92%	Member) [Go to Q4]	-	2	8
28	2.57%	Member) [Go to Close A]	-	2	26
22	2.02%	Close A]	-	5	17
326	29.91%	X = Refused	-	60	266
1,090	100.00%	Sum of All Responses	-	219	871

			11/15/2020	11/16/2020	11/17/2020
Q4 - Can you please give us the best phone number to reach you at?	Response				
246	69.89%	to Q5]	-	36	210
106	30.11%	B-Refused [Go to Q5]	-	27	79

0	0.00%				
0	0.00%				
352	100.00%	Sum of All Responses	-	63	289

Q5 - Can you provide us your email address?		Response	11/15/2020	11/16/2020	11/17/2020
18	7.26%	01-Yes [Go to Close B]	-	5	13
230	92.74%	02-No [Go to Close B]	-	31	199
0	0.00%				
248	100.00%	Sum of All Responses	-	36	212

EXHIBIT 2 D

0270 PA Absentee Live ID Topline

	11/9/2020	11/10/2020	11/11/2020
18037 Completes	4419	13618	0
834 survey** - Q4=01	178	656	
14,203 Machines	3465	10738	
3,000 Hang up/RC	776	2224	
3,521 Numbers/Languag	556	2965	
0 MA			
87.70% List Penetration			
24,581 Data Loads	24,581		

	9-Nov	10-Nov	11-Nov
Q1 - May I please speak to <lead on screen>?			
2,262	593	1,669	
422	102	320	
298	77	221	
739	160	579	
2,982	932	2789	0

	9-Nov	10-Nov	11-Nov
Q2 - Did you request an absentee ballot?			
1,114	331	783	
531	131	400	

36	1.42%	confirmed "Yes" [Go to Q3]	12	24
25	0.99%	confirmed "No" [Go to Q4]	9	16
91	3.59%	5. Unsure. [Go to Q3].	25	66
89	3.51%	moment. [Go to Close A]	17	72
544	21.44%	A]	105	439
107	4.22%	X = Refused <Go to CLOSE A>	29	78
147	5.79%	Q = Hangup <Go to CLOSE A>	36	111
2,537	100.00%	Sum of All Responses	695	1989
				0

Q3 - Did you mail back that ballot?		Response	9-Nov	10-Nov	11-Nov
452	39.75%	1. Yes. [Go to Go to Q4].	90	362	
632	55.58%	2. No [Go to Close A].	229	403	
11	0.97%	confirmed "Yes" [Go to Q4]	1	10	
11	0.97%	confirmed "No" [Go to Close A]	4	7	
15	1.32%	5. Unsure. [Go to Close A].	6	9	
2	0.18%	moment. [Go to Close A]	0	2	
14	1.23%	X = Refused <Go to CLOSE A>	5	9	
13	1.14%	Q = Hangup <Go to CLOSE A>	8	5	
1,137	100.00%	Sum of All Responses	343	807	0

Q4 - Can you please give us the best phone number to reach you at?		Response	9-Nov	10-Nov	11-Nov
834	87.61%	01 = Yes <Go to CLOSE B>	178	656	
118	12.39%	X = Refused <Go to CLOSE A>	36	82	
67	7.04%	Q = Hangup <Go to CLOSE A>	17	50	
952	100.00%	Sum of All Responses	231	788	0

EXHIBIT 2 E

0276 GA Unreturned_Absentee Live ID Topline

	11/16/2020	11/17/2020
15179 Completes	8143	7036
184 Q5=01 or 02	64	120
13,479 Answering Machines	7090	6389
1,516 up/RC	989	527
4,902 Numbers/Language	2436	2466
0 MA	0	0
58.45% List Penetration		
34,355 Data Loads	34,355	

Q1 - May I please speak to <lead on screen>?	Response	16-Nov	17-Nov
767	65.28% 1. Reached Target [Go to Q2].	446	321
255	21.70% [Go to Q2].	165	90
153	13.02% X = Refused <Go to CLOSE A>	104	49
385	32.77% Q = Hangup <Go to CLOSE A>	267	118
1,175	100.00% Sum of All Responses	982	578

Q2 - Did you request an absentee ballot?	Response	16-Nov	17-Nov
591	61.31% 1. Yes. [Go to Go to Q3].	343	248
128	13.28% 2. No. [Go to Q4].	84	44

39	4.05%	member confirmed "Yes" [Go to	24	15
14	1.45%	member confirmed "No" [Go to Q4]	11	3
40	4.15%	5. Unsure. [Go to Q3].	26	14
82	8.51%	moment. [Go to Close A]	48	34
70	7.26%	X = Refused <Go to CLOSE A>	42	28
58	6.02%	Q = Hangup <Go to CLOSE A>	33	25
964	100.00%	Sum of All Responses	611	411

Q3 - Did you mail back that ballot?		Response	16-Nov	17-Nov
240	38.52%	1. Yes. [Go to Go to Q4].	149	91
317	50.88%	2. No. [Go to Close A].	174	143
17	2.73%	member confirmed "Yes" [Go to	10	7
9	1.44%	member confirmed "No" [Go to	4	5
24	3.85%	Close A]	14	10
11	1.77%	5. Unsure. [Go to Close A].	8	3
5	0.80%	moment. [Go to Close A]	5	0
7	1.12%	X = Refused <Go to CLOSE A>	3	4
623	100.00%	Q = Hangup <Go to CLOSE A>	367	263
		Sum of All Responses		

Q4 - Can you please give us the best phone number to reach you		Response	16-Nov	17-Nov
313	82.15%	01 = Yes <Go to Q5>	205	108
49	12.86%	02 = No <Go to Q5>	26	23
19	4.99%	X = Refused <Go to CLOSE A>	13	6
18	4.72%	Q = Hangup <Go to CLOSE A>	10	8

381	100.00%	Sum of All Responses	254	145
Q5 - May we please have an email address to follow-up as well?				
99	28.86%	01 = Yes <Go to CLOSE B>	64	35
229	66.76%	02 = No <Go to CLOSE B>	144	85
15	4.37%	X = Refused <Go to CLOSE A>	11	4
19	5.54%	Q = Hangup <Go to CLOSE A>	12	7
343	100.00%	Sum of All Responses	231	131

EXHIBIT 2 F

William M. Briggs, PhD

Statistician to the Stars!

matt@wmbriggs.com

917-392-0691

1. EXPERIENCE

- (1) 2016: AUTHOR OF *Uncertainty: The Soul of Modeling, Probability & Statistics*, a book which argues for a complete and fundamental change in the philosophy and practice of probability and statistics. Eliminate hypothesis testing and estimation, and move to verifiable predictions. This includes AI and machine learning. Call this The Great Reset, but a good one.
- (2) 2004-2016 ADJUNCT PROFESSOR OF STATISTICAL SCIENCE, CORNELL UNIVERSITY, ITHACA, NEW YORK
I taught a yearly Masters course to people who (rightfully) hate statistics. Interests: philosophy of science & probability, epistemology, epidemiology (ask me about the all-too-common epidemiologist fallacy), Bayesian statistics, medicine, climatology & meteorology, goodness of forecasts, overconfidence in science; public understanding of science, limitations of science, scientism; scholastic metaphysics (as it relates to epistemology).
- (3) 1998-PRESENT. STATISTICAL CONSULTANT, VARIOUS COMPANIES
Most of my time is spent coaxing people out of their money to tell them they are too sure of themselves. All manner of analyses cheerfully undertaken. Example: Fraud analysis; I created the *Wall Street Journal's* College Rankings. I consultant regularly at Methodist and other hospitals, start-ups, start-downs, and with any institution willing to fork it over.
- (4) 2003-2010. RESEARCH SCIENTIST, NEW YORK METHODIST HOSPITAL, NEW YORK
Besides the usual, I sit/sat on the Institutional Review Committee to assess the statistics of proposed research. I was an Associate Editor for *Monthly Weather Review* (through 2011). Also a member of the American Meteorological Society's Probability and Statistics Committee (through 2011). At a hospital? Yes, sir; at a hospital. It rains there, too, you know.
- (5) FALL 2007, FALL 2010 VISITING PROFESSOR OF STATISTICS, DEPARTMENT OF MATHEMATICS, CENTRAL MICHIGAN UNIVERSITY, MT. PLEASANT, MI
Who doesn't love a visit from a statistician? Ask me about the difference between "a degree" and "an education."
- (6) 2003-2007, ASSISTANT PROFESSOR STATISTICS, WEILL MEDICAL COLLEGE OF CORNELL UNIVERSITY, NEW YORK, NEW YORK
Working here gave me a sincere appreciation of the influences of government money; grants galore.
- (7) 2002-2003. GOTHAM RISK MANAGEMENT, NEW YORK
A start-up then, after Enron's shenanigans, a start-down. We set future weather derivative and weather insurance contract prices that incorporated information from medium- and long-range weather and climate forecasts.
- (8) 1998-2002. DOUBLECLICK, NEW YORK
Lead statistician. Lot of computer this and thats; enormous datasets.
- (9) 1993-1998. GRADUATE STUDENT, CORNELL UNIVERSITY

2

Meteorology, applied climatology, and finally statistics. Was Vice Chair of the graduate student government; probably elected thanks to a miracle.

- (10) 1992-1993. NATIONAL WEATHER SERVICE, SAULT STE. MARIE, MI
Forecast storms o' the day and launched enormous balloons in the name of Science. My proudest moment came when I was able to convince an ancient IBM-AT machine to talk to an *analog*, 110 baud, phone-coupled modem, all using BASIC!
- (11) 1989-1992. UNDERGRADUATE STUDENT, CENTRAL MICHIGAN UNIVERSITY
Meteorology and mathematics. Started the local student meteorology group to chase tornadoes. Who knew Michigan had so few? Spent a summer at U Michigan playing with a (science-fiction-sounding) lidar.
- (12) 1983-1989. UNITED STATES AIR FORCE
Cryptography and other secret stuff. Shot things; learned pinochle. I adopted and became proficient with a fascinating and versatile vocabulary. Irritate me for examples. TS/SCI, etc. security clearance (now inactive).

2. EDUCATION

- (1) Ph.D., 2004, Cornell University. Statistics.
- (2) M.S., 1995, Cornell University. Atmospheric Science.
- (3) B.S., Summa Cum Laude, 1992, Central Michigan University. Meteorology and Math.

3. PUBLICATIONS

3.0.1. *Popular.*

- (1) Op-eds in various newspapers; articles in *Stream*, *Crisis Magazine*, *The Remnant*, *Quadrant*, *Quirks*; blog with ~70,000 monthly readers. Various briefs submitted to government agencies, such as California Air Resources Board, Illinois Department of Natural Resources. Talks and holding-forths of all kinds.

3.0.2. *Books.*

- (1) Richards, JW, WM Briggs, and D Axe, 2020. *UThe Price of Panic: How the Tyranny of Experts Turned a Pandemic into a Catastrophe*. Regnery. Professors Jay Richards, William Briggs, and Douglas Axe take a deep dive into the crucial questions on the minds of millions of Americans during one of the most jarring and unprecedented global events in a generation.
- (2) Briggs, WM., 2016. *Uncertainty: The Soul of Modeling, Probability & Statistics*. Springer. Philosophy of probability and statistics. A new (old) way to view and to use statistics, a way that doesn't lead to heartbreak and pandemic over-certainty, like current methods do.
- (3) Briggs, WM., 2008 *Breaking the Law of Averages: Real Life Probability and Statistics in Plain English*. Lulu Press, New York. Free text for undergraduates.
- (4) Briggs, WM., 2006 *So You Think You're Psychic?* Lulu Press, New York. Hint: I'll bet you're not.

3.0.3. *Methods.*

- (1) Briggs, WM and J.C. Hanekamp, 2020. Uncertainty In The MAN Data Calibration & Trend Estimates. *Atmospheric Environment*, In review.
- (2) Briggs, WM and J.C. Hanekamp, 2020. Adjustments to the Ryden & McNeil Ammonia Flux Model. *Soil Use and Management*, In review.
- (3) Briggs, William M., 2020. Parameter-Centric Analysis Grossly Exaggerates Certainty. In *Data Science for Financial Econometrics*, V Kreinovich, NN Thach, ND Trung, DV Thanh (eds.), In press.
- (4) Briggs, WM, HT Nguyen, D Trafimow, 2019. Don't Test, Decide. In *Behavioral Predictive Modeling in Econometrics*, Springer, V Kreinovich, S Sriboonchitta (eds.). In press.
- (5) Briggs, William M. and HT Nguyen, 2019. Clarifying ASA's view on p-values in hypothesis testing. *Asian Journal of Business and Economics*, 03(02), 1–16.
- (6) Briggs, William M., 2019. Reality-Based Probability & Statistics: Solving The Evidential Crisis (invited paper). *Asian Journal of Business and Economics*, 03(01), 37–80.
- (7) Briggs, William M., 2019. Everything Wrong with P-Values Under One Roof. In *Beyond Traditional Probabilistic Methods in Economics*, V Kreinovich, NN Thach, ND Trung, DV Thanh (eds.), pp 22–44.
- (8) Briggs, WM, HT Nguyen, D Trafimow, 2019. The Replacement for Hypothesis Testing. In *Structural Changes and Their Econometric Modeling*, Springer, V Kreinovich, S Sriboonchitta (eds.), pp 3–17.
- (9) Trafimow, D, V Amrhein, CN Areshenkoff, C Barrera-Causil, ..., WM Briggs, (45 others), 2018. Manipulating the alpha level cannot cure significance testing. *Frontiers in Psychology*, 9, 699. doi.org/10.3389/fpsyg.2018.00699.
- (10) Briggs, WM, 2018. Testing, Prediction, and Cause in Econometric Models. In *Econometrics for Financial Applications*, ed. Anh, Dong, Kreinovich, and Thach. Springer, New York, pp 3–19.
- (11) Briggs, WM, 2017. The Substitute for p-Values. *JASA*, 112, 897–898.
- (12) J.C. Hanekamp, M. Crok, M. Briggs, 2017. Ammoniak in Nederland. *Enkele kritische wetenschappelijke kanttekeningen*. V-focus, Wageningen.
- (13) Briggs, WM, 2017. Math: Old, New, and Equalitarian. *Academic Questions*, 30(4), 508–513.
- (14) Monckton, C, W Soon, D Legates, ... (several others), WM Briggs 2018. On an error in applying feedback theory to climate. In submission (currently *J. Climate*).
- (15) Briggs, WM, JC Hanekamp, M Crok, 2017. Comment on Goedhart and Huijsmans. *Soil Use and Management*, 33(4), 603–604.
- (16) Briggs, WM, JC Hanekamp, M Crok, 2017. Response to van Pul, van Zanten and Wichink Kruit. *Soil Use and Management*, 33(4), 609–610.
- (17) Jaap C. Hanekamp, William M. Briggs, and Marcel Crock, 2016. A volatile discourse - reviewing aspects of ammonia emissions, models, and atmospheric concentrations in The Netherlands. *Soil Use and Management*, 33(2), 276–287.

- (18) Christopher Monckton of Brenchley, Willie Soon, David Legates, William Briggs, 2015. Keeping it simple: the value of an irreducibly simple climate model. *Science Bulletin*. August 2015, Volume 60, Issue 15, pp 1378–1390.
- (19) Briggs, WM, 2015. The Third Way Of Probability & Statistics: Beyond Testing and Estimation To Importance, Relevance, and Skill. *arxiv.org/abs/1508.02384*.
- (20) Briggs, WM, 2015. The Crisis Of Evidence: Why Probability And Statistics Cannot Discover Cause. *arxiv.org/abs/1507.07244*.
- (21) David R. Legates, Willie Soon, William M. Briggs, Christopher Monckton of Brenchley, 2015. Climate Consensus and ‘Misinformation’: A Rejoinder to Agnotology, Scientific Consensus, and the Teaching and Learning of Climate Change. *Science and Education*, 24, 299–318, DOI 10.1007/s11191-013-9647-9.
- (22) Briggs, WM, 2014. The Problem Of Grue Isn’t. *arxiv.org/abs/1501.03811*.
- (23) Christopher Monckton of Brenchley, Willie Soon, David Legates, William Briggs, 2014. Why models run hot: results from an irreducibly simple climate model. *Science Bulletin*. January 2015, Volume 60, Issue 1, pp 122-135.
- (24) Briggs, WM, 2014. Common Statistical Fallacies. *Journal of American Physicians and Surgeons*, Volume 19 Number 2, 58–60.
- (25) Aalt Bast, William M. Briggs, Edward J. Calabrese, Michael F. Fenech, Jaap C. Hanekamp, Robert Heaney, Ger Rijkers, Bert Schwitters, Pieter Verhoeven, 2013. Scientism, Legalism and Precaution—Contending with Regulating Nutrition and Health Claims in Europe. *European Food and Feed Law Review*, 6, 401–409.
- (26) Legates, DR, Soon, W, and Briggs, 2013. Learning and Teaching Climate Science: The Perils of Consensus Knowledge Using Agnotology. *Science and Education*, DOI 10.1007/s11191-013-9588-3.
- (27) Briggs, WM, 2012. On Probability Leakage. *arxiv.org/abs/1201.3611*.
- (28) Briggs, WM, 2012. Why do statisticians answer questions no one ever asks? *Significance*. Volume 9 Issue 1 Doi: 10.1111/j.1740-9713.2012.00542.x. 30–31.
- (29) Briggs, WM, Soon, W, Legates, D, Carter, R, 2011. A Vaccine Against Arrogance. *Water, Air, & Soil Pollution: Volume 220, Issue 1 (2011)*, Page 5-6
- (30) Briggs, WM, and R Zaretski, 2009. Induction and falsifiability in statistics. *arxiv.org/abs/math/0610859*.
- (31) Briggs, WM, 2011. Discussion to A Gelman. Why Tables are Really Much Better than Graphs. *Journal Computational and Graphical Statistics*. Volume 20, 16–17.
- (32) Zaretski R, Gilchrist MA, Briggs WM, and Armagan A, 2010. Bias correction and Bayesian analysis of aggregate counts in SAGE libraries. *BMC Bioinformatics*, 11:72doi:10.1186/1471-2105-11-72.
- (33) Zaretski, R, Briggs, W, Shankar, M, Sterling, M, 2009. Fitting distributions of large scale power outages: extreme values and the effect of truncation. *International Journal of Power and Energy Systems*. DOI: 10.2316/Journal.203.2009.1.203-4374.

- (34) Briggs, WM, 2007. Changes in number and intensity of world-wide tropical cyclones *arxiv.org/physics/0702131*.
- (35) Briggs, WM, 2007. On the non-arbitrary assignment of equi-probable priors *arxiv.org/math.ST/0701331*.
- (36) Briggs, WM, 2007. On the changes in number and intensity of North Atlantic tropical cyclones *Journal of Climate*. **21**, 1387-1482.
- (37) Briggs, WM, Positive evidence for non-arbitrary assignments of probability, 2007. Edited by Knuth et al. Proceedings 27th International Workshop on Bayesian Inference and Maximum Entropy Methods in Science and Engineering. American Institute of Physics. 101-108.
- (38) Briggs, WM, R Zaretzki, 2007. The Skill Plot: a graphical technique for the evaluating the predictive usefulness of continuous diagnostic tests. *With Discussion. Biometrics*. **64(1)**, 250-6; discussion 256-61. PMID: 18304288.
- (39) Zaretzki R, Gilchrist MA, Briggs WM, 2010. MCMC Inference for a Model with Sampling Bias: An Illustration using SAGE data. *arxiv.org/abs/0711.3765*
- (40) Briggs, WM, and D Ruppert, 2006. Assessing the skill of yes/no forecasts for Markov observations. *Monthly Weather Review*. **134**, 2601-2611.
- (41) Briggs, WM, 2007. Review of *Statistical Methods in the Atmospheric Sciences* (second edition, 2006) by Wilks, D.S. *Journal of the American Statistical Association*, **102**, 380.
- (42) Briggs, WM, M Pocerich, and D Ruppert, 2005. Incorporating misclassification error in skill assessment. *Monthly Weather Review*, **133(11)**, 3382-3392.
- (43) Briggs, WM, 2005. A general method of incorporating forecast cost and loss in value scores. *Monthly Weather Review*, **133(11)**, 3393-3397.
- (44) Briggs, WM, and D Ruppert, 2005. Assessing the skill of Yes/No Predictions. *Biometrics*. **61(3)**, 799-807. PMID: 16135031.
- (45) Briggs, WM, 2004. Discussion to T Gneiting, LI Stanberry, EP Gritmit, L Held, NA Johnson, 2008. Assessing probabilistic forecasts of multivariate quantities, with an application to ensemble predictions of surface winds. *Test*. **17**, 240-242.
- (46) Briggs, WM, 2004. Discussion to Gel, Y, AE Raftery, T Gneiting, and V.J. Berrocal, 2004. Calibrated Probabilistic Mesoscale Weather Field Forecasting: The Geostatistical Output Perturbation (GOP) Method. *J. American Statistical Association*. **99 (467)**: 586-587.
- (47) Mozer, JB, and Briggs, WM, 2003. Skill in real-time solar wind shock forecasts. *J. Geophysical Research: Space Physics*, **108 (A6)**, SSH 9 p. 1-9, (DOI 10.1029/2003JA009827).
- (48) Briggs, WM, 1999. Review of *Forecasting: Methods and Applications* (third edition, 1998) by Makridakis, Wheelwright, and Hyndman; and *Elements of Forecasting* (first edition, 1998) by Diebold. *Journal of the American Statistical Association*, **94**, 345-346.
- (49) Briggs, W.M., and R.A. Levine, 1997. Wavelets and Field Forecast Verification. *Monthly Weather Review*, **25 (6)**, 1329-1341.
- (50) Briggs, WM, and DS Wilks, 1996. Estimating monthly and seasonal distributions of temperature and precipitation using the new CPC long-range forecasts. *Journal of Climate*, **9**, 818-826.

6

- (51) Briggs, WM, and DS Wilks, 1996. Extension of the CPC long-lead temperature and precipitation outlooks to general weather statistics. *Journal of Climate*, **9**, 3496-3504.

3.0.4. *Applications.*

- (1) Jamorabo, Daniel, Renelus, Benjamin, Briggs, WM, 2019. "Comparative outcomes of EUS-guided cystogastrostomy for peripancreatic fluid collections (PFCs): A systematic review and meta-analysis, 2019. *Therapeutic Advances in Gastrointestinal Endoscopy*, in press.
- (2) Benjamin Renelus, S Paul, S Peterson, N Dave, D amorabo, W Briggs, P Kancharla, 2019. Racial disparities with esophageal cancer mortality at a high-volume university affiliated center: An All ACCESS Invitation, *Journal of the National Medical Association*, in press.
- (3) Mehta, Bella, S Ibrahim, WM Briggs, and P Efthimiou, 2019. Racial/Ethnic variations in morbidity and mortality in Adult Onset Still's Disease: An analysis of national dataset", *Seminars in Arthritis and Rheumatism*, doi: 10.1016/j.semarthrit.2019.04.0044.
- (4) Ivanov A, Dabiesingh DS, Bhumireddy GP, Mohamed A, Asfour A, Briggs WM, Ho J, Khan SA, Grossman A, Klem I, Sacchi TJ, Heitner JF. Prevalence and Prognostic Significance of Left Ventricular Noncompaction in Patients Referred for Cardiac Magnetic Resonance Imaging. *Circ Cardiovasc Imaging*. 2017 Sep;10(9). pii: e006174. doi: 10.1161/CIRCIMAGING.117.006174.
- (5) Ivanov A, Kaczowska BA, Khan SA, Ho J, Tavakol M, Prasad A, Bhumireddy G, Beall AF, Klem I, Mehta P, Briggs WM, fpaSacchi TJ, Heitner JF, 2017. Review and Analysis of Publication Trends over Three Decades in Three High Impact Medicine Journals. *PLoS One*. 2017 Jan 20;12(1):e0170056. doi: 10.1371/journal.pone.0170056.
- (6) A. Ivanova, G.P. Bhumireddy, D.S. Dabiesingh, S.A. Khana, J. Hoa N. Krishna, N. Dontineni, J.A Socolow, W.M. Briggs, I. Klem, T.J. Sacchi, J.F. Heitner, 2016. Importance of papillary muscle infarction detected by cardiac magnetic resonance imaging in predicting cardiovascular events. *International Journal of Cardiology*. Volume 220, 1 October 2016, Pages 558–563. PMID: 27390987.
- (7) A Ivanov, J Yossef, J Taillon, B Worku, I Gulkarov, A Tortolani, TJ Sacchi, WM Briggs, SJ Brener, JA Weingarten, JF Heitner, 2015. Do pulmonary function tests improve risk stratification before cardiothoracic surgery? *Journal of Thoracic and Cardiovascular Surgery*. 2015 Oct 30. pii: S0022-5223(15)02165-0. doi: 10.101. PMID: 26704058.
- (8) Chen O, Sharma A, Ahmad I, Bourji N, Nestoiter K, Hua P, Hua B, Ivanov A, Yossef J, Klem I, Briggs WM, Sacchi TJ, Heitner JF, 2015. Correlation between pericardial, mediastinal, and intrathoracic fat volumes with the presence and severity of coronary artery disease, metabolic syndrome, and cardiac risk factors. *Eur Heart J Cardiovasc Imaging*. 2015 Jan;16(1):37-46. doi: 10.1093/ehjci/jeu145.
- (9) Chery J, Semaan E, Darji S, Briggs W, Yarmush J, D'Ayala M, 2014. Impact of regional versus general anesthesia on the clinical outcomes of patients undergoing major lower extremity amputation. *Ann Vasc Surg*, 2014 Jul;28(5):1149-56. PMID: 24342828.
- (10) Visconti A, Gaeta T, Cabezon M, Briggs W, Pyle M., 2013. Focused Board Intervention (FBI): A Remediation Program for Written Board Preparation

- and the Medical Knowledge Core Competency. *J Grad Med Educ.* 2013 Sep;5(3):464-7. PMID: 24404311.
- (11) Annika Krystyna, D Kumari, R Tenney, R Kosanovic, T Safi, WM Briggs, K Hennessey, M Skelly, E Enriquez, J Lajeune, W Ghani and MD Schwalb, 2013. Hepatitis c antibody testing in African American and Hispanic men in New York City with prostate biopsy. *Oncology Discovery*, Vol 1. DOI: 10.7243/2052-6199-1-1.
 - (12) Ziad Y. Fayad, Elie Semaan, Bashar Fahoum, W. Matt Briggs, Anthony Tortolani, and Marcus D'Ayala, 2013. Aortic mural thrombus in the normal or minimally atherosclerotic aorta: A systematic review and meta-analysis of the available literature. *Ann Vasc Surg.*, Apr;27(3):282-90. DOI:10.1016/j.avsg.2012.03.011.
 - (13) Elizabeth Haines, Gerardo Chiricolo, Kresimir Aralica, William Briggs, Robert Van Amerongen, Andrew Laudenbach, Kevin O'Rourke, and Lawrence Melniker MD, 2012. Derivation of a Pediatric Growth Curve for Inferior Vena Caval Diameter in Healthy Pediatric Patients. *Crit Ultrasound J.* 2012 May 28;4(1):12. doi: 10.1186/2036-7902-4-12.
 - (14) Wei Li, Piotr Gorecki, Elie Semaan, William Briggs, Anthony J. Tortolani, Marcus D'Ayala, 2011. Concurrent Prophylactic Placement of Inferior Vena Cava Filter in gastric bypass and adjustable banding operations: An analysis of the Bariatric Outcomes Longitudinal Database (BOLD). *J. Vascular Surg.* 2012 Jun;55(6):1690-5. doi: 10.1016/j.jvs.2011.12.056.
 - (15) Krystyna A, Kosanovic R, Tenney R, Safi T, Briggs WM, et al. (2011) Colonoscopy Findings in Men with Transrectal Ultrasound Guided Prostate Biopsy: Association of Colonic Lipoma with Prostate Cancer. *J Cancer Sci Ther* S4:002. doi:10.4172/1948-5956.S4-002
 - (16) Birkhahn RH, Wen W, Datillo PA, Briggs WM, Parekh A, Arkun A, Byrd B, Gaeta TJ, 2012. Improving patient flow in acute coronary syndromes in the face of hospital crowding. *J Emerg Med.* 2012 Aug;43(2):356-65. PMID: 22015378.
 - (17) Birkhahn RH, Haines E, Wen W, Reddy L, Briggs WM, Datillo PA., 2011. Estimating the clinical impact of bringing a multimarker cardiac panel to the bedside in the ED. *Am J Emerg Med.* 2011 Mar;29(3):304-8.
 - (18) Krystyna A, Safi T, Briggs WM, Schwalb MD., 2011. Correlation of hepatitis C and prostate cancer, inverse correlation of basal cell hyperplasia or prostatitis and epidemic syphilis of unknown duration. *Int Braz J Urol.* 2011 Mar-Apr;37(2):223-9; discussion 230.
 - (19) Muniyappa R, Briggs WM, 2010. Limited Predictive Ability of Surrogate Indices of Insulin Sensitivity/Resistance in Asian Indian Men: A Calibration Model Analysis. *AJP - Endocrinology and Metabolism.* 299(6):E1106-12. PMID: 20943755.
 - (20) Birkhahn RH, Blomkalns A, Klausner H, Nowak R, Raja AS, Summers R, Weber JE, Briggs WM, Arkun A, Diercks D. The association between money and opinion in academic emergency medicine. *West J Emerg Med.* 2010 May;11(2):126-32. PMID: 20823958.
 - (21) Loizzo JJ, Peterson JC, Charlson ME, Wolf EJ, Altemus M, Briggs WM, Vahdat LT, Caputo TA, 2010. The effect of a contemplative self-healing

- program on quality of life in women with breast and gynecologic cancers. *Altern Ther Health Med.*, May-Jun;16(3):30-7. PMID: 20486622.
- (22) Krystyna A, Safi T, Briggs WM, Schwalb MD, 2010. Higher morbidity in prostate cancer patients after transrectal ultrasound guided prostate biopsy with 3-day oral ciprofloxacin prophylaxis, independent of number of cores. *Brazilian Journal of Urology.* Mar-Apr;37(2):223-9; discussion 230. PMID:21557839.
 - (23) Arkun A, Briggs WM, Patel S, Datillo PA, Bove J, Birkhahn RH, 2010. Emergency department crowding: factors influencing flow *West J Emerg Med.* Feb;11(1):10-5.PMID: 20411067.
 - (24) Li W, D'Ayala M, Hirshberg A, Briggs W, Wise L, Tortolani A, 2010. Comparison of conservative and operative treatment for blunt carotid injuries: analysis of the National Trauma Data Bank. *J Vasc Surg.* Mar;51(3):593-9, 599.e1-2.PMID: 20206804.
 - (25) D'Ayala M, Huzar T, Briggs W, Fahoum B, Wong S, Wise L, Tortolani A, 2010. Blood transfusion and its effect on the clinical outcomes of patients undergoing major lower extremity amputation. *Ann Vasc Surg.*, May;24(4):468-73. Epub 2009 Nov 8.PMID: 19900785.
 - (26) Tavakol M, Hassan KZ, Abdula RK, Briggs W, Oribabor CE, Tortolani AJ, Sacchi TJ, Lee LY, Heitner JF., 2009. Utility of brain natriuretic peptide as a predictor of atrial fibrillation after cardiac operations. *Ann Thorac Surg.* Sep;88(3):802-7.PMID: 19699901.
 - (27) Zandieh SO, Gershel JC, Briggs WM, Mancuso CA, Kuder JM., 2009. Re-visiting predictors of parental health care-seeking behaviors for nonurgent conditions at one inner-city hospital. *Pediatr Emerg Care.*, Apr;25(4):238-243.PMID: 19382324.
 - (28) Birkhahn RH, Blomkalns AL, Klausner HA, Nowak RM, Raja AS, Summers RL, Weber JE, Briggs WM, Arkun A, Diercks D., 2008. Academic emergency medicine faculty and industry relationships. *Acad Emerg Med.*, Sep;15(9):819-24.PMID: 19244632.
 - (29) Westermann H, Choi TN, Briggs WM, Charlson ME, Mancuso CA. Obesity and exercise habits of asthmatic patients. *Ann Allergy Asthma Immunol.* 2008 Nov;101(5):488-94. doi: 10.1016/S1081-1206(10)60287-6.
 - (30) Boutin-Foster C., Ogedegbe G., Peterson J., Briggs M., Allegrante J., Charlson ME., 2008. Psychosocial mediators of the relationship between race/ethnicity and depressive symptoms in Latino and white patients with coronary artery disease. *J. National Medical Association.* **100(7)**, 849-55. PMID: 18672563
 - (31) Charlson ME, Charlson RE, Marinopoulos S, McCulloch C, Briggs WM, Hollenberg J, 2008. The Charlson comorbidity index is adapted to predict costs of chronic disease in primary care patients. *J Clin Epidemiol.* Dec;61(12):1234-40. PMID: 18619805.
 - (32) Mancuso CA, Westermann H, Choi TN, Wenderoth S, Briggs WM, Charlson ME, 2008. Psychological and somatic symptoms in screening for depression in asthma patients. *J. Asthma.* **45(3)**, 221-5. PMID: 18415830.
 - (33) Ullery, BW, JC Peterson, FM, WM Briggs, LN Girardi, W Ko, AJ Tortolani, OW Isom, K Krieger, 2007. Cardiac Surgery in Nonagenarians:

- Should We or Shouldn't We? *Annals of Thoracic Surgery*. **85(3)**, 854-60. PMID: 18291156.
- (34) Mancuso, CA, T Choi, H Westermann, WM Briggs, S Wenderoth, 2007. Patient-reported and Physician-reported Depressive Conditions in Relation to Asthma Severity and Control. *Chest*. **133(5)**, 1142-8. PMID: 18263683.
- (35) Rosenzweig JS, Van Deusen SK, Okpara O, Datillo PA, Briggs WM, Birkhahn RH, 2008. Authorship, collaboration, and predictors of extramural funding in the emergency medicine literature. *Am J Emerg Med*. **26(1)**, 5-9. PMID: 18082774.
- (36) Westermann H, Choi TN, Briggs WM, Charlson ME, Mancuso CA, 2008. Obesity and exercise habits of asthmatic patients. *Ann Allergy Asthma Immunol*. Nov;101(5):488-94. PMID: 19055202.
- (37) Hogle NJ, Briggs WM, Fowler DL, 2007. Documenting a learning curve and test-retest reliability of two tasks on a virtual reality training simulator in laparoscopic surgery. *J Surg Educ*. **64(6)**, 424-30. PMID: 18063281.
- (38) D'Ayala, M, C Martone, R M Smith, WM Briggs, M Potouridis, J S Deitch, and L Wise, 2006. The effect of systemic anticoagulation in patients undergoing angioaccess surgery. *Annals of Vascular Surgery*. **22(1)**, 11-5. PMID: 18055171.
- (39) Charlson ME, Peterson F, Krieger K, Hartman GS, Hollenberg J, Briggs WM, et al., 2007. Improvement of outcomes after coronary artery bypass II: a randomized trial comparing intraoperative high versus customized mean arterial pressure. *J. Cardiac Surgery*. **22(6)**, 465-72. PMID: 18039205.
- (40) Charlson ME, Peterson F, Boutin-Foster C, Briggs WM, Ogedegbe G, McCulloch C, et al., 2008. Changing health behaviors to improve health outcomes after angioplasty: a randomized trial of net present value versus future value risk communication.. *Health Education Research*. **23(5)**, 826-39. PMID: 18025064.
- (41) Charlson, M, Peterson J., Syat B, Briggs WM, Kline R, Dodd M, Murad V, Dione W, 2007. Outcomes of Community Based Social Service Interventions in Homebound Elders *Int. J. Geriatric Psychiatry*. **23(4)**, 427-32. PMID: 17918183.
- (42) Hogle NJ, Briggs WM, Fowler DL. Documenting a learning curve and test-retest reliability of two tasks on a virtual reality training simulator in laparoscopic surgery. *J Surg Educ*. 2007 Nov-Dec;64(6):424-30. PMID: 18063281.
- (43) Mancuso, CA, T Choi, H Westermann, WM Briggs, S Wenderoth, 2007. Measuring physical activity in asthma patients: two-minute walk test, repeated chair rise test, and self-reported energy expenditure. *J. Asthma*. **44(4)**, 333-40. PMID: 17530534.
- (44) Charlson ME, Charlson RE, Briggs W, Hollenberg J, 2007. Can disease management target patients most likely to generate high costs? The impact of comorbidity. *J Gen Intern Med*. **22(4)**, 464-9. PMID: 17372794.
- (45) Charlson ME, Boutin-Foster C, Mancuso CA, Peterson F, Ogedegbe G, Briggs WM, Robbins L, Isen A, Allegrante JP, 2006. Randomized Controlled Trials of Positive Affect and Self-affirmation to Facilitate Healthy

- Behaviors in Patients with Cardiopulmonary Diseases: Rationale, Trial Design, and Methods. *Contemporary Clinical Trials*. **28(6)**, 748-62. PMID: 17459784.
- (46) Charlson ME, Boutin-Foster C., Mancuso C., Ogedegbe G., Peterson J., Briggs M., Allegrante J., Robbins L., Isen A., 2007. Using positive affect and self affirmation to inform and to improve self management behaviors in cardiopulmonary patients: Design, rationale and methods. *Controlled Clinical Trials*. November 2007 (Vol. 28, Issue 6, Pages 748-762).
- (47) Melniker LA, Leibner E, McKenney MG, Lopez P, Briggs WM, Mancuso CA., 2006. Randomized Controlled Clinical Trial of Point-of-Care, Limited Ultrasonography (PLUS) for Trauma in the Emergency Department: The First Sonography Outcomes Assessment Program (SOAP-1) Trial. *Annals of Emergency Medicine*. **48(3)**, 227-235. PMID: 16934640.
- (48) Milling, TJ, C Holden, LA Melniker, WM Briggs, R Birkhahn, TJ Gaeta, 2006. Randomized controlled trial of single-operator vs. two-operator ultrasound guidance for internal jugular central venous cannulation. *Acad Emerg Med.*, **13(3)**, 245-7. PMID: 16495416.
- (49) Milla F, Skubas N, Briggs WM, Girardi LN, Lee LY, Ko W, Tortolani AJ, Krieger KH, Isom OW, Mack CA, 2006. Epicardial beating heart cryoablation using a novel argon-based cryoclamp and linear probe. *J Thorac Cardiovasc Surg.*, **131(2)**, 403-11. PMID: 16434271.
- (50) Birkhahn, SK Van Deusen, O Okpara, PA Datillo, WM Briggs, TJ Gaeta, 2006. Funding and publishing trends of original research by emergency medicine investigators over the past decade. *Annals of Emergency Medicine*, **13(1)**, 95-101. PMID: 16365335.
- (51) Birkhahn, WM Briggs, PA Datillo, SK Van Deusen, TJ Gaeta, 2006. Classifying patients suspected of appendicitis with regard to likelihood. *American Journal of Surgery*, **191(4)**, 497-502. PMID: 16531143
- (52) Charlson ME, Charlson RE, Briggs WM, Hollenberg J, 2006. Can disease management target patients most likely to generate high costs. *J. General Internal Medicine*. **22(4)**, 464-9.
- (53) Milling, TJ, J Rose, WM Briggs, R Birkhahn, TJ Gaeta, JJ Bove, and LA Melniker, 2005. Randomized, controlled clinical trial of point-of-care limited ultrasonography assistance of central venous cannulation: the Third Sonography Outcomes Assessment Program (SOAP-3) Trial. *Crit Care Med*. **33(8)**, 1764-9. PMID: 16096454.
- (54) Garfield JL, Birkhahn RH, Gaeta TJ, Briggs WM, 2004. Diagnostic Delays and Pathways on Route to Operative Intervention in Acute Appendicitis. *American Surgeon*. **70(11)**, 1010-1013. PMID: 15586517.
- (55) Birkhahn RH, Gaeta TJ, Tloczkowski J, Mundy TA, Sharma M, Bove JJ, Briggs WM, 2003. Emergency medicine trained physicians are proficient in the insertion of transvenous pacemakers. *Annals of Emergency Medicine*. **43 (4)**, 469-474. PMID: 15039689.

3.1. Talks (I am years behind updating these).

- (1) Briggs, 2016. The Crisis Of Evidence: Probability & The Nature Of Cause. Institute of Statistical Science, Academia Sinica, Taipei, Taiwan.
- (2) Wei Li, Piotr Gorecki, Robert Autin, William Briggs, Elie Semaan, Anthony J. Tortolani, Marcus D'Ayala, 2011. Concurrent Prophylactic Placement of

- Inferior Vena Cava Filter (CPPOIVCF) in Gastric Bypass and Adjustable Banding Operations: An analysis of the Bariatric Outcomes Longitudinal Database. Eastern Vascular Society 25th Annual Meeting, 2011.
- (3) Wei Li, Jo Daniel, James Rucinski, Syed Gardezi, Piotr Gorecki, Paul Thodiyil, Bashar Fahoum, William Briggs, Leslie Wise, 2010. FACSFactors affecting patient disposition after ambulatory laparoscopic cholecystectomy (ALC) cheanalysis of the National Survey of Ambulatory Surgery (NSAS). American College of Surgeons.
 - (4) Wei Li, Marcus D'Ayala, et al., William Briggs, 2010. Coronary bypass and carotid endarterectomy (CEA): does a combined operative approach offer better outcome? - Outcome of different management strategies in patients with carotid stenosis undergoing coronary artery bypass grafting (CABG). Vascular Annual Meeting.
 - (5) Briggs, WM, 2007. On equi-probable priors, MAX ENT 2007, Saratoga Springs, NY.
 - (6) Briggs, WM, and RA Zaretski, 2006. On producing probability forecasts (from ensembles). 18th Conf. on Probability and Statistics in the Atmospheric Sciences, Atlanta, GA, Amer. Meteor. Soc.
 - (7) Briggs, WM, and RA Zaretski, 2006. Improvements on the ROC Curve: Skill Plots for Forecast Evaluation. *Invited*. Joint Research Conference on Statistics in Quality Industry and Technology, Knoxville, TN.
 - (8) Briggs, WM, and RA Zaretski, 2005. Skill Curves and ROC Curves for Diagnoses, or Why Skill Curves are More Fun. Joint Statistical Meetings, American Stat. Soc., Minneapolis, MN.
 - (9) Briggs W.M., 2005. On the optimal combination of probabilistic forecasts to maximize skill. *International Symposium on Forecasting* San Antonio, TX. International Institute of Forecasters.
 - (10) Briggs, WM, and D Ruppert, 2004. Assessing the skill of yes/no forecasts for Markov observations. 17th Conf. on Probability and Statistics in the Atmospheric Sciences, Seattle, WA, Amer. Meteor. Soc.
 - (11) Melniker, L, E Liebner, B Tiffany, P Lopez, WM Briggs, M McKenney, 2004. Randomized clinical trial of point-of-care limited ultrasonography (PLUS) for trauma in the emergency department. *Annals of Emergency Medicine*, **44**.
 - (12) Birkhahn RH, Gaeta TJ, Van Deusen SK, Briggs WM, 2004. Classifying patients suspected of appendicitis with regard to likelihood. *Annals of Emergency Medicine*, **44** (4): S17-S17 51 Suppl. S.
 - (13) Zandieh, SO, WM Briggs, JM Kuder, and CA Mancuso, 2004. Negative perceptions of health care among caregivers of children auto-assigned to a Medicaid managed care health plan. Ambulatory Pediatric Association Meeting, San Francisco, CA; and National Research Service Award Trainees Conference, San Diego, CA.
 - (14) Melniker, L, E Liebner, B Tiffany, P Lopez, M Sharma, WM Briggs, M McKenney, 2003. Cost Analysis of Point-of-care, Limited Ultrasonography (PLUS) in Trauma Patients: The Sonography Outcomes Assessment Program (SOAP)-1 Trial. *Academic Emergency Medicine*, **11**, 568.

- (15) Melniker, LA, WM Briggs, and CA Mancuso, 2003. Including comorbidity in the assessment of trauma patients: a revision of the trauma injury severity score. *J. Clin Epidemiology*, Sep., **56(9)**, 921. PMID: 14505784.
- (16) Briggs, WM, and RA Levine, 1998. Comparison of forecasts using the bootstrap. 14th Conf. on Probability and Statistics in the Atmospheric Sciences Phoenix, AZ, Amer. Meteor. Soc., 1-4.
- (17) Briggs, WM, and R Zaretski, 1998. The effect of randomly spaced observations on field forecast error scores. 14th Conf. on Probability and Statistics in the Atmospheric Sciences Phoenix, AZ, Amer. Meteor. Soc., 5-8.
- (18) Briggs, WM, and RA Levine, 1996. Wavelets and image comparison: new approaches to field forecast verification. 13th Conf. on Probability and Statistics in the Atmospheric Sciences, San Francisco, CA, Amer. Meteor. Soc., 274-277.
- (19) Briggs, WM, and DS Wilks, 1996. Modifying parameters of a daily stochastic weather generator using long-range forecasts. 13th Conf. on Probability and Statistics in the Atmospheric Sciences, San Francisco, CA, Amer. Meteor. Soc., 243-2246.

EXHIBIT 3

Matt Braynard @MattBraynard · Nov 20
Update:
-Residency Analysis of ABS/EV Voters
These are the two indicators of someone no longer eligible to vote due to residency:
NCOA = Voters who filed change of address to another state.
SVR = Subsequent Voter Registration in another state
Merged = NCOA+SVR Deduped
42 1K 2.1K

Matt Braynard @MattBraynard · Nov 20
State / NCOA / SVR / Merged
AZ / 5,084 / 744 / 5,790
GA / 15,700 / 4926 / 20,311
MI / 12,120 / 1,170 / 13,248
NV / 5,145 / 3,401 / 8,502
PA / 7,426 / 7,051 / 14,477
WI / 6,207 / 765 / 6,966
9 178 493

Matt Braynard @MattBraynard · Nov 20
The SVR component was greatly hampered by the lack of reliable DOB from state voter records and/or commercial vendors, so these numbers are all artificially low. We only matched when we had a full DOB we were confident of.
3 82 397

Matt Braynard @MattBraynard · Nov 20
- Double ABS/EV Voter Analysis
Voters who cast early/absentee in two+ states, and not including anyone who voted in person on E-Day as that data is not widely available. If it were, these numbers would be much higher.
Counts are also artificially low due to DOB issues.
4 82 360

[Matt Braynard on Twitter: "Update: -Residency Analysis of ABS/EV Voters These are the two indicators of someone no longer eligible to vote due to residency: NCOA = Voters who filed change of address to another state. SVR = Subsequent Voter Registration in another state Merged = NCOA+SVR Deduped" / Twitter](#)

EXHIBIT 4

Declaration of [REDACTED]

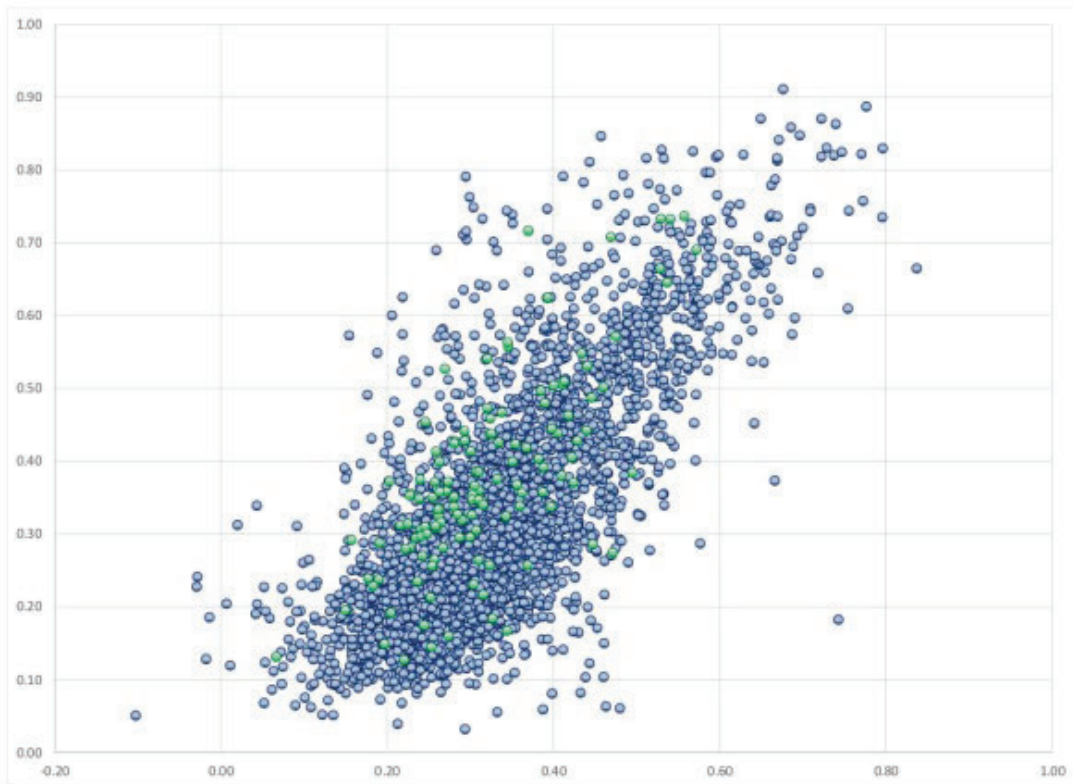
Pursuant to 28 U.S.C Section 1746, I, [REDACTED], make the following declaration.

1. I am over the age of 21 years and am a resident of Monroe County, Florida.
2. I am under no legal disability that would prevent me from giving this declaration.
3. I hold a Bachelor of Science degree in Mathematics and a Master of Science degree in Statistics.
4. For thirty years, I have conducted statistical data analysis for companies in various industries, including aerospace, consumer packaged goods, disease detection and tracking, and fraud detection.
5. From November 13th, 2020 through November 28th, 2020, I conducted in-depth statistical analysis of publicly available data on the 2020 U.S. Presidential Election. This data included vote counts for each county in the United States, U.S. Census data, and type of voting machine data provided by the U.S. Election Assistance Committee.
6. The analysis yielded several “red flags” concerning the percentage of votes won by candidate Biden in counties using voting machines provided by Dominion Voting Systems. These red flags occurred in several States in the country, including possible red flag in Maricopa County, Arizona.
7. I began by using Chi-Squared Automatic Interaction Detection (CHAID), which treats the data in an agnostic way—that is, it imposes no parametric assumptions that could otherwise introduce

bias. Here, I posed the following question: “Do any voting machine types appear to have unusual results?” The answer provided by the statistical technique/algorithm was that machines from Dominion Voting Systems (Dominion) produced abnormal results.

8. Subsequent graphical and statistical analysis shows the unusual pattern involving machines from Dominion occurs in at least 100 counties and multiple States. Since machines from Dominion were used in Maricopa County, it is possible the unusual pattern continues there.
9. The results from most, if not all counties using the Dominion machines is three to five point six percentage points higher in favor of candidate Biden than the results should be. This pattern is seen easily in graphical form when the results from “Dominion” counties are overlaid against results from “non-Dominion” counties. The results from “Dominion” counties do not match the results from the rest of the counties in the United States. The results are certainly statistically significant, with a p-value of < 0.00004 . This translates into a statistical impossibility that something unusual involving Dominion machines is *not* occurring. This pattern appears in multiple States and the margin of votes implied by the unusual activity would easily sway the election results in those States. The margin of votes implied by the unusual pattern would certainly sway the election results in Arizona.
10. The following graph shows the pattern. The x-axis is our predicted percentage candidate Biden should win. The y-axis is the actual percentage Biden won. The green dots are counties in the

United States that use Dominion voting machines. Almost all of them are above an imaginary blue center prediction line, when in normal situations approximately half of them would be below the prediction line (as evidence by approximately half the counties in the U.S. (blue dots) that are below the blue centerline). More easily put, the green dots (counties with Dominion machines) are simply “too high”. The p-value of statistical analysis regarding the centerline for the green dots (Counties with Dominion machines) is 0.000000049, pointing to a statistical impossibility that this is a “random” statistical anomaly. Some external force caused this anomaly.



11. To confirm that Dominion machines were the source of the pattern/anomaly, I conducted further analysis using propensity scoring using U.S. census variables (Including ethnicities, income, professions, population density and other social/economic data) , which was used to place counties into paired groups. Such an analysis is important because one concern could be that counties with Dominion systems are systematically different from their counterparts, so abnormalities in the margin for Biden are driven by other characteristics unrelated to the election.
12. After matching counties using propensity score analysis, the only difference between the groups was the presence of Dominion machines. This approach again showed a highly statistically significant difference between the two groups, with candidate Biden again averaging three percentage points higher in Dominion counties than in the associated paired county. The associated p-value is < 0.00005 , against indicating a statistical impossibility that something unusual is not occurring involving Dominion machines.
13. The results of the analysis and the pattern seen in the included graph strongly suggest a systemic, system-wide algorithm was enacted by an outside agent. Our estimate of the possible impact in Maricopa County is 3 percentage points, causing the results of Arizona's vote tallies to be inflated accordingly.
14. This is based on the residual between Biden's actual vote percentage in Maricopa County and the predicted vote percentage,

which is obtained from a national model using county level data on demographic Census characteristics (e.g., percent white, black, asian, etc, percent self employed, and the industrial composition).

15. The best estimate of impact in Maricopa (only county with Dominion in AZ) is 3%. The national analysis yielded 5.6% as the estimate of impacted votes, which would imply a larger number of votes impacted in AZ. To be more conservative, I defer to 3%.
16. Statistical estimating yields that in Arizona, the best estimate of the number of impacted votes is 62,282. However, calculating a 95% confidence interval from national data yields that as many as 97,576 votes may have been impacted in Arizona.

I declare under penalty of perjury that the forgoing is true and correct.
Executed this November 28th, 2020.

,



11/28/20

EXHIBIT 5

10/25/20

MCTEC Envelope Separation Room —

I had requested to volunteer in Signature Verification as I felt — and still do — it is such an important area. (I was concerned about ballot harvesting.) But there is NO WAY to provide any oversight. (This also lends itself to LESS THAN DESIRABLE oversight.)

Another observation I noted is at each monitor this task is accomplished by an individual, not by a two-person team of one Republican and one Democrat (as in Adjudication).

I worked in both of the Signature Verification rooms as a Republican volunteer observer. We could perform NO EFFECTIVE oversight as we were seated in a small designated area from which we could not move, the majority of the computer monitors were faced away from us, and we could not read the few screens that were turned our way due to distance.

10/25/20 Room 2 and 10/28/20 Room 1

MCTEC Signature Verification Rooms 1 and 2 —

2. While serving as an observer, I personally witnessed the following:

1. I served as an official legal observer of the 2020 general election. I observed at the following location(s): Maricopa County Tabulation and Election Center (MCTEC) and five polling locations in Maricopa County.

I make this Declaration of my own personal knowledge, and I am competent to testify to the matters contained herein.

DECLARATION

EXHIBIT 5 A

The envelope separation room is a huge, long room containing dozens of tables of two-person teams (one Republican and one Democrat) opening ballot envelopes and separating the items. We were escorted to the designated observation area on the left end of the front of the room. The area was a "taped off on the floor", small rectangle containing two chairs, one for a Republican and one for a Democrat observer. We were not allowed to move from this area. The distance was such that NO MEANINGFUL oversight could occur.

Republican Volunteer Poll Observer —

10/07/20 McDowell Square, 5114 W McDowell Rd, Phoenix, AZ 85035
All day we Republican and Democrat observers stood along a wall, unable to walk around to observe most of the functions. The Inspector was Bob.
10/23/20 9201 S Avenida Del Yaqui, Guadalupe, AZ 85283
We Republican and Democrat observers (one each) were seated and not allowed to walk around to observe most of the functions. Additionally, the Inspector Francis brought over a page of the polling locations' rules to two poll workers and then me because we had conversed. She told us we were not allowed to talk AT ALL. The two workers had been discussing dancing and music and I had answered "Big Band music" to a question, "What kind of music was Glenn Miller?" This polling location had a very repressive atmosphere. I felt very unwelcome all day.
10/24/20 & 10/27/20 & 10/31/20 845 West Southern Ave., Phoenix, AZ 85041
We Republican and Democrat observers (one each) were seated and not allowed to walk around to observe most of the functions. However, we were allowed to converse with staff as long as nothing political was said. We all knew that. And we could freely walk around outside. The Inspector Joe fostered a friendly atmosphere and addressed questions.
10/29/20 Fowler School, 6707 W Van Buren St, Phoenix, AZ 85043
We Republican and Democrat observers (one each) were seated to the left in the front of the cafeteria/gym. We were allowed to walk down to observe from afar the ballot printing function. We did not try to walk around to observe the other functions.
11/03/20 Election Day, Horizon Church, 1401 E Liberty Lane, Phoenix, AZ 85048
The Inspector was James. The space was very small — long and narrow. I sat in a designated chair on one wall. I could freely walk around and observe the functions. What I witnessed throughout the day that concerned me was this: a voter would insert their ballot into one of the two on-site tabulators, then the ballot would kick out due

EXHIBIT 5 B

Printed Name: Diane L. Serra

Signature: 

Dated November 25, 2020.

true and correct of my own personal knowledge.

have read the above Declaration, am familiar with its contents, and know the same to be

I declare under penalty of perjury under the laws of the State of Arizona that I

While working in Tabulation, alongside the Democratic volunteer observers Jeff and Robin Greson, I helped select randomly two sample trays for the Hand Count. The trays consisted of 200 ballots each, being run through two different machines: one of the large HPRC tabulators and one of the Canons. This was part of the plan to pull 52 trays/make up 52 sealed boxes, from which 26 boxes would be randomly chosen for the Hand Count. The other 26 would be available if a new set was needed for some reason. What I feel is important is I know the pulling of the 52 trays was completed before Election Day. No Election Day ballots were included in the Hand Count. Jeff Greson would know the date the last boxes were created and sealed. They say the Hand Count was 100% on the money. Perhaps someone could freely manipulate the tabulation of the votes on Election Day if they knew none would be looked at in the Hand Count?

MCTEC Tabulation and Adjudication Room —

to an over-vote. A poll worker (various) would correctly advise the person they could do a whole new ballot or agree to having this race skipped and the rest of the ballot processed. I only saw one voter ask to do a new ballot. I felt the poll workers were verbally steering people/encouraging people to agree to skip the over-vote race, process the rest of the ballot, and leave. I did observe the poll worker press a button on the tabulator. I was not close enough to see what it was.

10/25/20

MCTEC Envelope Separation Room —

I had requested to volunteer in Signature Verification as I felt — and still do — it is such an important area. (I was concerned about ballot harvesting.) But there is NO WAY to provide any oversight. (This also lends itself to LESS THAN DESIRABLE oversight.)

Another observation I noted is at each monitor this task is accomplished by an individual, not by a two-person team of one Republican and one Democrat (as in Adjudication).

I worked in both of the Signature Verification rooms as a Republican volunteer observer. We could perform NO EFFECTIVE oversight as we were seated in a small designated area from which we could not move, the majority of the computer monitors were faced away from us, and we could not read the few screens that were turned our way due to distance.

10/25/20 Room 2 and 10/28/20 Room 1

MCTEC Signature Verification Rooms 1 and 2 —

2. While serving as an observer, I personally witnessed the following:

1. I served as an official legal observer of the 2020 general election. I observed at the following location(s): Maricopa County Tabulation and Election Center (MCTEC) and five polling locations in Maricopa County.

testify to the matters contained herein.

I make this Declaration of my own personal knowledge, and I am competent to

DECLARATION

EXHIBIT 6

STATE OF COLORADO)
County of Douglas) ss.

COMES NOW, Affiant Joseph T. Oltmann, being first duly sworn, under oath, and states under penalty of perjury that the following information is true and accurate within his personal knowledge and belief:

My name Joseph Oltmann. I am over eighteen years of age. I am not suffering under any mental disability and am competent to give this sworn affidavit. I am able to read and write and to give this affidavit voluntarily and on my own free will and accord. No one has used any threats, force, pressure, or intimidation to make me sign this affidavit. I make this affidavit in support of the truth.

I am the CEO of a tech company based just outside of Denver, Colorado. I am also the founder of an organization called FEC United. [Fecunited.com] The goal of this organization is to restore constitutional integrity to our community and empower those in our community to stand up to state and national leadership that intends to suppress the rights of individuals holistically.

Through this organization "FEC" I became a target of journalists who began to slander both me and my organization. I became the topic of Antifa and extremists through my involvement in a movement to resist the narrative that police are bad and our society represented the rhetoric shared by these extremists. As a result of these attacks, I started researching Antifa, BLM, Inc. and their connection to violence and unrest inside of our communities. As a result, I set out to infiltrate Antifa meetings and de-mask those Antifa members who are journalists in the mainstream media in Colorado specifically.

On or about the week of September 27, 2020, I was able to attend an Antifa meeting which appeared to be between Antifa members in Colorado Springs and in Denver Colorado. I cannot verify the connection between the two or the leadership as they were disorganized. Discussions of Our Revolution and Antifa were discussed. Rhetoric of "eliminating fascists" and frustration as to the dwindling of support to rally in the street was evident.

Then I honed in among other conversations key actors in the organization who work for local and state news publications. One such person of interest was Heidi Beedle, identified leader of Our Revolution in El Paso County (Southern Colorado) and Antifa leader of the same area.

Heidi's name is actually Sean Beedle. She is a journalist at Colorado Springs Independent, Colorado Springs Business Journal and a freelance writer for several online publications. Others to remain unnamed in this were present.

The conversation went like this:

Someone identified as "Eric" began to speak. Someone asked who Eric was, and someone else replied "he is the Dominion guy" [paraphrased].

Eric then began to speak after being told to continue, but was interrupted and asked by someone, "What are we going to do if Trump wins this fucking election?"

Eric responded, "Don't worry about the election. Trump is not going to win. I made fucking sure of that.. Hahaha"

Someone responded, "Fucking right."

Eric continued with fortifying the groups and recruiting. I would describe his tone as eccentric and boisterous. I wrote down his name and started to do some research into him.

At the time, I thought that they were so disconnected with reality that they think they can "make sure Trump is not elected."

I started with a simple google search: Keywords: "Eric," "Dominion," "Denver Colorado." The fifth result in organic search returned:

[Dominion Voting Systems | Employee Profiles, Emails, Mutual ...](#)

www.leadcandy.io > company > Dominion-Voting-Syst...

Find people working at Dominion Voting Systems. LeadCandy provides Full ... Denver, Colorado. VIEW FULL PROFILE ... FULL PROFILE. Eric Coomer's photo ...

Above that were results for Eric Schussler- Old Dominion University and Eric E Johnson, Attorney - Sherman & Howard. The first two on organic search however was as follows:

[Dominion - Colorado Secretary of State](#)

www.sos.state.co.us > elections > files > projectPlans
PDF

Sep 9, 2016 — our most recent pilots in the City and County of Denver and Mesa County.
... 1 Democracy Suite is a registered trademark of Dominion Voting Systems. ... Eric
Coomer graduated from the University of California, Berkeley in ...

And

[Eric Coomer's email & phone | Dominion Voting Systems's ...](#)

rocketreach.co › eric-coomer-email_7112825

Location, Denver, Colorado, United States. Work, Director, Market Strategy @ Dominion
Voting Systems Member, Board of Directors @ Friends of Levitt Pavilion ...

I began doing research on Eric Coomer and discovered that Colorado Secretary of state
link the following about Dr. Eric Coomer on page 26:

“Eric Coomer graduated from the University of California, Berkeley in 1997 with a Ph.D. in Nuclear Physics. After working in IT consulting for several years, Eric entered the elections industry in 2005 with Sequoia Voting Systems as Chief Software Architect. After three years with the company, Eric took over all development operations as Vice President of Engineering. When Sequoia was acquired by Dominion Voting Systems in 2010, Eric joined the DVS team as Vice President of US Engineering overseeing development in the Denver, Colorado office.

Recently, Eric has taken over as the Director of Product Strategy driving the creation of next generation products through close collaboration with customers, combined with a deep understanding of technology and the needs of Elections departments throughout the United States and abroad. Eric has been an active participant in the development of the IEEE common data format for Elections systems, as well as the working group for developing standards for Risk-Limiting Audits for elections results. When not designing new products, Eric supports large and small scale customers during Election season.”

I did some cursory research on Eric, but my conclusion was that he was either a part of the government or not relevant to the conversation. In other words, this was not a target I would

identify as being influential in Antifa. My conclusion was based on his credentials of having a PhD in Nuclear Physics. Did not add up for someone with that intelligence. I set it aside and concentrated my focus on the activist journalist who were actually Antifa members.

On October 15, 2020 I spoke at an FEC meeting in Bandimere Speedway. It was a rally around the unconstitutional actions of Jefferson County, Colorado government leadership to hurt Bandimere Speedway. I spoke and before the event started they escorted a suspected Antifa Journalist Erik Maulbetsch [Colorado Recorder] off the premises. In that meeting I talked about outing activist journalists who were Antifa and holding them accountable in our community for attacking organizations like FEC United that serve the community.

These activist journalists frequently slander people of faith, conservatives and call them names that defame them in the community. I had enough and warned that we would call them out by name. Maulbetsch wrote an article reflecting this as he was listening in online and decided to omit details about the meeting, causing the entire journalistic community to wonder if they were on the list. It had a positive effect contrary to their intentions.

On Friday November 6th, I received a forwarded article about Georgia irregularities on the election day. I normally do not read many of these articles because I am inundated with information both from FEC, and my company. I started reading it and noticed Eric Coomer was the spokesperson for a company called Dominion Voting Systems. I immediately stopped and started to go back through my notes to find the info on Eric Coomer. I then started research Dominion Voting Systems. The information became rather scary as everywhere I looked I found Eric's name. Some listing him as VP of Security and others calling him Director of Strategy and Security. I began my search for everything Eric Coomer, Dr. Eric Coomer and any information related to legal filings, RFPs, states using Dominion, Colorado uses and even areas in Colorado that do not use Dominion.

I then turned my attention to Eric Coomer's Facebook profile and page while I gathered information on correlating email addresses, profiles, screen names, etc. Searching Twitter, Reddit, Facebook, 4Chan, etc etc.

I was able to get screenshots of Eric Coomer's Facebook posts going back to 2016. What I discovered was disturbing. Anti-Trump rhetoric, posts referring to: Fuck USA, Fuck the Police, A.C.A.B., posts that were anti Conservative, and even posts being happy someone died. Then the bigger shocker. He reposted the Antifa "Manifesto" letter to Donald Trump. I knew that I had the right guy and someone that was clearly mentally unstable and radical. I started digging into the

code irregularities and tying all of the pieces together with the irregularities and the Dominion uses in the disputed states. The correlation was astonishing. I then found the information related to justifying voting machines being online and his justification that they had “hardware and IP address protection”. This statement by itself is FALSE.

I then attempted to reach out to all sources to bring this information to light. Calling major news stations and attempting to connect with the DOJ.

I took the information to the listeners of an organization that I also own called Conservative Daily. We have a podcast that we do on weekdays. I felt I had enough information and was confident that the Eric on the conference call was the same Eric Coomer that worked for Dominion. I was also confident that given the Facebook and other information I was able to collect that Eric Coomer was interfering with the election and as he admits in one of his posts that people at his company think and feel the same way he does. I began to research his patents, who owns them, the pattern of states they acquired as clients.

I began to research the connection to Diane Feinstein, her husband, campaign manager, Clinton Foundation and became worried that the finger of radicals had taken away the voice of the American people in deciding the election. I used ARIMA analysis to show me trends on data and probability models to prove that they were in fact using code and technology to ghost votes, switch votes or even remove probable ballots completely. Code is random unless it is not. Since we are a data company and understand artificial intelligence and use of neural networks, we understand the capabilities of creating chaos in outcome based on weighted density of probable voters.

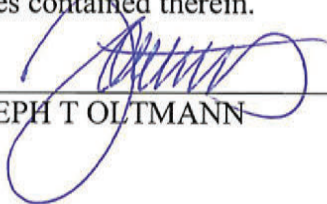
These statements are true and accurate to the best of my knowledge.



Joseph Oltmann

STATE OF COLORADO
COUNTY OF Douglas

Personally appeared before me, LYNN KIEFFER, a Notary Public in and for the aforesaid State and County, JOSEPH T OLTMANN, the within named bargainer, with whom I am personally acquainted and who, after being duly sworn, acknowledged that she executed the foregoing Agreement for the purposes contained therein.




JOSEPH T OLTMANN

Sworn to and subscribed before me this 13th day of November, 2020.

My Commission Expires:

07-24-2021



NOTARY PUBLIC

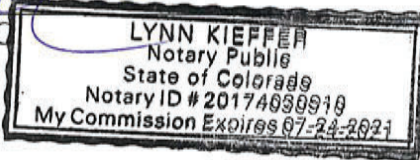


EXHIBIT 7

E
X
H
I
B
I
T

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

DONNA CURLING, ET AL.,)	
)	
Plaintiffs,)	
)	CIVIL ACTION
vs.)	
)	FILE NO. 1:17-cv-2989-AT
BRAD RAFFENSPERGER,)	
ET AL.,)	
)	
Defendants.)	

DECLARATION OF HARRI HURSTI

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

1. My name is Harri Hursti. I am over the age of 21 and competent to give this testimony. The facts stated in this declaration are based on my personal knowledge, unless stated otherwise.

2. My background and qualifications in voting system cybersecurity are set forth in my December 16, 2019 declaration. (Doc. 680-1, pages 37 *et seq*). I stand by everything in that declaration and in my August 21, 2020 declaration. (Doc. 800-2).

3. I am also an expert in ballot scanning because of extensive background in digital imaging prior by work researching election systems. In addition, in 2005 I started an open source project for scanning and auditing paper ballots from images. As a result, I am familiar with different scanner types, how scanner settings and image processing features change the images, and how file format choices affect the quality and accuracy of the ballots.

4. I am engaged as an expert in this case by Coalition for Good Governance.

5. In developing this declaration and opinion, I visited Atlanta to observe certain operations of the June 9, 2020 statewide primary, and the August 11 runoff. During the June 9 election, I was an authorized poll watcher in some locations and was a public observer in others. On August 11, I was authorized as an expert inspecting and observing under the Coalition for Good Governance's Rule 34 Inspection request in certain polling places and the Fulton County Election Preparation Center. As I will explain below in this declaration, my extensive experience in the area of voting system security and my observations of these elections lead to additional conclusions beyond those in my December 16, 2019 declaration. Specifically:

- a) the scanner and tabulation software settings being employed to determine which votes to count on hand marked paper ballots are likely causing clearly intentioned votes not to be counted;
- b) the voting system is being operated in Fulton County in a manner that escalates the security risk to an extreme level; and
- c) voters are not reviewing their BMD printed ballots, which causes BMD generated results to be un-auditable due to the untrustworthy audit trail.

Polling Place Observations

6. Election observation on Peachtree Christian Church. The ballot marking devices were installed so that 4 out of 8 touchscreen devices were clearly visible from the pollbook check in desk. Voter's selections could be effortlessly seen from over 50 ft away.

7. Over period of about 45 minutes, I only observed one voter who appeared to be studying the ballot after picking it up from the printer before casting it in the scanner. When voters do not fully verify their ballot prior to casting, the ballots cannot be considered a reliable auditable record.

8. The scanner would reject some ballots and then accept them after they were rotated to a different orientation. I noted that the scanner would vary in the amount of time that it took to accept or reject a ballot. The delay varied between 3

and 5 seconds from the moment the scanner takes the ballot until the scanner either accepts the ballot or rejects it. This kind of behavior is normal on general purpose operating systems multitasking between multiple applications, but a voting system component should be running only a single application without outside dependencies causing variable execution times.

9. Further research is necessary to determine the cause of the unexpected scanning delays. A system that is dedicated to performing one task repeatedly should not have unexplained variation in processing time. As security researcher, we are always suspicious about any unexpected variable delays, as those are common telltale signs of many issues, including a possibility of unauthorized code being executed. So, in my opinion changes of behaviors between supposedly identical machines performing identical tasks should always be investigated.

When ballots are the same and are produced by a ballot marking device, there should be no time difference whatsoever in processing the bar codes. Variations in time can be the result of many things - one of them is that the scanner encounters an error reading the bar code and needs to utilize error correcting algorithms to recover from that error. Further investigation is

necessary to determine the root cause of these delays, the potential impact of the error correcting algorithms if those are found to be the cause, and whether the delay has any impact upon the vote.

10. Election observation in Central Park Recreation Center. The Poll place manager told me that no Dominion trained technician had reported on location to help them that morning.

11. The ballot marking devices were originally installed in a way that voter privacy was not protected, as anyone could observe across the room how people are voting on about 2/3 devices.

12. The ballot scanner took between 4 and 6 seconds to accept the ballot. I observed only one ballot being rejected.

13. Generally, voters did not inspect the ballots after taking it from the printer and casting it into the scanner.

14. Election observation in Fanplex location. Samantha Whitley and Harrison Thweatt were poll watchers at the Fanplex polling location. They contacted me at approximately 9:10am about problems they were observing with the operation of the BMDs and Poll Pads and asked me to come to help them

understand the anomalies they were observing. I arrived at FanPlex at approximately 9:30am.

15. I observed that the ballot scanner located by a glass wall whereby standing outside of the building observe the scanning, would take between 6 and 7 seconds to either accept or reject the ballot.

16. For reasons unknown, on multiple machines, while voters were attempting to vote, the ballot marking devices sometimes printed “test” ballots. I was not able to take a picture of the ballot from the designated observation area, but I overheard the poll worker by the scanner explaining the issue to a voter which was sent back to the Ballot-Marking Device to pick up another ballot from the printer tray. Test ballots are intended to be used to test the system but without being counted by the system during an election. The ballot scanner in election settings rejects test ballots, as the scanners at FanPlex did. This caused confusion as the voters needed to return to the ballot-marking device to retrieve the actual ballot. Some voters returned the test ballot into the printer tray, potentially confusing the next voter. Had voters been reviewing the ballots at all before taking them to the scanner, they would have noticed the “Test Ballot” text on the ballot. I observed no voter really questioning a poll worker why a “Test” ballot was printed in the first place.

17. Obviously, during the election day, the ballot marking device should not be processing or printing any ballot other than the one the voter is voting. While the cause of the improper printing of ballots should be examined, the fact that this was happening at all is likely indicative of a wrong configuration given to the BMD, which in my professional opinion raises another question: Why didn't the device print only test ballots? And how can the device change its behavior in the middle of the election day? Is the incorrect configuration originating from the Electronic Pollbook System? What are the implications for the reliability of the printed ballot and the QR code being counted?

18. Election observation Park Tavern. The scanner acceptance delay did not vary as it had in previous locations and was consistently about 5 seconds from the moment the scanner takes the ballot, to the moment the scanner either accepts the ballot or rejects it. The variation between scanners at different locations is concerning because these are identical physical devices and should not behave differently while performing the identical task of scanning a ballot.

19. The vast majority of voters at Park Tavern did not inspect the ballots after taking them from the printer and before casting them in the scanner.

Fulton Tabulation Center Operation-Election Night, August 11, 2020

20. In Fulton County Election Preparation Center (“EPC”) on election night I reviewed certain operations as authorized by Rule 34 inspection.

21. I was permitted to view the operations of the upload of the memory devices coming in from the precincts to the Dominion Election Management System (“EMS”) server. The agreement with Fulton County was that I could review only for a limited period of time; therefore, I did not review the entire evening’s process. Also, Dominion employees asked me to move away from the monitors containing the information and messages from the upload process and error messages, limiting my ability to give a more detailed report with documentation and photographs of the screens. However, my vantage point was more than adequate to observe that system problems were recurring and the Dominion technicians operating the system were struggling with the upload process.

22. It is my understanding the same EMS equipment and software had been used in Fulton County’s June 9, 2020 primary election.

23. It is my understanding that the Dominion technician (“Dominic”) charged with operating the EMS server for Fulton County had been performing

these duties at Fulton County for several months, including during the June 9 primary.

24. During my August 11 visit, and a follow-up visit on August 17, I observed that the EMS server was operated almost exclusively by Dominion personnel, with little interaction with EPC management, even when problems were encountered. In my conversations with Derrick Gilstrap and other Fulton County Elections Department EPC personnel, they professed to have limited knowledge of or control over the EMS server and its operations.

25. Outsourcing the operation of the voting system components directly to the voting system vendors' personnel is highly unusual in my experience and of grave concern from a security and conflict of interest perspective. Voting system vendors' personnel have a conflict of interest because they are not inclined to report on, or address, defects in the voting systems. The dangers this poses is aggravated by the absence of any trained County personnel to oversee and supervise the process.

26. In my professional opinion, the role played by Dominion personnel in Fulton County, and other counties with similar arrangements, should be considered an elevated risk factor when evaluating the security risks of Georgia's voting system.

27. Based on my observations on August 11 and August 17, Dell computers running the EMS that is used to process Fulton county votes appeared not to have been hardened.

28. In essence, hardening is the process of securing a system by reducing its surface of vulnerability, which is larger when a system performs more functions; in principle it is to reduce the general purpose system into a single-function system which is more secure than a multipurpose one. Reducing available ways of attack typically includes changing default passwords, the removal of unnecessary software, unnecessary usernames or logins, grant accounts and programs with the minimum level of privileges needed for the tasks and create separate accounts for privileged operations as needed, and the disabling or removal of unnecessary services.

29. Computers performing any sensitive and mission critical tasks such as elections should unquestionably be hardened. Voting system are designated by the Department of Homeland Security as part of the critical infrastructure and certainly fall into the category of devices which should be hardened as the most fundamental security measure. In my experience, it is unusual, and I find it unacceptable for an EMS server not to have been hardened prior to installation.

30. The Operating System version in the Dominion Election Management computer, which is positioned into the rack and by usage pattern appears to be the main computer, is Windows 10 Pro 10.0.14393. This version is also known as the Anniversary Update version 1607 and it was released August 2, 2016. Exhibit A is a true and correct copy of a photograph that I took of this computer.

31. When a voting system is certified by the EAC, the Operating System is specifically defined, as Windows 10 Pro was for the Dominion 5.5-A system. Unlike consumer computers, voting systems do not and should not receive automatic “upgrades” to newer versions of the Operating System. without undergoing tests for conflicts with the new operating system software.

32. That computer and other computers used in Georgia’s system for vote processing appear to have home/small business companion software packages included. Exhibits B and C are true and correct copies of photographs that I took of the computer located in the rack and the computer located closest to the rack on the table to the right. The Start Menu shows a large number of game and entertainment software icons. As stated before, one of the first procedures of hardening is removal of all unwanted software, and removal of those game icons and the associated games and installers alongside with all other software which is not absolutely needed in the computer for election processing purposes would be

one of the first and most basic steps in the hardening process. In my professional opinion, independent inquiry should be promptly made of all 159 counties to determine if the Dominion systems statewide share this major deficiency.

33. Furthermore, when I asked the Dominion employee Dominic assigned to the Fulton County election server operation about the origin of the Windows operating system, he answered that he believed that “it has been provided by the State.”

34. Since Georgia’s Dominion system is new, it is a reasonable assumption that all machines in the Fulton County election network had the same version of Windows installed. However, not only the two computers displayed different entertainment software icons, but additionally one of the machines in Fulton’s group of election servers had an icon of computer game called “*Homescapes*” which is made by Playrix Holding Ltd., founded by Dmitry and Igor Bukham in Vologda, Russia. Attached as Exhibit C is a true and correct copy of a photograph that I took of the Fulton voting system computer” Client 02”. The icon for *Homescapes* is shown by the arrow on Exhibit C.

35. The *Homescapes* game was released in August 2017, one year after Fulton County’s operating system release. If the *Homescapes* game came with the operating system it would be unusual, because at the time of the release of

Homescares, Microsoft had already released 3 major Microsoft Windows 10 update releases after build 14393 and before the release of that game. This calls into question whether all Georgia Dominion system computers have the same operating system version, or how the game has come to be having a presence in Fulton's Dominion voting system.

36. Although this Dominion voting system is new to Georgia, the Windows 10 operating system of at least the 'main' computer in the rack has not been updated for 4 years and carries a wide range of well-known and publicly disclosed vulnerabilities. At the time of this writing, The National Vulnerability Database maintained by National Institute of Standards and Technology lists 3,177 vulnerabilities mentioning "Windows 10 Pro" and 203 vulnerabilities are specifically mentioning "Windows 10 Pro 1607" which is the specific version number of the build 14393 that Dominion uses.

37. Even without internet connectivity, unhardened computers are at risk when those are used to process removable media. It was clear that when Compact Flash storage media containing the ballot images, audit logs and results from the precinct scanners were connected to the server, the media was automounted by the operating system. When the operating system is automounting a storage media, the operating system starts automatically to interact with the device. The zero-day

vulnerabilities exploiting this process has been recurrently discovered from all operating systems, including Windows. Presence of automount calls also into question presence of another setting which is always disabled in hardening process. It is autorun, which automatically executes some content on the removable media. While this is convenient for consumers, it poses extreme security risk.

38. Based on my experience and mental impression observing the Dominion technician's activities, Fulton County's EMS server management seems to be an *ad hoc* operation with no formalized process. This was especially clear on the manual processing of the memory cards storage devices coming in from the precincts on election night and the repeated access of the operating system to directly access filesystem, format USB devices, etc. This kind of operation is naturally prone to human errors. I observed personnel calling on the floor asking if all vote carrying compact flash cards had been delivered from the early voting machines for processing, followed by later finding additional cards which had been overlooked in apparent human error. Later, I heard again one technician calling on the floor asking if all vote carrying compact flashes had been delivered. This clearly demonstrates lack of inventory management which should be in place to ensure, among other things, that no rogue storage devices would be inserted into the computer. In response, 3 more compact flash cards were hand-delivered. Less

than 5 minutes later, I heard one of the county workers say that additional card was found and was delivered for processing. All these devices were trusted by printed label only and no comparison to an inventory list of any kind was performed.

39. In addition, operations were repeatedly performed directly on the operating system. Election software has no visibility into the operations performed directly on the operating system, and therefore those are not included in election system event logging. Those activities can only be partially reconstructed from operating system logs – and as these activities included copying election data files, election software log may create false impression that the software is accessing the same file over a period of time, while in reality the file could had been replaced with another file with the same name by activities commanded to the operating system. Therefore, any attempt to audit the election system operated in this manner must include through analysis of all operating system logs, which complicates the auditing process. Unless the system is configured properly to collect file system auditing data is not complete. As the system appears not to be hardened, it is unlikely that the operating system has been configured to collect auditing data.

40. A human error when operating live election system from the operating system can result in a catastrophic event destroying election data or even rendering the system unusable. Human error is likely given the time pressure involved and,

at least in Fulton County, no formal check lists or operating procedures were followed to mitigate the human error risk. The best practice is to automate trivial tasks to reduce risk of human error, increase the quality assurance of overall operations and provide auditability and transparency by logging.

41. Uploading of memory cards had already started before I arrived at EPC. While one person was operating the upload process, the two other Dominion employees were troubleshooting issues which seemed to be related to ballot images uploads. I repeatedly observed error messages appearing on the screen of the EMS server. I was not able to get picture of the errors on August 11th, I believe the error was the same or similar that errors recurring August 17th as shown on Exhibit D and discussed later in this declaration. Dominion employees were troubleshooting the issue with ‘trial-and-error’ approach. As part of this effort they accessed “Computer Management” application of Windows 10 and experimented with trouble shooting the user account management feature. This demonstrates that they had complete access to the computer. This means there are no meaningful access separation and privileges and roles controls protecting the county’s primary election servers. This also greatly amplifies the risk of catastrophic human error and malicious program execution.

42. I overheard the Dominion technician's conversation that they had issues with file system structure and "need 5 files out of EMS server and paste. Delete everything out of there and put it there." To communicate the gravity of the situation to each other they added "Troubleshooting in the live environment". These conversations increased the mental image that they were not familiar the issue they were troubleshooting.

43. After about 45 minutes of trying to solve the issue by instructions received over the phone, the two Dominion employees' (who had been troubleshooting) behavior changed. The Dominion staff member walked behind the server rack and made manual manipulations which could not be observed from my vantage point. After that they moved with their personal laptops to a table physically farther away from the election system and stopped trying different ways to work around the issue in front of the server, and no longer talked continuously with their remote help over phone.

44. In the follow-up-calls I overheard them ask people on the other end of the call to check different things, and they only went to a computer and appeared to test something and subsequently take a picture of the computer screen with a mobile phone and apparently send it to a remote location.

45. Based on my extensive experience, this all created a strong mental impression that the troubleshooting effort was being done remotely over remote access to key parts of the system. Additionally, new wireless access point with a hidden SSID access point name appeared in the active Wi-Fi stations list that I was monitoring, but it may have been co-incidental. Hidden SSIDs are used to obscure presence of wireless networking from casual observers, although they do not provide any real additional security.

46. If in fact remote access was arranged and granted to the server, this has gravely serious implications for the security of the new Dominion system. Remote access, regardless how it is protected and organized is always a security risk, but furthermore it is transfer of control out of the physical perimeters and deny any ability to observe the activities.

47. I also observed USB drives marked with the Centon DataStick Pro Logo with no visible inventory control numbering system being taken repeatedly from the EMS server rack to the Fulton managers' offices and back. The Dominion employee told me that the USB drives were being taken to the Election Night Reporting Computer in another office. This action was repeated several times during the time of my observation. Carrying generic unmarked and therefore unidentifiable media out-of-view and back is a security risk – especially when the

exact same type of devices was piled on the desk near the computer. During the election night, the Dominion employees reached to storage box and introduced more unmarked storage devices into the ongoing election process. I saw no effort made to maintain a memory card inventory control document or chain of custody accounting for memory cards from the precincts.

48. I also visited the EPC on August 17. During that visit, the staff working on uploading ballots for adjudication experienced an error which appeared similar to the one on election night. This error was repeated with multitude of ballots and at the time we left the location, the error appeared to be ignored, rather than resolved. (EXHIBIT D - the error message and partial explanation of the error being read by the operator.).

49. The security risks outlined above – operating system risks, the failure to harden the computers, performing operations directly on the operating systems, lax control of memory cards, lack of procedures, and potential remote access, are extreme and destroy the credibility of the tabulations and output of the reports coming from a voting system.

50. Such a risk could be overcome if the election were conducted using hand marked paper ballots, with proper chain of custody controls. For elections conducted with hand marked paper ballots, any malware or human error involved

in the server security deficiencies or malfunctions could be overcome with a robust audit of the hand marked paper ballots and in case of irregularities detected, remedied by a recount. However, given that BMD ballots are computer marked, and the ballots therefore unauditible for determining the result, no recovery from system security lapses is possible for providing any confidence in the reported outcomes.

Ballot Scanning and Tabulation of Vote Marks

51. I have been asked to evaluate the performance and reliability of Georgia's Dominion precinct and central count scanners in the counting of votes on hand marked paper ballots.

52. On or about June 10th, Jeanne Dufort and Marilyn Marks called me to seek my perspective on what Ms. Dufort said she observed while serving as a Vote Review Panel member in Morgan County. Ms. Dufort told me that she observed votes that were not counted as votes nor flagged by the Dominion adjudication software.

53. Because of the ongoing questions this raised related to the reliability of the Dominion system tabulation of hand marked ballots, I was asked by Coalition Plaintiffs to conduct technical analysis of the scanner and tabulation accuracy. That analysis is still in its early stages.

54. Before addressing the particulars of my findings and research into the accuracy of Dominion's scanning and tabulation, I will address the basic process by which an image on a voted hand marked paper ballot is processed by scanner and tabulation software generally. It is important to understand that the Dominion scanners are Canon off the shelf scanners and their embedded software were designed for different applications than ballot scanning which is best conducted with scanners specifically designed for detecting hand markings on paper ballots.

55. Contrary of public belief, the scanner is not taking a picture of the paper. The scanner is illuminating the paper with a number of narrow spectrum color lights, typically 3, and then using software to produce an approximation what the human eye would be likely to see if there would had been a single white wide-spectrum light source. This process takes place in partially within the scanner and embedded software in the (commercial off the shelf) scanner and partially in the driver software in the host computer. It is guided by number of settings and configurations, some of which are stored in the scanner and some in the driver software. The scanner sensors gather more information than will be saved into the resulting file and another set of settings and configurations are used to drive that part of the process. The scanners also produce anomalies which are automatically removed from the images by the software. All these activities are performed

outside of the Dominion election software, which is relying on the end product of this process as the input.

56. I began reviewing Dominion user manuals in the public domain to further investigate the Dominion process.

57. On August 14, I received 2 sample Fulton County August 11 ballots of high-speed scanned ballot from Rhonda Martin, who stated that she obtained them from Fulton County during Coalition Plaintiff's discovery. The image characteristics matched the file details I had seen on the screen in EPC. The image is TIFF format, about 1700 by 2200 pixels with 1-bit color depth (= strictly black or white pixels only) with 200 by 200 dots per square inch ("dpi") resolution resulting in files that are typically about 64 or 73 kilo bytes in size for August 11 ballots. With this resolution, the outer dimension of the oval voting target is about 30 by 25 pixels. The oval itself (that is, the oval line that encircles the voting target) is about 2 pixels wide. The target area is about 450 pixels; the area of the target a tight bounding box would be 750 pixels and the oval line encircling the target is 165 pixels. In these images, the oval itself represented about 22% value in the bounding box around the vote target oval.

58. Important image processing decisions are done in scanner software and before election software threshold values are applied to the image. These

scanner settings are discussed in an excerpt Dominion's manual for ICC operations. My understanding is that the excerpt of the Manual was received from Marilyn Marks who stated that she obtained it from a Georgia election official in response to an Open Records request. Attached as Exhibit E is page 9 of the manual. Box number 2 on Exhibit E shows that the settings used are not neutral factory default settings.

59. Each pixel of the voters' marks on a hand marked paper ballot will be either in color or gray when the scanner originally measures the markings. The scanner settings affect how image processing turns each pixel from color or gray to either black or white in the image the voting software will later process. This processing step is responsible for major image manipulation and information reduction before the election software threshold values are calculated. This process has a high risk of having an impact upon how a voter mark is interpreted by the tabulation software when the information reduction erases markings from the scanned image before the election software processes it.

60. In my professional opinion, any decision by Georgia's election officials about adopting or changing election software threshold values is premature before the scanner settings are thoroughly tested, optimized and locked.

61. The impact of the scanner settings is minimal for markings made with a black felt pen but can be great for markings made with any color ballpoint pens. To illustrate this, I have used standard color scanning settings and applied then standard conversion from a scanned ballot vote target with widely used free and open source image processing software “GNU Image Manipulation Program version 2.10.18” EXHIBIT G shows the color image being converted with the software’s default settings from color image to Black-and-White only. The red color does not meet the internal conversion algorithm criteria for black, therefore it gets erased to white instead.

62. Dominion manual for ICC operations clearly show that the scanner settings are changed from neutral factory default settings. EXHIBIT H shows how these settings applied different ways alter how a blue marking is converted into Black-and-White only image.

63. The optimal scanner settings are different for each model of scanner and each type of paper used to print ballots. Furthermore, because scanners are inherently different, the manufacturers use hidden settings and algorithms to cause neutral factory settings to produce similar baseline results across different makes and models. This is well-studied topic; academic and image processing studies published as early as 1979 discuss the brittleness of black-or-white images in

conversion. Subsequently, significance for ballot counting has been discussed in academic USENIX conference peer-reviewed papers.

64. On the August 17th at Fulton County Election Preparation Center Professor Richard DeMillo and I participated in a scan test of August 11 test ballots using a Fulton County owned Dominion precinct scanner. Two different ballot styles were tested, one with 4 races and one with 5 races. Attached as Exhibits I and J show a sample ballots with test marks.

65. A batch of 50 test ballots had been marked by Rhonda Martin with varying types of marks and varying types of writing instruments that a voter might use at home to mark an absentee ballot. Professor DeMillo and I participated in marking a handful of ballots.

66. Everything said here concerning the August 17 test is based on a very preliminary analysis. The scanner took about 6 seconds to reject the ballots, and one ballot was only acceptable “headfirst” while another ballot only “tail first.” Ballot scanners are designed to read ballots “headfirst” or “tail first,” and front side and backside and therefore there should not be ballots which are accepted only in one orientation. I observed the ballots to make sure that both ballots had been cleanly separated from the stub and I could not identify any defects of any kind on the ballots.

67. There was a 15 second cycle from the time the precinct scanner accepted a ballot to the time it was ready for the next ballot. Therefore, the maximum theoretical capacity with the simple 5 race ballot is about 4 ballots per minute if the next ballot is ready to be fed into the scanner as soon as the scanner was ready to take it. In a real-world voting environment, it takes considerably longer because voters move away from the scanner, the next voter must move in and subsequently figure where to insert the ballot. The Dominion precinct scanner that I observed was considerably slower than the ballot scanners I have tested over the last 15 years. This was done with a simple ballot, and we did not test how increase of the number of races or vote targets on the ballot would affect the scanning speed and performance.

68. Though my analysis is preliminary, this test reveals that a significant percentage of filled ovals that would to a human clearly show voter's intent failed to register as a vote on the precinct count scanner.

69. The necessary testing effort has barely begun at the time of this writing, as only limited access to equipment has been made available. I have not had access to the high-volume mail ballot scanner that is expected to process millions of mail ballots in Georgia's upcoming elections. However, initial results suggest that significant revisions must be made in the scanning settings to avoid a

widespread failure to count certain valid votes that are not marked as filled in ovals. Without testing, it is impossible to know, if setting changes alone are sufficient to cure the issue.

Scanned Ballot Tabulation Software Threshold Settings

70. Georgia is employing a Dominion tabulation software tool called “Dual Threshold Technology” for “marginal marks.” (See Exhibit M) The intent of the tool is to detect voter marks that could be misinterpreted by the software and flag them for review. While the goal is admirable, the method of achieving this goal is quite flawed.

71. While it is compelling from development cost point of view to use commercial off the shelf COTS scanners and software, it requires additional steps to ensure that the integration of the information flow is flawless. In this case, the software provided by the scanner manufacturer and with settings and configurations have great impact in how the images are created and what information is removed from the images before the election software processes it. In recent years, many defective scanner software packages have been found. These software flaws include ‘image enhancement’ features which have remained enabled even when the feature has been chosen to be disabled from the scanner software provided by the manufacturer. An example of dangerous feature to keep

enabled is ‘Punch Hole Removal’, intended to make images of documents removed from notebook binders to look more aesthetically pleasing. The software can and in many cases will misinterpret a voted oval as a punch hole and erase the vote from the image file and to make this worse, the punch holes are expected to be found only in certain places near the edge of the paper, and therefore it will erase only votes from candidates whose targets are in those target zones.

72. Decades ago, when computing and storage capacity were expensive black-and-white image commonly meant 1-bit black-or-white pixel images like used by Dominion system. As computer got faster and storage space cheaper during the last 2-3 decades black-and-white image has become by default meaning 255 shades of gray grayscale images. For the purposes of reliable digitalization of physical documents, grayscale image carries more information from the original document for reliable processing and especially when colored markings are being processed. With today’s technology, the difference in processing time and storage prices between grayscale and 1-bit images has become completely meaningless, and the benefits gained in accuracy are undeniable.

73. I am aware that the Georgia Secretary of State’s office has stated that Georgia threshold settings are national industry standards for ballot scanners (Exhibit K). This is simply untrue. If, there were an industry standard for that, it

would be part of EAC certification. There is no EAC standard for such threshold settings. As mentioned before, the optimal settings are products of many elements. The type of the scanner used, the scanner settings and configuration, the type of the paper used, the type of the ink printer has used in printing the ballots, color dropout settings, just to name few. Older scanner models, which were optical mark recognitions scanners, used to be calibrated using calibration sheet – similar process is needed to be established for digital imaging scanners used this way as the ballot scanners.

74. Furthermore, the software settings in Exhibit E box 2 show that the software is instructed to ignore all markings in red color (“Color drop-out: Red”), This clearly indicates that the software was expecting the oval to be printed in Red and therefore it will be automatically removed from the calculation. The software does not anticipate printed black ovals as used in Fulton County. Voters have likely not been properly warned that any pen they use which ink contains high concentration of red pigment particles is at risk of not counting, even if to the human eye the ink looks very dark.

75. I listened to the August 10 meeting of the State Board of Elections as they approved a draft rule related to what constitutes a vote, incorporating the following language:

Ballot scanners that are used to tabulate optical scan ballots marked by hand shall be set so that:

- 1. Detection of 20% or more fill-in of the target area surrounded by the oval shall be considered a vote for the selection;*
- 2. Detection of less than 10% fill-in of the target area surrounded by the oval shall not be considered a vote for that selection;*
- 3. Detection of at least 10% but less than 20% fill-in of the target area surrounded by the oval shall flag the ballot for adjudication by a vote review panel as set forth in O.C.G.A. 21-2-483(g). In reviewing any ballot flagged for adjudication, the votes shall be counted if, in the opinion of the vote review panel, the voter has clearly and without question indicated the candidate or candidates and answers to questions for which such voter desires to vote.*

76. The settings discussed in the rule are completely subject to the scanner settings. How the physical marking is translated into the digital image is determined by those values and therefore setting the threshold values without at the same time setting the scanner settings carries no value or meaning. If the ballots will be continuing to be printed with black only, there is no logic in having any drop-out colors.

77. Before the State sets threshold standards for the Dominion system, extensive testing is needed to establish optimal configuration and settings for each step of the process. Also, the scanners are likely to have settings additional configuration and settings which are not visible menus shown in the manual excerpt. All those should be evaluated and tested for all types of scanners approved for use in Georgia, including the precinct scanners

78. As temporary solution, after initial testing, the scanner settings and configuration should be locked and then a low threshold values should be chosen. All drop-out colors should be disabled. This will increase the number of ballots chosen for human review and reduce the number of valid votes not being counted as cast.

Logic and Accuracy Testing

79. Ballot-Marking Device systems inherits the same well-documented systemic security issues embedded in direct-recording electronic (DRE) voting machine design. Such design flaws eventually are causing the demise of DRE voting system across the country as it did in Georgia. In essence the Ballot Marking Device is a general-purpose computer running a general-purpose operating system with touchscreen that is utilized as a platform to run a software, very similar to DRE by displaying a ballot to the voter and recording the voter's intents. The main difference is that instead of recording those internally digitally, it prints out a ballot summary card of voter's choices.

80. Security properties of this approach would be positively different from DREs if the ballot contained only human-readable information and all voters are required to and were capable of verifying their choices from the paper ballot summary. That of course is unrealistic.

81. When voter fails to inspect the paper ballot and significant portion of the information is not in human readable from as a QR barcode, Ballot-Marking Device based voting effectively inherits most of the negative and undesirable security and reliability properties directly from DRE paradigm, and therefore should be subject to the same testing requirements and mitigation strategies as DREs.

82. In response to repeating myriad of issues with DREs, which have been attributed to causes from screen calibration issues to failures in ballot definition configuration distribution, a robust Logic & Accuracy testing regulation have been established. These root causes are present in BMDs and therefore should be evaluated in the same way as DREs have been.

I received the Georgia Secretary of State's manual "Logic and Accuracy Procedures" "Version 1.0 January 2020 from Rhonda Martin. Procedure described in section D "Testing the BMD and Printer" is taking significant shortcuts, presumably to cut the labor work required. (Section D is attached as Exhibit L) These shortcuts significantly weaken the security and reliability posture of the system and protections against already known systemic pitfalls, usability predicaments and security inadequacies.

CONCLUSIONS

83. The scanner software and tabulation software settings and configurations being employed to determine which votes to count on hand marked paper ballots are likely causing clearly intentioned votes not to be counted as cast.

84. The method of using 1-bit images and calculated relative darkness values from such pre-reduced information to determine voter marks on ballots is severely outdated and obsolete. It artificially and unnecessarily increases the failure rates to recognize votes on hand-marked paper ballots. As a temporary mitigation, optimal configurations and settings for all steps of the process should be established after robust independent testing to mitigate the design flaw and augment it with human assisted processes, but that will not cure the root cause of the software deficiency which needs to be addressed.

85. The voting system is being deployed, configured and operated in Fulton County in a manner that escalates the security risk to an extreme level and calls into question the accuracy of the election results. The lack of well-defined process and compliance testing should be addressed immediately using independent experts. The use and the supervision of the Dominion personnel operating Fulton County's Dominion Voting System should be evaluated.

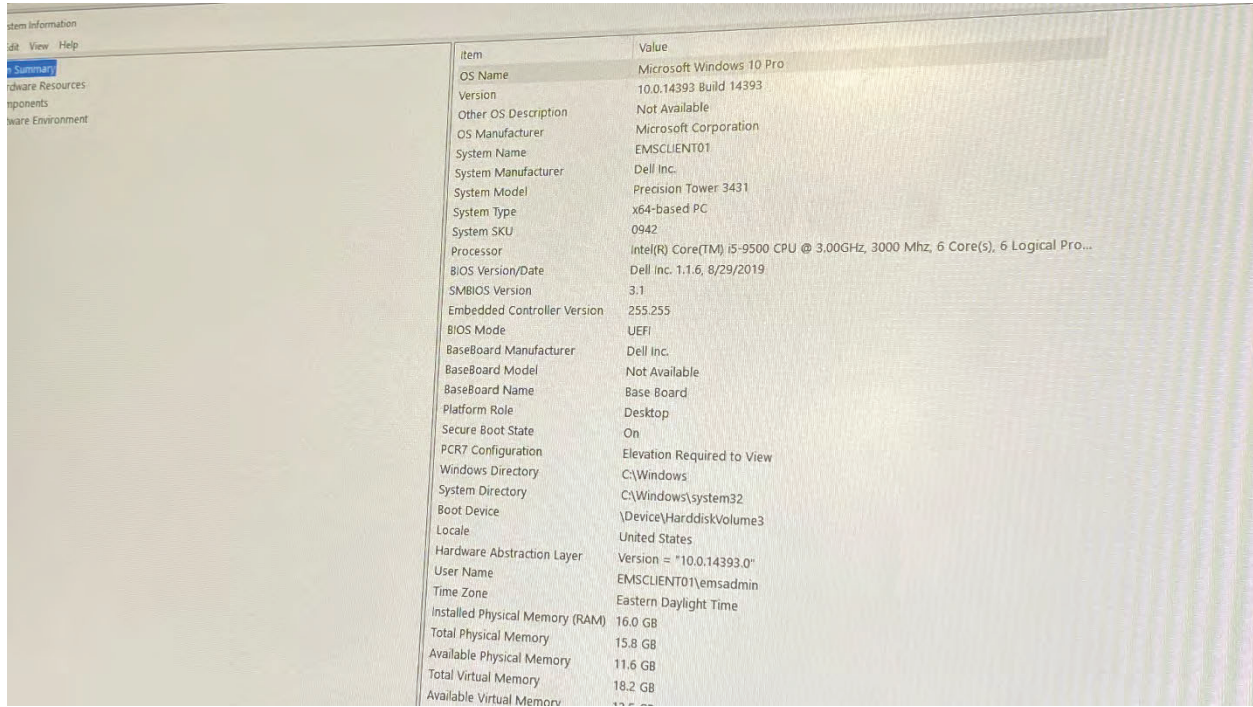
86. Voters are not reviewing their BMD printed ballots before scanning and casting them, which causes BMD-generated results to be un-auditable due to the untrustworthy audit trail. Furthermore, because BMDs are inheriting known fundamental architectural deficiencies from DREs, no mitigation and assurance measures can be weakened, including but not limited to Logic and Accuracy Testing procedures.

This 24th day of August 2020.



Harri Hursti

EXHIBIT A:



The image shows a screenshot of the Windows System Information utility. The window title is "System Information" and it has a menu bar with "File", "View", and "Help". On the left side, there is a navigation pane with the following items: "Summary" (highlighted in blue), "Hardware Resources", "Components", and "Software Environment". The main area displays a list of system information items and their corresponding values.

Item	Value
OS Name	Microsoft Windows 10 Pro
Version	10.0.14393 Build 14393
Other OS Description	Not Available
OS Manufacturer	Microsoft Corporation
System Name	EMSCIENT01
System Manufacturer	Dell Inc.
System Model	Precision Tower 3431
System Type	x64-based PC
System SKU	0942
Processor	Intel(R) Core(TM) i5-9500 CPU @ 3.00GHz, 3000 Mhz, 6 Core(s), 6 Logical Pro...
BIOS Version/Date	Dell Inc. 1.1.6, 8/29/2019
SMBIOS Version	3.1
Embedded Controller Version	255.255
BIOS Mode	UEFI
BaseBoard Manufacturer	Dell Inc.
BaseBoard Model	Not Available
BaseBoard Name	Base Board
Platform Role	Desktop
Secure Boot State	On
PCR7 Configuration	Elevation Required to View
Windows Directory	C:\Windows
System Directory	C:\Windows\system32
Boot Device	\Device\HarddiskVolume3
Locale	United States
Hardware Abstraction Layer	Version = "10.0.14393.0"
User Name	EMSCIENT01\emsadmin
Time Zone	Eastern Daylight Time
Installed Physical Memory (RAM)	16.0 GB
Total Physical Memory	15.8 GB
Available Physical Memory	11.6 GB
Total Virtual Memory	18.2 GB
Available Virtual Memory	12.2 GB

EXHIBIT B:



EXHIBIT C:

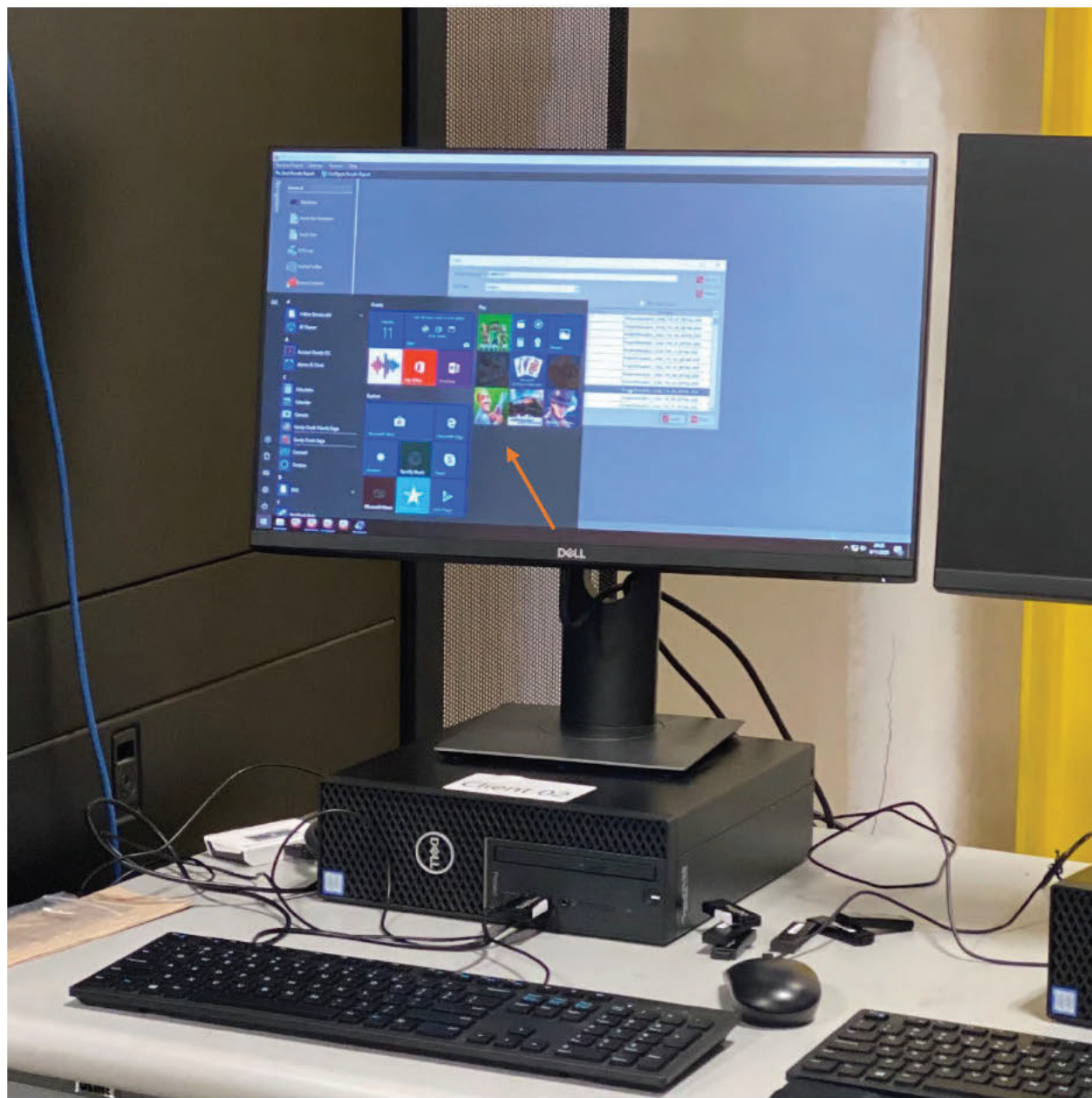


EXHIBIT D:

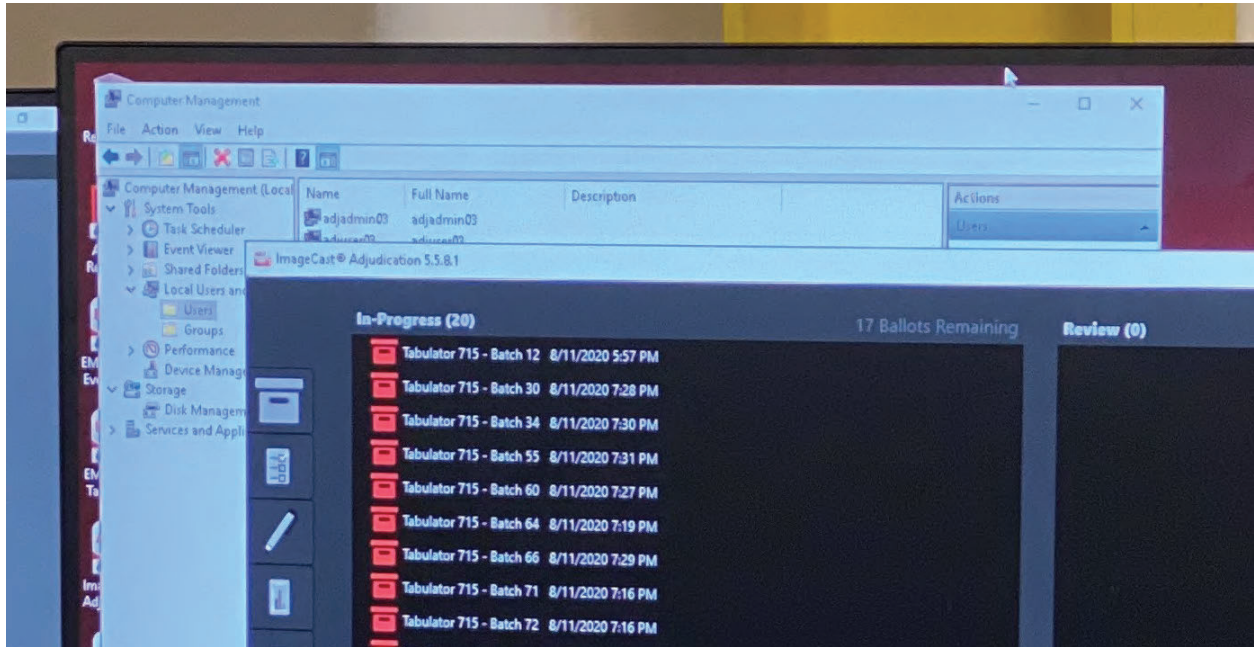


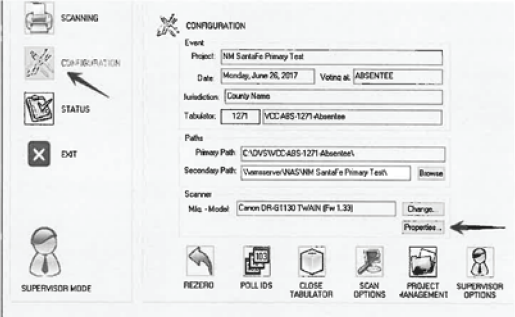
EXHIBIT E:

ICC SCANNER DRIVER SETTINGS

DOMINION VOTING

1

1. Click on the **ADMINISTRATOR MODE** icon in the lower left corner of the window. Enter the Supervisor password.
2. Click the **CONFIGURATION** button option on the left side of the window then click the **Properties** button located in the lower **Scanner** section.



2 Verify/select the following settings:

- a. **Color Drop-out:** Red
- b. **Detect by Length:** Not selected
- c. **Detect by Ultrasonic:** Selected
- d. **Deskew:** Selected
- e. **Edge Cleanup:** Selected
- f. **Doc Orientation:** Portrait
- g. **Brightness:** Set to 90
- h. **Contrast:** 4
- i. **Gamma:** Not selected
- j. **Moire Reduction:** Not selected
- k. **Imprinter:** Not selected

Click the **Apply** button then click the **OK** button.

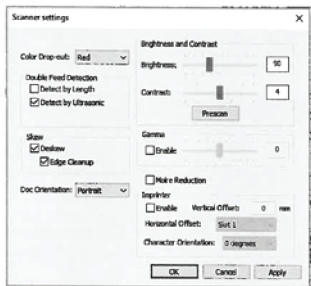


EXHIBIT F:

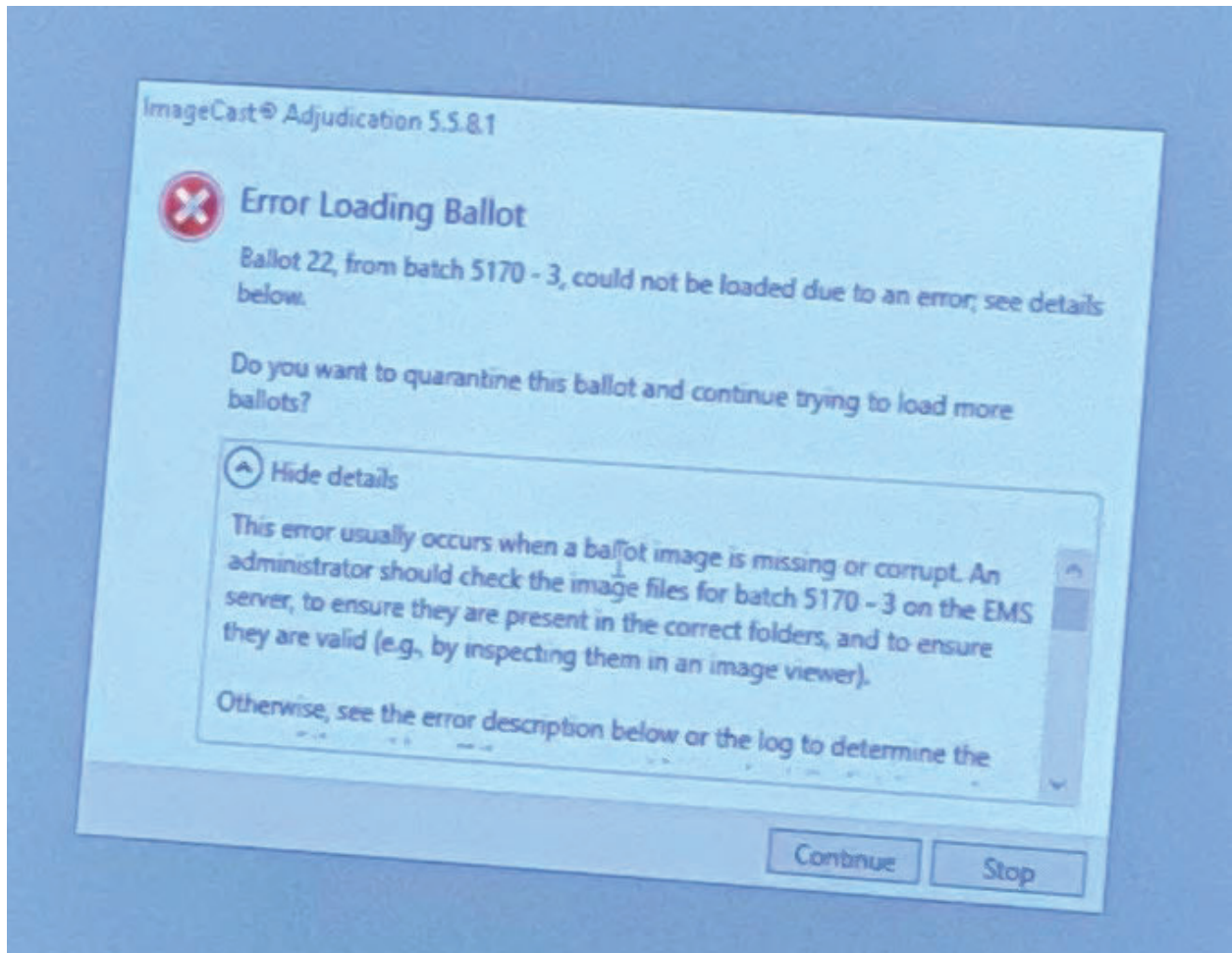


EXHIBIT G:



EXHIBIT H:



EXHIBIT I:

49

Copyright © 2020 Dominion Voting Inc. All Rights Reserved

FULTON COUNTY
993-SC13

OFFICIAL ABSENTEE/PROVISIONAL/EMERGENCY BALLOT

OFFICIAL DEMOCRATIC PARTY PRIMARY AND
NONPARTISAN GENERAL ELECTION RUNOFF BALLOT
OF THE STATE OF GEORGIA
AUGUST 11, 2020

To vote, blacken the Oval (●) next to the candidate of your choice. To vote for a person whose name is not on the ballot, manually WRITE his or her name in the write-in section and blacken the Oval (●) next to the write-in section. If you desire to vote YES or NO for a PROPOSED QUESTION, blacken the corresponding Oval (●). Use only blue or black pen or pencil.

Do not vote for more candidates than the number allowed for each specific office. Do not cross out or erase. If you erase or make other marks on the ballot or tear the ballot, your vote may not count.

If you change your mind or make a mistake, you may return the ballot by writing "Spoiled" across the face of the ballot and return envelope. You may then mail the spoiled ballot back to your county board of registrars, and you will be issued another official absentee ballot. Alternatively, you may surrender the ballot to the poll manager of an early voting site within your county or the precinct to which you are assigned. You will then be permitted to vote a regular ballot.

"I understand that the offer or acceptance of money or any other object of value to vote for any particular candidate, list of candidates, issue, or list of issues included in this election constitutes an act of voter fraud and is a felony under Georgia law." [O.C.G.A. 21-2-284(e) and 21-2-383(a)]

<p>For State Representative In the General Assembly From 65th District (Vote for One)</p> <p><input type="radio"/> Sharon Beasley-Teague (Incumbent)</p> <p><input checked="" type="radio"/> Mandisha A. Thomas</p>	<p>NONPARTISAN GENERAL ELECTION RUNOFF</p> <p>For Judge, Superior Court of the Atlanta Judicial Circuit (To Succeed Constance C. Russell) (Vote for One)</p> <p><input checked="" type="radio"/> Melynee Leftridge Harris</p> <p><input type="radio"/> Tamika Hrobowski-Houston</p>
<p>For District Attorney of the Atlanta Judicial Circuit (Vote for One)</p> <p><input type="radio"/> Paul Howard (Incumbent)</p> <p><input checked="" type="radio"/> Fani Willis</p>	<p>For Member, Fulton County School Board District 4 (Vote for One)</p> <p><input checked="" type="radio"/> Franchesca Warren</p> <p><input type="radio"/> Sandra C. Wright</p>
<p>For Sheriff (Vote for One)</p> <p><input checked="" type="radio"/> Theodore "Ted" Jackson (Incumbent)</p> <p><input type="radio"/> Patrick "Pat" Labat</p>	

703

EXHIBIT J:

Copyright © 2020 Dominion Voting Inc. All Rights Reserved

FULTON COUNTY
802-UC01A

OFFICIAL ABSENTEE/PROVISIONAL/EMERGENCY BALLOT

OFFICIAL DEMOCRATIC PARTY PRIMARY AND
NONPARTISAN GENERAL ELECTION RUNOFF BALLOT
OF THE STATE OF GEORGIA
AUGUST 11, 2020

To vote, blacken the Oval (●) next to the candidate of your choice. To vote for a person whose name is not on the ballot, manually WRITE his or her name in the write-in section and blacken the Oval (●) next to the write-in section. If you desire to vote YES or NO for a PROPOSED QUESTION, blacken the corresponding Oval (●). Use only blue or black pen or pencil.

Do not vote for more candidates than the number allowed for each specific office. Do not cross out or erase. If you erase or make other marks on the ballot or tear the ballot, your vote may not count.

If you change your mind or make a mistake, you may return the ballot by writing "Spoiled" across the face of the ballot and return envelope. You may then mail the spoiled ballot back to your county board of registrars, and you will be issued another official absentee ballot. Alternatively, you may surrender the ballot to the poll manager of an early voting site within your county or the precinct to which you are assigned. You will then be permitted to vote a regular ballot.

"I understand that the offer or acceptance of money or any other object of value to vote for any particular candidate, list of candidates, issue, or list of issues included in this election constitutes an act of voter fraud and is a felony under Georgia law." (O.C.G.A. 21-2-284(e) and 21-2-383(a))

<p>For State Representative In the General Assembly From 65th District (Vote for One)</p> <p><input checked="" type="checkbox"/> Sharon Beasley-Teague (Incumbent)</p> <p><input type="checkbox"/> Mandisha A. Thomas</p>	<p>NONPARTISAN GENERAL ELECTION RUNOFF</p> <p>For Judge, Superior Court of the Atlanta Judicial Circuit (To Succeed Constance C. Russell) (Vote for One)</p> <p><input type="checkbox"/> Melynee Leftridge Harris</p> <p><input checked="" type="checkbox"/> Tamika Hrobowski-Houston</p>	<p><i>Outstaked on 2nd pass concluded rely Sarah Couldn't first pass</i></p>
<p>For District Attorney of the Atlanta Judicial Circuit (Vote for One)</p> <p><input type="checkbox"/> Paul Howard (Incumbent)</p> <p><input checked="" type="checkbox"/> Fani Willis</p>		
<p>For Sheriff (Vote for One)</p> <p><input type="checkbox"/> Theodore "Ted" Jackson (Incumbent)</p> <p><input checked="" type="checkbox"/> Patrick "Pat" Labat</p>		

731

EXHIBIT K:



Gabriel Sterling
@GabrielSterling



Replying to [@MarilynRMarks1](#) [@rahulbali](#) and 9 others

Again, all Central scanners were set at the industry standard 0-13% is not a mark (the oval is 5%) 14-28% is the ambiguous level to be checked by review panels, 29%+ is a mark. You ar pointing out the inherent issues with HMPBs that we don't see with BMD marked ballots.

8:02 PM · Jun 13, 2020 from [Georgia, USA](#) · [Twitter for iPhone](#)



EXHIBIT L:



- Create a voter card from Poll Pad for each unique ballot style within the designated Polling Location
 - Recommend labels be placed on card identifying what ballot style will be displayed by BMD once card is inserted
 - BMD removes the activation code from the Voter Card once used, therefore create the card again from Poll Pad after each use by a BMD

D. Testing the BMD and Printer

Use a combination of Poll Worker Card with Ballot Activation Codes for the polling location, and Voter Cards created from a Poll Pad loaded with the LA/Advance Voting dataset to bring up ballots on the BMD

- Produce at least one printed ballot from each BMD assigned to the polling location
- Produce a test deck from the BMDs assigned to the polling location for each unique ballot style within the polling location. The test deck must contain at least one vote for each candidate listed in each race within the unique ballot style
 - **Example:** Ballot from BMD 1 contains a vote for only the first candidate in each race listed on Ballot Style 1, Ballot from BMD 2 contains a vote only for the second candidate in each race on Ballot Style 1, and continue through the line of devices until all candidates in all races within the unique ballot style have received a single vote
 - **If Number of BMDs outnumber the number of vote positions on the unique ballot style,** start the vote pattern over until all BMDs have produced one printed ballot
 - **If Number of unique ballot styles in the polling place is greater than 1,** once the vote pattern is complete for a unique ballot style, proceed to the next BMD in line to start the review of the next unique Ballot Style
 - **All unique ballot styles do not have to be tested on each BMD**
- Review BMD-generated Test Deck and confirm the vote content before placing in the designated Polling Place Scanner

E. Testing the Polling Place Scanner

- Scan the BMD-generated Test Deck into the Polling Place Scanner
- Scan one blank optical scan ballot style(s) associated to the Polling Place to verify the Polling Place Scanner will recognize the ballot style in case of emergency
- Verify Scanner(s) shows a number of Ballot Cast equal to the number of ballots in the BMD-generated test deck plus the scanned blank Optical Scan ballot styles
- Firmly place the Security Key Tab in the Security Key Slot
- Touch Close Polls
- Enter the passcode
- Touch Enter
- Touch Yes
- Touch No for additional tapes (Scanner will automatically produce 3 copies of the closing tape)

EXHIBIT M:

THE DOMINION DIFFERENCE

DUAL THRESHOLD TECHNOLOGY (MARGINAL MARKS)

From its early beginnings, Dominion Voting has emphasized the use of digital scanning, and continues to set the standard in digital image acquisition and analysis in the tabulation of digitally scanned ballots. When a ballot is fed into an ImageCast® tabulator - at the precinct level or centrally - a complete duplex image is created and then analyzed for tabulation by evaluating the pixel count of a voter mark. The pixel count of each mark is compared with two thresholds (which can be defined through the Election Management System) to determine what constitutes a vote. If a mark falls above the upper threshold, it's a valid vote. If a mark falls below the lower threshold, it will not be counted as a vote.

However, if a mark falls between the two thresholds (known as the "ambiguous zone"), it will be deemed as a marginal mark and the ballot will be returned to the voter for corrective action (please see diagram below). With this feature, the voter is given the ability to determine his or her intent, not an inspection or recount board after the fact, when it is too late. The chart below illustrates the Marginal Mark threshold interpretation.

Mark	Mark Density	Classification
Mark #1	~10%	Not Counted
Mark #2	~25%	Marginal
Mark #3	~55%	Counted
Mark #4	~95%	Counted

THE DOMINION DIFFERENCE

DUAL THRESHOLD TECHNOLOGY

EXHIBIT 8

STATEMENT BY ANA MERCEDES DÍAZ CARDOZO

I, Ana Mercedes Díaz Cardozo, hereby declare the following:

1. My name is Ana Mercedes Díaz Cardozo. I'm known as Ana Diaz by many. I am an adult of the sound mind and was born in Caracas, Venezuela on March 24, 1960. I'm a naturalized American citizen. I reside at 923 Gulf Stream Court, Weston, Florida 33327.

2. I make this statement voluntarily and on my own initiative. I have not been promised, nor do I expect to receive anything in exchange for my testimony and give this statement. I have no expectation of any benefit or reward and understand that there are those who can try to hurt me for what I say in this statement.

3. I moved from Venezuela to the United States in 2004 due to political corruption and rapid decline in my home country of Venezuela. I want to alert the public and let the world know the truth about corruption, manipulation, and lies committed through a conspiracy of individuals and businesses with the intention of betraying the honest people of the United States and its legally constituted institutions and fundamental rights as citizens. This conspiracy began more than a decade ago in Venezuela and has spread to countries around the world. It is a conspiracy to unjustly gain and maintain power and wealth. These are political leaders, powerful companies, and others whose purpose is to gain and maintain power by changing people's free will and subverting the proper course of governing.

4. After graduating from high school, I attended the University of Santa Maria in Caracas, Venezuela and graduated as a lawyer in 1987. Then I studied a postgraduate degree in administrative law at the University of Central Venezuela. Before I could submit my thesis for a Master's degree in Administrative Law, I moved to the United States. I'm certified as an arbiter of international trade.

5. I was a career official for 25 years at the Supreme Electoral Council of Venezuela, which is the name that it was called in the 1970's. It is currently called the National Electoral Council. This is the highest electoral administrative agency in Venezuela and oversees all elections in Venezuela. In 1979, at the age of 19, I began my career at the Supreme Electoral Council of Venezuela as secretary in the regional delegation of the federal district. When I graduated from the university as a lawyer, my position on the Supreme Electoral Council changes to the position as an adviser to the Judicial Council of the Supreme Council Electoral. In 1991, I was appointed Assistant Director General of Political Parties, where I served until Hugo Chavez came to power in 1998. Also during this time, I served for seven years as a member of the Legislative Commission of the Venezuelan Electoral Council. It was the role of the Legislative Commission to review and identify any issues related to candidates

for elected positions. The Legislative Commission and my office had access to many resources within the various departments of the Electoral Council, including an information technology section that had experts in computers, computer programming, computer systems and telecommunications features such as modems, telephone lines. I was regularly in communication with the various departments of the Electoral Body for my daily duties. In the last years of my work for the Electoral Counsel, a little of my activities and duties were to learn about electronic voting systems and their functioning by Council experts.

6. As Deputy Director General of Political Parties in the Supreme Electoral Council, it was my duty to oversee everything related to political parties in Venezuela, particularly the participation of political parties in elections and the selection and qualifications of candidates for political office. My office reviewed everything to do with the ability of political parties to participate in the electoral process. Before a political party could be formed, it had to undergo a process for approval. This included legal approval of the party name, its colors and a list of its members. The proposed party had to have a certain percentage of Venezuela's population depending on whether it wanted to be a regional or national party. It could not be constituted as a political party until it was approved by the Supreme Electoral Council. My office also oversaw the creation of ballots that bore the name of the candidates and any party symbol or color that the candidate would like to use. When our office approved these matters, we sent the ballot for printing and circulation. Any conflict over which group could be a political party, which would be a candidate for elected office, how that candidate would be included in the vote, were decided by my office. I was a signatory to all decisions taken by the Political Parties office at the Supreme Electoral Council.

7. After Hugo Chavez was elected, he changed the Venezuelan Constitution. One such change was in the Supreme Electoral Council, now the Electoral Power. In February 2009, a national referendum was passed to change Venezuela's Constitution to end mandate limits for elected officials, including the President of Venezuela. This change allowed Hugo Chavez to be re-elected an unlimited number of times.

8. In 2003, I was appointed Director General of Political Parties at the National Electoral Council. At the end of that year there was a national effort to hold a referendum to remove Hugo Chavez from the post of President. In 2004 I was appointed to the Validation Committee that was responsible for reviewing petitions, the requirements of the signatories were their name, their signature, their fingerprint and their identification number. I discovered many ways that the party in power was trying to override requests. One was the change of forms to reflect that the petition was a referendum on the removal of members of the Venezuelan Congress

rather than the removal of the Venezuelan president. The purpose of manipulating petitions was to prevent a referendum to remove President Chavez from office. I investigated the allegations of fraud with the referendum petitions and lobbied for the fraudulent changes to be rectified. Because of my resistance and protests to this voter fraud, I received a letter in March 2004 stating that my position was trusted and trust had been lost in me and I was fired from the service.

9. After my dismissal, I decided to commit to the study of electoral processes both within Venezuela and in other countries, particularly in South American countries that were experiencing electoral unrest and government manipulation of constitutions, laws and elections. I joined a small group of highly educated and informed people who had access to information about the Venezuelan government and its activities. This group and I conduct interviews with Venezuelan citizens, read news publications and specialized treaties, and write evaluating the political, economic, legal and electoral changes taking place in Venezuela, South American countries, and other parts of the world controlled by socialist dictators and oligarchies. I read these treatises, studies, and publications to educate myself on how elections were manipulated and the use of empirical analysis to detect and identify the manipulation of elections and their results. In addition, I have collected copies of official Venezuelan government documents.

10. Official documents of the Venezuelan government include documents showing the bidding process for the implementation of a new electronic voting system in March 2004 and the award of the contract for that new system to Smartmatic. A true and authentic copy of the venezuelan National Electoral Council's tender documents, internal memorandums and contract signed between the Venezuelan government and the SBC Consortium (Smartmatic) are labeled Exhibit 1 and this statement is attached. I received the documents that constitute Exhibit 1 from a reliable person who had taken some notes on the documents and highlighted some parts for my attention. I have not made any alterations to what I have received, and the substantive content of the documents is authentic. For convenience, I've had the Bates document tagged at the bottom right of each page.

11. I have studied the documents contained in Exhibit 1 and have several observations. Exhibit 1 says that it is a contract between the National Electoral Council and the SBC Consortium (Smartmatic) and is dated 15 March 2004. It has a stamp that says Bolivarian Republic of Venezuela, Secretary General of the National Electoral Council. That is the official seal of the Secretary of the National Electoral Council. The initials at the bottom right side confirm the document's authenticity.

12. You would notice that page DIAZ 00002 is important because it shows that the contract is being made on February 16, 2004. Page DIAZ 00027, reflects that on February 14, 2004 at 11:50 a.m., in the Council's session room, Francisco Carrasquero López, Ezequiel Zamora Presilla, Jorge Rodríguez Gómez (Jorge Rodríguez), Sobella Mejías, and William Pacheco Medina, Vice President, the directors of the Secretary General of Electoral Voters respectively, in order to proceed with the delivery to the technical commissions, designated at the meeting dated 13 February 2004, they opened the tender envelopes containing the tenders of the companies that wanted to be awarded a contract for the automation of Venezuela's voting system and the processes used to carry out the 2004 referendum on the revocation of Hugo Chavez's election. Below you can read the amounts of offers made by Smartmatic SBC, Diebold and other bidders.

13. Then, on page DIAZ 000031, there is an internal note from the Director General of Administration, Mr. Medina. It was dated 14 February 2004 and said that a report on the research and evaluation of companies bidding for the automation of the voting system needed to be prepared.

14. It would then draw attention to the page marked DIAZ 000029. It is a document made on February 13, 2004. While this page is out of sequence, it shows the speed at which the decision was made to award the electoral system contract. The tender began on February 13 and had ended on February 16th -- a three-day period to review contracts and evaluate the specifications and performance of bidders' systems, including software, hardware, security, performance and bidding costs for the procurement, installation, training and operation of the systems. By February 16th, a decision to choose Smartmatic was made. This is convincing evidence that there was no genuine competition for the electoral system contract or serious consideration for alternative contracts. There was no due diligence and the bidding was rigged. It is not possible that within three or four days to do the formal investigation to evaluate the bids and award a contract of this size and important. The impropriety of this action is confirmed by the fact that the contract with Smartmatic was signed a month later, on 15 March 2004.


15. After the contract was awarded to Smartmatic, it was learned that Smartmatic had no previous experience in conducting elections and electoral tabulations. More importantly, it was discovered that the Smartmatic voting system contained two-way communication functions that allowed voting data not only to be sent to a central system of operation and voting, but the central voting system in operation and tabulation to send operational instructions and data to voting machines. It is not mentioned in the contract documents and specifications that the system would be bidirectional and would allow the transmission of data and instructions from the central operating system directly to voting machines. One

simply has to examine the system diagram on page DIAZ 000057 of Exhibit 1. If this feature of the Smartmatic system had been disclosed to the Electoral Council, it could not have adequately accepted Smartmatic's offer because it would allow the Smartmatic voting system to be handled in a way that manipulated votes and interfered with the legitimate voting and electoral process by impersonating the will to govern officials with the will of the electorate: the citizens of Venezuela. It was not surprising that Hugo Chávez and his successors then constantly won the election through the use and manipulation of the Smartmatic voting system.

16. In the 16 years since I left my post as Director General of Political Parties at the National Electoral Council of Venezuela, I have studied the electoral systems of Bolivia, Colombia, Ecuador, Guatemala, Honduras and Nicaragua and have observed elections and participated in pro-democratic forums in Colombia, Ecuador, Honduras and Nicaragua. I have also studied and researched electoral processes in Europe, participating in public academic conferences in Spain and Italy on the subject of democratic electoral processes.

17. Based on my specialized experiences with electoral systems, I have a firm view that no legitimate electronic voting system should be allowed to have the ability of two-way communications to send data and instructions between central tabulation operations and voting machines over telephone lines or the Internet. Having such characteristics compromise the integrity of the entire voting process by allowing injection of data and instructions to manipulate voting before, during and after an election and to avoid detection of processes and mechanisms designed to prevent voting manipulation and fraud.

I declare under penalty of perjury that the above is true and correct and that this Statement was prepared in Dallas County, Texas, and executed on November 20, 2020.



Ana Mercedes Díaz Cardozo

EXHIBIT 9

Declaration of Seth Keshel

Pursuant to 28 U.S.C Section 1746, I, Seth Keshel, make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I am a trained data analyst with experience in multiple fields, including service in the United States Army as a Captain of Military Intelligence, with a one-year combat tour in Afghanistan. My experience includes political involvement requiring a knowledge of election trends and voting behavior.
3. I reside at 233 Muir Hill Dr., Aledo, TX 76008.
4. My affidavit highlights substantial deviance from statistical norms and results regarding voting patterns in Arizona.
5. All 2020-related voting totals are taken from the Decision Desk HQ unofficial tracker, are not certified, and are subject to change from the time of the creation of this affidavit.
6. Arizona is a rapidly growing state, with 287,001 new Democrat registrations and 269,164 new Republican registrations statewide since the 2016 general election. Republicans hold a 3% registration edge statewide (35.2% to 32.2%), and a 3.9% registration edge in Maricopa County (35.3% to 31.4%), the state's largest county which has cast roughly 61.1% of all votes counted statewide thus far in Arizona's 2020 presidential race.
7. Republicans have out-registered Democrats in voter registration since the March presidential primaries. Statewide, since the end of

primaries, Republicans have added 148,485 to their rolls, compared to 116,389 for Democrats. In Maricopa County, Republicans lead 87,000 to 76,417 in this time period. This is an indicator of momentum heading into the general election favoring Republicans.

8. Maricopa County has been won by the Republican candidate in every election since 1952, including in 1996 when Democrat Bill Clinton carried the state, and in 2016, when Donald Trump won the county with the weakest performance relative to registered Republicans since at least 2004. In that year, he tallied just 97 votes per 100 registered Republicans in the county, below George W. Bush's total in 2004 (100), John McCain's in 2008 (108), and Mitt Romney's in 2012 (109). Statewide in 2016, Trump's numbers lagged the previous three Republican votes per 100 registered statewide (105, 110, and 110), at just 101 votes per 100 registered Republicans. This year, with counts not certified and subject to adjustment, Trump's performance in Maricopa County equals Mitt Romney's high of 109 votes per 100 registered Republicans and matches two previous highs of 110 votes per 100 registered Republicans statewide. This indicates strong base support, crossover support, independent support, and minimal party defections. Biden's totals however, per 100 registered Democrats, are well above established trendlines for Democrats. Statewide, he has 121 votes per 100 registered Democrats, 14 votes higher than the previous high (Obama, 2012, 107 votes), and 15 higher than Hillary Clinton's total in 2016. In Maricopa County, Biden has 128 votes per 100 registered Democrats, a full 10 votes higher than Barack Obama's 2012 total, and 14 above

Hillary Clinton's. These figures can be observed in Exhibit A to this affidavit.

9. In Maricopa County, Democrats grew by 118,116 votes (from Al Gore to John Kerry) between 2000 and 2004. Hillary Clinton added 100,619 votes to Barack Obama's 2012 total in 2016. Thus far in the count, Joe Biden has added 337,646 votes in Maricopa County in a single cycle, a 48.0% increase in a county that already had a high number of Democratic votes relative to the other large counties in the nation. This comes as President Trump has reconsolidated his lost voter base from 2016 with his own 33.2% increase in the county.
10. Maricopa County received 1.52 new Democratic votes for every new registered Democrat in 2008, reversed into a losing number in 2012, and then received 0.93 new votes for every new registered Democrat in 2016. This year, they are receiving 1.72 new Democratic votes for every new registered Democrat in the county.
11. Among comparable 2016 counties (within 100,000 votes of Maricopa's 2016 Democratic vote total), Maricopa County towers above the rest in percentage of new Democratic votes, with 48.0% more (337,646 new Democrat votes) than in 2016, a virtually impossible number. Comparable counties are also growing counties with expanding voter rolls, with none of the counties won by a Republican presidential nominee since 2004. This information is available in Exhibit B.
 - a. Orange County, California, has 198,203 (32.5%) more new Democrat votes.

- b. San Diego County, California, has 221,302 (30.1%) more new Democrat votes.
 - c. Harris County, Texas, has 203,999 (28.8%) more new Democrat votes.
 - d. King County, Washington, has 185,810 (25.9%) more new Democrat votes.
 - e. Miami-Dade County, Florida, has lost 6,499 (-1.0%) Democrat votes since 2016.
12. Excepting Miami-Dade for its notable loss in raw Democratic votes, Maricopa County Democratic vote growth in line with Orange, San Diego, Harris, and King Counties should align with slightly more than 900,000 votes in the county for Joe Biden, not 1.04 million.
13. Pima County, Arizona, has also shown 35.8% Democratic raw vote growth (80,320 votes) in a single cycle. President Trump has increased his vote total in the county by 24.1%, with a vote total now surpassing Obama's total in this county in 2012. The previous high for increase in this county for Democrats was 45,440 votes in 2004.
14. Of the remaining 13 counties, these show proper progression in keeping with historic party registration trends:
- a. Pinal
 - b. Graham
 - c. Greenlee
 - d. Santa Cruz
 - e. Yuma
 - f. La Paz

- g. Mohave
- h. Gila
- i. Yavapai

15. These 4 counties show deviation from standard progression associated with historic party registration trends:

- a. Apache – shifted one point in favor of Republicans in registration since 2016 but gave Trump a defeat margin 2,647 votes greater than in 2016, as Biden added a record number of votes in one cycle despite registration trends.
- b. Coconino – shifted three points in favor of Democrats but has a heavier than expected margin in favor of Biden, particularly since Republicans also gained in this county.
- c. Navajo – trended four points in favor of Republican registration since 2016, but Trump’s margin of victory remained all but unchanged, save for 156 votes, even though Trump added nearly 7,000 more votes to his total in a county heavily trending Republican.
- d. Cochise – trended four points in favor of Republican registration since 2016, but Trump’s margin of victory is nearly unchanged, up just 297 votes.



Seth Keshel

18 Nov. 2020

Aledo, Texas

EXHIBIT 9 A&B

**More Mega Counties within 100,000 votes (+ or -) of 2016 Maricopa Dem Vote (702,907)
 % Increase in Dem Votes in 2020**

*Pima County included for comparison in Arizona

*Orange, San Diego, Harris, and King average 29.2% increase in Dem votes

-A 29.2% Increase in Maricopa County would mean 205,249 more Dem Votes (908,156 total)

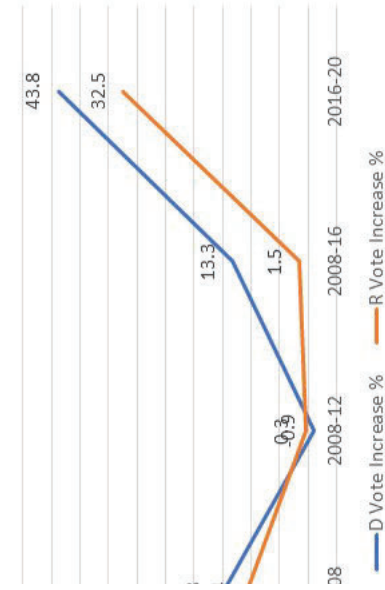
*Previous highs for one-cycle increase in Dem Votes

-Maricopa – 118,166 (2004)

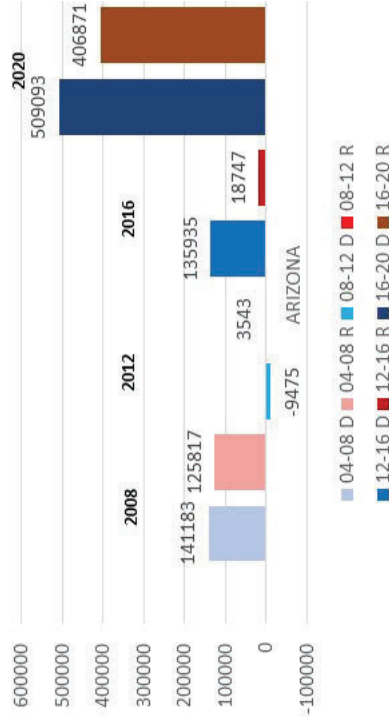
-Pima – 45,440 (2004)

UNITIES	% Increase Dem Votes 16-20	2016 Dem Votes	2020 Dem Votes	Amount
AZ (AZ)	48.03%	702,907	1,040,533	337,626
CA (CA)	35.75%	224,661	304,981	80,320
CO (CA)	32.49%	609,961	808,164	198,203
TX (TX)	30.09%	735,476	956,778	221,302
ND (ND)	28.82%	707,914	911,913	203,999
FL (FL)	25.87%	718,322	904,132	185,810
	-1.04%	624,146	617,647	-6,499

% Increase in Raw Votes by Party
Arizona



Votes Added From Previous Election by Party
Arizona



Dem Rep/Votes per 100 Registered

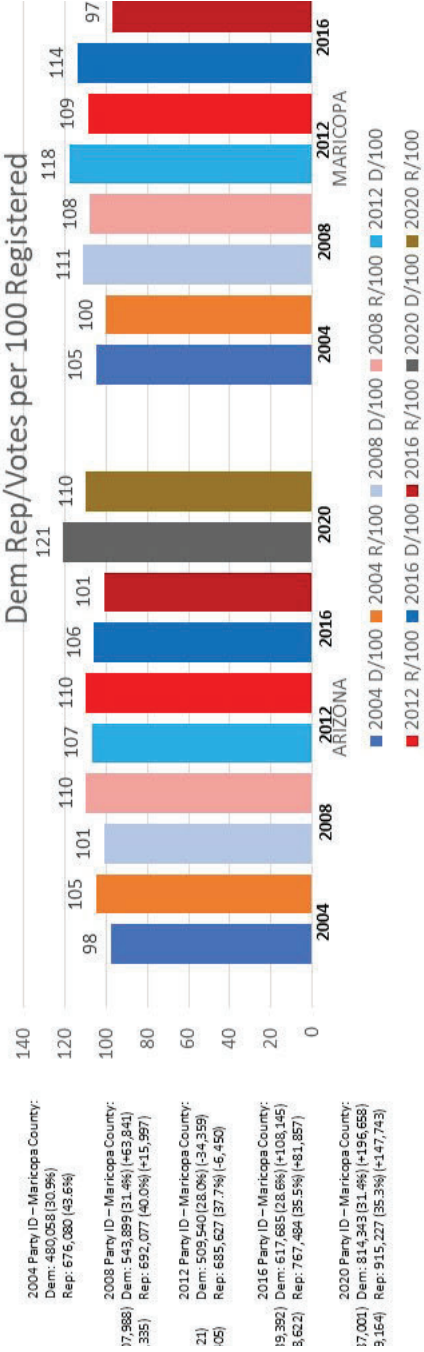


EXHIBIT 9 S

Declaration of Seth Keshel

Pursuant to 28 U.S.C Section 1746, I, Seth Keshel, make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I am a trained data analyst with experience in multiple fields, including service in the United States Army as a Captain of Military Intelligence, with a one-year combat tour in Afghanistan. My experience includes political involvement requiring a knowledge of election trends and voting behavior.
3. I reside at 233 Muir Hill Dr., Aledo, TX 76008.
4. My affidavit highlights substantial deviance from statistical norms and results regarding voting patterns in Arizona.
5. All 2020-related voting totals are taken from the Decision Desk HQ unofficial tracker, are not certified, and are subject to change from the time of the creation of this affidavit.
6. Arizona is a rapidly growing state, with 287,001 new Democrat registrations and 269,164 new Republican registrations statewide since the 2016 general election. Republicans hold a 3% registration edge statewide (35.2% to 32.2%), and a 3.9% registration edge in Maricopa County (35.3% to 31.4%), the state's largest county which has cast roughly 61.1% of all votes counted statewide thus far in Arizona's 2020 presidential race.
7. Republicans have out-registered Democrats in voter registration since the March presidential primaries. Statewide, since the end of

primaries, Republicans have added 148,485 to their rolls, compared to 116,389 for Democrats. In Maricopa County, Republicans lead 87,000 to 76,417 in this time period. This is an indicator of momentum heading into the general election favoring Republicans.

8. Maricopa County has been won by the Republican candidate in every election since 1952, including in 1996 when Democrat Bill Clinton carried the state, and in 2016, when Donald Trump won the county with the weakest performance relative to registered Republicans since at least 2004. In that year, he tallied just 97 votes per 100 registered Republicans in the county, below George W. Bush's total in 2004 (100), John McCain's in 2008 (108), and Mitt Romney's in 2012 (109). Statewide in 2016, Trump's numbers lagged the previous three Republican votes per 100 registered statewide (105, 110, and 110), at just 101 votes per 100 registered Republicans. This year, with counts not certified and subject to adjustment, Trump's performance in Maricopa County equals Mitt Romney's high of 109 votes per 100 registered Republicans and matches two previous highs of 110 votes per 100 registered Republicans statewide. This indicates strong base support, crossover support, independent support, and minimal party defections. Biden's totals however, per 100 registered Democrats, are well above established trendlines for Democrats. Statewide, he has 121 votes per 100 registered Democrats, 14 votes higher than the previous high (Obama, 2012, 107 votes), and 15 higher than Hillary Clinton's total in 2016. In Maricopa County, Biden has 128 votes per 100 registered Democrats, a full 10 votes higher than Barack Obama's 2012 total, and 14 above

Hillary Clinton's. These figures can be observed in Exhibit A to this affidavit.

9. In Maricopa County, Democrats grew by 118,116 votes (from Al Gore to John Kerry) between 2000 and 2004. Hillary Clinton added 100,619 votes to Barack Obama's 2012 total in 2016. Thus far in the count, Joe Biden has added 337,646 votes in Maricopa County in a single cycle, a 48.0% increase in a county that already had a high number of Democratic votes relative to the other large counties in the nation. This comes as President Trump has reconsolidated his lost voter base from 2016 with his own 33.2% increase in the county.
10. Maricopa County received 1.52 new Democratic votes for every new registered Democrat in 2008, reversed into a losing number in 2012, and then received 0.93 new votes for every new registered Democrat in 2016. This year, they are receiving 1.72 new Democratic votes for every new registered Democrat in the county.
11. Among comparable 2016 counties (within 100,000 votes of Maricopa's 2016 Democratic vote total), Maricopa County towers above the rest in percentage of new Democratic votes, with 48.0% more (337,646 new Democrat votes) than in 2016, a virtually impossible number. Comparable counties are also growing counties with expanding voter rolls, with none of the counties won by a Republican presidential nominee since 2004. This information is available in Exhibit B.
 - a. Orange County, California, has 198,203 (32.5%) more new Democrat votes.

- b. San Diego County, California, has 221,302 (30.1%) more new Democrat votes.
 - c. Harris County, Texas, has 203,999 (28.8%) more new Democrat votes.
 - d. King County, Washington, has 185,810 (25.9%) more new Democrat votes.
 - e. Miami-Dade County, Florida, has lost 6,499 (-1.0%) Democrat votes since 2016.
12. Excepting Miami-Dade for its notable loss in raw Democratic votes, Maricopa County Democratic vote growth in line with Orange, San Diego, Harris, and King Counties should align with slightly more than 900,000 votes in the county for Joe Biden, not 1.04 million.
13. Pima County, Arizona, has also shown 35.8% Democratic raw vote growth (80,320 votes) in a single cycle. President Trump has increased his vote total in the county by 24.1%, with a vote total now surpassing Obama's total in this county in 2012. The previous high for increase in this county for Democrats was 45,440 votes in 2004.
14. Of the remaining 13 counties, these show proper progression in keeping with historic party registration trends:
- a. Pinal
 - b. Graham
 - c. Greenlee
 - d. Santa Cruz
 - e. Yuma
 - f. La Paz

- g. Mohave
- h. Gila
- i. Yavapai

15. These 4 counties show deviation from standard progression associated with historic party registration trends:

- a. Apache – shifted one point in favor of Republicans in registration since 2016 but gave Trump a defeat margin 2,647 votes greater than in 2016, as Biden added a record number of votes in one cycle despite registration trends.
- b. Coconino – shifted three points in favor of Democrats but has a heavier than expected margin in favor of Biden, particularly since Republicans also gained in this county.
- c. Navajo – trended four points in favor of Republican registration since 2016, but Trump’s margin of victory remained all but unchanged, save for 156 votes, even though Trump added nearly 7,000 more votes to his total in a county heavily trending Republican.
- d. Cochise – trended four points in favor of Republican registration since 2016, but Trump’s margin of victory is nearly unchanged, up just 297 votes.



Seth Keshel

18 Nov. 2020

Aledo, Texas

EXHIBIT 10

Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters

Andrew W. Appel[†]
Princeton University

Richard A. DeMillo[†]
Georgia Tech

Philip B. Stark[†]
Univ. of California, Berkeley

December 27, 2019

Abstract

The complexity of U.S. elections usually requires computers to count ballots—but computers can be hacked, so election integrity requires a voting system in which paper ballots can be recounted by hand. However, paper ballots provide no assurance unless they accurately record the vote as the voter expresses it.

Voters can express their intent by indelibly hand-marking ballots, or using computers called ballot-marking device (BMDs). Voters can make mistakes in expressing their intent in either technology, but only BMDs are also subject to hacking, bugs, and misconfiguration of the software that prints the marked ballots. Most voters do not review BMD-printed ballots, and those who do often fail to notice when the printed vote is not what they expressed on the touchscreen. Furthermore, there is no action a voter can take to demonstrate to election officials that a BMD altered their expressed votes, nor is there a corrective action that election officials can take if notified by voters—there is no way to deter, contain, or correct computer hacking in BMDs. These are the essential security flaws of BMDs.

Risk-limiting audits can assure that the votes recorded on paper ballots are tabulated correctly, but no audit can assure that the votes on paper are the ones expressed by the voter on a touchscreen: Elections conducted on current BMDs cannot be confirmed by audits. We identify two properties of voting systems, *contestability* and *defensibility*, necessary for audits to confirm election outcomes. No available EAC-certified BMD is contestable or defensible.

[†]Authors are listed alphabetically; they contributed equally to this work.

1 Introduction: Criteria for Voting Systems

Elections for public office and on public questions in the United States or any democracy must produce outcomes based on the votes that voters *express* when they indicate their choices on a paper ballot or on a machine. Computers have become indispensable to conducting elections, but computers are vulnerable. They can be hacked—compromised by insiders or external adversaries who can replace their software with fraudulent software that deliberately miscounts votes—and they can contain design errors and bugs—hardware or software flaws or configuration errors that result in misrecording or mis-tabulating votes. Hence there must be some way, *independent* of any software in any computers, to ensure that reported election outcomes are correct, i.e., consistent with the expressed votes as intended by the voters.

Voting systems should be *software independent*, meaning that “an undetected change or error in its software cannot cause an undetectable change or error in an election outcome” [29, 30, 31]. Software independence is similar to tamper-evident packaging: if somebody opens the container and disturbs the contents, it will leave a trace.

The use of software-independent voting systems is supposed to ensure that if someone fraudulently hacks the voting machines to steal votes, we’ll know about it. But we also want to know *the true outcome* in order to avoid a do-over election.¹ A voting system is *strongly software independent* if it is software independent and, moreover, a detected change or error in an election outcome (due to change or error in the software) can be corrected using only the ballots and ballot records of the current election [29, 30]. Strong software independence combines tamper evidence with a kind of resilience: there’s a way to tell whether faulty software caused a problem, and a way to recover from the problem if it did.

Software independence and *strong software independence* are now standard terms in the analysis of voting systems, and it is widely accepted that voting systems should be software independent. Indeed, version 2.0 of the Voluntary Voting System Guidelines (VVSG 2.0) incorporates this principle [10].

But as we will show, these standard definitions are incomplete and inadequate, because in the word *undetectable* they hide several important questions: *Who* detects the change or error in an election outcome? How can a person *prove* that she has detected

¹Do-overs are expensive; they may delay the inauguration of an elected official; there is no assurance that the same voters will vote in the do-over election as voted in the original; they decrease public trust. And if the do-over election is conducted with the same voting system that can only detect but not correct errors, then there may need to be a do-over of the do-over, *ad infinitum*.

an error? *What happens* when someone detects an error—does the election outcome remain erroneous? Or conversely: How can an election administrator *prove* that the election outcome not been altered, or prove that the correct outcome was recovered if a software malfunction was detected? The standard definition does not distinguish evidence available to an election official, to the public, or just to a single voter; nor does it consider the possibility of false alarms.

Those questions are not merely academic, as we show with an analysis of ballot-marking devices. Even if some *voters* “detect” that the printed output is not what they expressed to the BMD—even if some of *those* voters report their detection to election officials—there is no mechanism by which the *election official* can “detect” whether a BMD has been hacked to alter election outcomes. The questions of *who detects*, and *then what happens*, are critical—but unanswered by the standard definitions.

We will define the terms *contestable* and *defensible* to better characterize properties of voting systems that make them acceptable for use in public elections.²

A voting system is *contestable* if an undetected change or error in its software that causes a change or error in an election outcome can always produce *public* evidence that the outcome is untrustworthy. For instance, if a voter selected candidate A on the touchscreen of a BMD, but the BMD prints candidate B on the paper ballot, then this A-vs-B evidence is available to the individual voter, but the voter cannot demonstrate this evidence to anyone else, since nobody else saw—nor should have seen—where the voter touched the screen.³ Thus, the voting system does not provide a way for the voter who observed the misbehavior to prove to anyone else that there was a problem, even if the problems altered the reported outcome. Such a system is therefore not *contestable*.

While the definition of software independence might allow evidence available only to individual voters as “detection,” such evidence does not suffice for a system to be contestable. Contestability is software independence, plus the requirement that “detect” implies “can generate public evidence.” “Trust me” does not count as public evidence. If a voting system is not contestable, then problems voters “detect” might never see the light of day, much less be addressed or corrected.⁴

²There are other notions connected to contestability and defensibility, although essentially different: Benaloh et al. [6] define a *P-resilient canvass framework*, *personally verifiable P-resilient canvass framework*, and *privacy-perserving personally verifiable P-resilient canvass frameworks*.

³See footnote 18.

⁴If voters are the only means of detecting and quantifying the effect of those problems—as they are for BMDs—then in practice the system is not strongly software independent. The reason is that, as we will show, such claims by (some) voters *cannot* correct software-dependent changes to other voters’ ballots, and *cannot* be used as the basis to invalidate or correct an election outcome. Thus, BMD-based

Similarly, while strong software independence demands that a system be able to report the correct outcome even if there was an error or alteration of the software, it does not require *public evidence* that the (reconstructed) reported outcome is correct. We believe, therefore, that voting systems must also be *defensible*. We say that a voting system is defensible if, when the reported electoral outcome is correct, it is possible to generate convincing public evidence that the reported electoral outcome is correct—despite any malfunctions, software errors, or software alterations that might have occurred. If a voting system is not defensible, then it is vulnerable to “crying wolf”: malicious actors could claim that the system malfunctioned when in fact it did not, and election officials will have no way to prove otherwise.

By analogy with *strong software independence*, we define: A voting system is *strongly defensible* if it is defensible and, moreover, a detected change or error in an election outcome (due to change or error in the software) can be corrected (with convincing public evidence) using only the ballots and ballot records of the current election.

In short, a system is contestable if it can generate public evidence of a problem whenever a reported outcome is wrong, while a system is defensible if it can generate public evidence whenever a reported outcome is correct—despite any problems that might have occurred. Contestable systems are publicly tamper-evident; defensible systems are publicly, demonstrably resilient.

Defensibility is a key requirement for *evidence-based elections* [38]: defensibility makes it possible in principle for election officials to generate convincing evidence that the reported winners really won—if the reported winners did really win. (We say an election *system* may be defensible, and an *election* may be evidence-based; there’s much more *process* to an election than just the choice of system.)

Examples. The only known practical technology for contestable, strongly defensible voting is a system of *hand-marked paper ballots*, kept demonstrably physically secure, counted by machine, audited manually, and recountable by hand.⁵ In a hand-marked paper ballot election, ballot-marking software cannot be the source of an error or change-of-election-outcome, because no software is used in marking ballots. Ballot-scanning-and-counting software can be the source of errors, but such errors can be

election systems are not even (weakly) software independent, unless one takes “detection” to mean “somebody claimed there was a problem, with no evidence to support that claim.”

⁵The election must also generate convincing evidence that physical security of the ballots was not compromised, and the audit must generate convincing public evidence that the audit itself was conducted correctly.

detected and corrected by audits.

That system is *contestable*: if an optical scan voting machine reports the wrong outcome because it miscounted (because it was hacked, misprogrammed, or miscalibrated), the evidence is *public*: the paper ballots, recounted before witnesses, will not match the claimed results, also witnessed. It is *strongly defensible*: a recount before witnesses can demonstrate that the reported outcome is correct, or can find the correct outcome if it was wrong—and provide public evidence that the (reconstructed) outcome is correct.

Some other paper-based systems such as Prêt-à-Voter [32] and Scantegrity [9] are also contestable and strongly defensible (provided the marked ballots are kept demonstrably secure through tabulation and posting). Scantegrity inherits these properties from the fact that it amounts to a cryptographic enhancement of hand-marked paper ballots. Prêt-à-Voter has these properties if the blank ballots are audited appropriately before the election.

Paper-based systems that rely on the “Benaloh challenge”—to ensure that the encryption of the vote printed on the ballot (by an electronic device) is correct—generally are neither contestable nor defensible.⁶ The reason is that, while the challenge can produce public evidence that a machine did not accurately encrypt the plaintext vote on the ballot, if the machine prints the wrong plaintext vote and a correct encryption of that incorrect vote, there is no evidence the voter can use to prove that to anyone else. STAR-Vote [5] is an example of such a system.

Over 40 states now use some form of paper ballot for most voters [18]. Most of the remaining states are taking steps to adopt paper ballots. But *not all voting systems that use paper ballots are equally secure*.

Some are not even software independent. Some are software independent, but not strongly software independent, contestable, or defensible. In this report we explain:

- *Hand-marked paper ballot* systems are the only practical technology for contestable, strongly defensible voting systems.
- *Some ballot-marking devices (BMDs)* can be software independent, but they not strongly software independent, contestable, or defensible. Hacked or misprogrammed BMDs can alter election outcomes undetectably, so elections conducted using BMDs cannot provide public evidence that reported outcomes are correct. If BMD malfunctions are detected, there is no way to determine who

⁶Nor are they strongly software independent.

really won. Therefore BMDs should not be used by voters who are able to mark an optical-scan ballot with a pen.

- *All-in-one BMD or DRE+VVPAT voting machines* are not software independent, contestable, or defensible. They should not be used in public elections.

2 Background

We briefly review the kinds of election equipment in use, their vulnerability to computer hacking (or programming error), and in what circumstances risk-limiting audits can mitigate that vulnerability.

Voting equipment

Although a voter may form an intention to vote for a candidate or issue days, minutes, or seconds before actually casting a ballot, that intention is a psychological state that cannot be directly observed by anyone else. Others can have access to that intention through what the voter (privately) *expresses* to the voting technology by interacting with it, e.g., by making selections on a BMD or marking a ballot by hand.⁷ Voting systems must accurately record the vote as the voter *expressed* it.

With a *hand-marked paper ballot optical-scan* system, the voter is given a paper ballot on which all choices (candidates) in each contest are listed; next to each candidate is a *target* (typically an oval or other shape) which the voter marks with a pen to indicate a vote. Ballots may be either preprinted or printed (unvoted) at the polling place using *ballot on demand* printers. In either case, the voter creates a tamper-evident record of intent by marking the printed paper ballot with a pen.

Such hand-marked paper ballots may be scanned and tabulated at the polling place using a *precinct-count optical scanner* (PCOS), or may be brought to a central place to

⁷We recognize that voters make mistakes in expressing their intentions. For example, they may misunderstand the layout of a ballot or express an unintended choice through a perceptual error, inattention, or lapse of memory. The use of touchscreen technology does not necessarily correct for such user errors, as every smartphone user who has mistyped an important text message knows. Poorly designed ballots, poorly designed touchscreen interfaces, and poorly designed assistive interfaces increase the rate of error in voters' expressions of their votes. For the purposes of this report, we assume that properly engineered systems seek to minimize such usability errors.

be scanned and tabulated by a *central-count optical scanner* (CCOS). Mail-in ballots are typically counted by CCOS machines.

After scanning a ballot, a PCOS machine deposits the ballot in a secure, sealed ballot box for later use in recounts or audits; this is *ballot retention*. Ballots counted by CCOS are also retained for recounts or audits.⁸

Paper ballots can also be hand counted, but in most jurisdictions (especially where there are many contests on the ballot) this is hard to do quickly; Americans expect election-night reporting of unofficial totals. Hand counting—i.e., manually determining votes directly from the paper ballots—is appropriate for audits and recounts.

A *ballot-marking device* (BMD) provides a computerized user interface that presents the ballot to voters and captures their expressed selections—for instance, a touchscreen interface or an assistive interface that enables voters with disabilities to vote independently. Voter inputs (expressed votes) are recorded electronically. When a voter indicates that the ballot is complete and ready to be cast, the BMD prints a paper version of the electronically marked ballot. We use the term *BMD* for devices that mark ballots but do not tabulate or retain them, and *all-in-one* for devices that combine ballot marking, tabulation, and retention into the same paper path.

The paper ballot printed by a BMD may be in the same format as an optical-scan form (e.g., with ovals filled as if by hand) or it may list just the names of the candidate(s) selected in each contest. The BMD may also encode these selections into barcodes or QR codes for optical scanning. We discuss issues with barcodes later in this report.

An *all-in-one touchscreen voting machine* combines computerized ballot marking, tabulation, and retention in the same paper path. All-in-one machines come in several configurations:

- DRE+VVPAT machines—direct-recording electronic (DRE) voting machines with a voter-verifiable paper audit trail (VVPAT)—provide the voter a touchscreen (or other) interface, then print a paper ballot that is displayed to the voter under glass. The voter is expected to review this ballot and approve it, after which the machine deposits it into a ballot box. DRE+VVPAT machines do not contain optical scanners; that is, they do not read what is marked on the paper ballot; instead, they tabulate the vote directly from inputs to the touchscreen or other interface.

⁸Regulations and procedures governing custody and physical security of ballots are uneven and in many cases inadequate, but straightforward to correct because of decades of development of best practices.

- BMD+Scanner all-in-one machines⁹ provide the voter a touchscreen (or other) interface to input ballot choices and print a paper ballot that is ejected from a slot for the voter to inspect. The voter then reinserts the ballot into the slot, after which the all-in-one BMD+scanner scans it and deposits it into a ballot box. Or, some BMD+Scanner all-in-one machines display the paper ballot behind plexi-glass for the voter to inspect, before mechanically depositing it into a ballot box.

Opscan+BMD with separate paper paths. At least one model of voting machine (the Dominion ICP320) contains an optical scanner (opscan) and a BMD in the same cabinet,¹⁰ so that the optical scanner and BMD-printer are not in the same paper path; no possible configuration of the software could cause a BMD-marked ballot to be deposited in the ballot box without human handling of the ballot. We do not classify this as an *all-in-one* machine.

Hacking

There are many forms of computer hacking. In this analysis of voting machines we focus on the alteration of voting machine software so that it miscounts votes or mis-marks ballots to alter election outcomes. There are many ways to alter the software of a voting machine: a person with physical access to the computer can open it and directly access the memory; one can plug in a special USB thumbdrive that exploits bugs and vulnerabilities in the computer's USB drivers; one can connect to its WiFi port or Bluetooth port or telephone modem (if any) and exploit bugs in those drivers, or in the operating system.

“Air-gapping” a system (i.e., never connecting it to the Internet nor to any other network) does not automatically protect it. Before each election, election administrators must transfer a *ballot definition* into the voting machine by inserting a *ballot definition cartridge* that was programmed on election-administration computers that may have been connected previously to various networks; it has been demonstrated that vote-changing viruses can propagate via these ballot-definition cartridges [17].

Hackers might be corrupt insiders with access to a voting-machine warehouse; corrupt insiders with access to a county's election-administration computers; outsiders who can gain remote access to election-administration computers; outsiders who can

⁹Some voting machines, such as the ES&S ExpressVote, can be configured as either a BMD or a BMD+Scanner all-in-one. Others, such as the ExpressVoteXL, work only as all-in-one machines.

¹⁰More precisely, the ICP320 optical scanner and the BMD audio+buttons interface are in the same cabinet, but the printer is a separate box.

gain remote access to voting-machine manufacturers’ computers (and “hack” the firmware installed in new machines, or the firmware updates supplied for existing machines), and so on. Supply-chain hacks are also possible: the hardware installed by a voting system vendor may have malware pre-installed by the vendor’s component suppliers.¹¹

Computer systems (including voting machines) have so many layers of software that it is impossible to make them perfectly secure [23, pp. 89–91]. When manufacturers of voting machines use the best known security practices, adversaries may find it more difficult to hack a BMD or optical scanner—but not impossible. Every computer in every critical system is vulnerable to compromise through hacking, insider attacks or exploiting design flaws.

Election assurance through risk-limiting audits

To ensure that the reported electoral outcome of each contest corresponds to what the voters expressed, the most practical known technology is a *risk-limiting audit* (RLA) of trustworthy paper ballots [34, 35, 22]. The National Academies of Science, Engineering, and Medicine, recommend routine RLAs after every election [23], as do many other organizations and entities concerned with election integrity.¹²

The *risk limit* of a risk-limiting audit is the maximum chance that the audit will not correct the reported electoral outcome, if the reported outcome is wrong. “Electoral outcome” means the political result—who or what won—not the exact tally. “Wrong” means that the outcome does not correspond to what the voters expressed.

A RLA involves manually inspecting randomly selected paper ballots following a rigorous protocol. The audit stops if and when the sample provides convincing evidence that the reported outcome is correct; otherwise, the audit continues until every ballot has been inspected manually, which reveals the correct electoral outcome if the paper trail is trustworthy. RLAs protect against vote-tabulation errors, whether those errors are caused by failures to follow procedures, misconfiguration, miscalibration, faulty

¹¹Given that many chips and other components are manufactured in China and elsewhere, this is a serious concern. Carsten Schürmann has found Chinese pop songs on the internal memory of voting machines (C. Schürmann, personal communication, 2018). Presumably those files were left there accidentally—but this shows that malicious code *could* have been pre-installed deliberately, and that neither the vendor’s nor the election official’s security and quality control measures discovered and removed the extraneous files.

¹²Among them are the Presidential Commission on Election Administration, the American Statistical Association, the League of Women Voters, and Verified Voting Foundation.

engineering, bugs, or malicious hacking.¹³

The risk limit should be determined as a matter of policy or law. For instance, a 5% risk limit means that, if a reported outcome is wrong solely because of tabulation errors, there is at least a 95% chance that the audit procedure will correct it. Smaller risk limits give higher confidence in election outcomes, but require inspecting more ballots, other things being equal. RLAs never revise a correct outcome.

RLAs can be very efficient, depending in part on how the voting system is designed and how jurisdictions organize their ballots. If the computer results are accurate, an efficient RLA with a risk limit of 5% requires examining just a few—about 7 divided by the margin—ballots selected randomly from the contest.¹⁴ For instance, if the margin of victory is 10% and the results are correct, the RLA would need to examine about $7/10\% = 70$ ballots to confirm the outcome at 5% risk. For a 1% margin, the RLA would need to examine about $7/1\% = 700$ ballots. The sample size does not depend much on the total number of ballots cast in the contest, only on the margin of the winning candidate's victory.

RLAs assume that a full hand tally of the paper trail would reveal the correct electoral outcomes: the paper trail must be trustworthy. Other kinds of audits, such as *compliance audits* [6, 22, 38, 36] are required to establish whether the paper trail itself is trustworthy. Applying an RLA procedure to an untrustworthy paper trail cannot limit the risk that a wrong reported outcome goes uncorrected.

Properly preserved hand-marked paper ballots ensure that expressed votes are identical to recorded votes. But BMDs might not record expressed votes accurately, for instance, if BMD software has bugs, was misconfigured, or was hacked: BMD print-out is not a trustworthy record of the expressed votes. Neither a compliance audit nor a RLA can possibly check whether errors in recording expressed votes altered election outcomes. RLAs that rely on BMD output therefore cannot limit the risk that an incorrect reported election outcome will go uncorrected.

A paper-based voting system (such as one that uses optical scanners) is systematically more secure than a paperless system (such as DREs) *only if the paper trail is trustworthy and the results are checked against the paper trail using a rigorous method such as an RLA or full manual tally*. If it is possible that error, hacking, bugs, or mis-

¹³RLAs do not protect against problems that cause BMDs to print something other than what was shown to the voter on the screen, nor do they protect against problems with ballot custody.

¹⁴Technically, it is the *diluted margin* that enters the calculation. The diluted margin is the number of votes that separate the winner with the fewest votes from the loser with the most votes, divided by the number of ballots cast, including undervotes and invalid votes.

calibration caused the recorded-on-paper votes to differ from the expressed votes, an RLA or even a full hand recount cannot not provide convincing public evidence that election outcomes are correct: such a system cannot be *defensible*. In short, paper ballots provide little assurance against hacking if they are never examined or if the paper might not accurately reflect the votes expressed by the voters.

3 (Non)Contestability/Defensibility of BMDs

A BMD-generated paper trail is not a reliable record of the vote expressed by the voter. Like any computer, a BMD (or a DRE+VVPAT) is vulnerable to bugs, misconfiguration, hacking, installation of unauthorized (fraudulent) software, and alteration of installed software.

If a hacker sought to steal an election by altering BMD software, what would the hacker program the BMD to do? In cybersecurity practice, we call this the *threat model*.

The simplest threat model is this one: In some contests, not necessarily top-of-the-ticket, change a small percentage of the votes (such as 5%).

In recent national elections, analysts have considered a candidate who received 60% of the vote to have won by a landslide. Many contests are decided by less than a 10% margin. Changing 5% of the votes can change the margin by 10%, because “flipping” a vote for one candidate into a vote for a different candidate changes the difference in their tallies—i.e., the margin—by 2 votes. If hacking or bugs or misconfiguration could change 5% of the votes, that would be a very significant threat.

Although public and media interest often focus on top-of-the-ticket races such as President and Governor, elections for lower offices such as state representatives, who control legislative agendas and redistricting, and county officials, who manage elections and assess taxes, are just as important in our democracy. Altering the outcome of smaller contests requires altering fewer votes, so fewer voters are in a position to notice that their ballots were misprinted. And most voters are not as familiar with the names of the candidates for those offices, so they might be unlikely to notice if their ballots were misprinted, even if they checked.

Research in a real polling place in Tennessee during the 2018 election, found that half the voters *didn't look at all* at the paper ballot printed by a BMD, even when they were holding it in their hand and directed to do so while carrying it from the BMD to the optical scanner [13]. Those voters who did look at the BMD-printed ballot

spent *an average of 4 seconds* examining it to verify that the eighteen or more choices they made were correctly recorded. That amounts to 222 milliseconds per contest, barely enough time for the human eye to move and refocus under perfect conditions and not nearly enough time for perception, comprehension, and recall [27]. A study by other researchers [7], in a simulated polling place using real BMDs deliberately hacked to alter one vote on each paper ballot, found that only 6.6% of voters told a pollworker something was wrong.¹⁵¹⁶ The same study found that among voters who examined their hand-marked ballots, half were unable to recall key features of ballots cast moments before, a prerequisite step for being able to recall their own ballot choices. This finding is broadly consistent with studies of effects like “change blindness” or “choice blindness,” in which human subjects fail to notice changes made to choices made only seconds before [19].

Suppose, then, that 10% of voters examine their paper ballots carefully enough to even *see* the candidate’s name recorded as their vote for legislator or county commissioner. Of those, perhaps only half will remember the name of the candidate they intended to vote for.¹⁷

Of those who notice that the vote printed is not the candidate they intended to vote for, what will they think, and what will they do? Will they think, “Oh, I must have made a mistake on the touchscreen,” or will they think, “Hey, the machine is cheating or malfunctioning!” There’s no way for the voter to know for sure—voters do make mistakes—and there’s *absolutely* no way for the voter to prove to a pollworker or election official that a BMD printed something other than what the voter entered on the

¹⁵You might think, “the voter really *should* carefully review their BMD-printed ballot.” But because the scientific evidence shows that voters *do not* [13] and cognitively *cannot* [16] perform this task well, legislators and election administrators should provide a voting system that counts the votes *as voters express them*.

¹⁶Studies of voter confidence about their ability to verify their ballots are not relevant: in typical situations, subjective confidence and objective accuracy are at best weakly correlated. The relationship between confidence and accuracy has been studied in contexts ranging from eyewitness accuracy [8, 12, 40] to confidence in psychological clinical assessments [14] and social predictions [15]. The disconnect is particularly severe at high confidence. Indeed, this is known as “the overconfidence effect.” For a lay discussion, see *Thinking, Fast and Slow* by Nobel economist Daniel Kahnemann [20].

¹⁷We ask the reader, “do you know the name of the most recent losing candidate for county commissioner?” We recognize that some readers of this document *are* county commissioners, so we ask those readers to imagine the frame of mind of their constituents.

screen.¹⁸¹⁹

Either way, polling-place procedures generally advise voters to ask a pollworker for a new ballot if theirs does not show what they intended. Pollworkers should void that BMD-printed ballot, and the voter should get another chance to mark a ballot. Anecdotal evidence suggests that many voters are too timid to ask, or don't know that they have the right to ask, or are not sure whom to ask. Even if a voter asks for a new ballot, training for pollworkers is uneven, and we are aware of no formal procedure for resolving disputes if a request for a new ballot is refused. Moreover, there is no sensible protocol for ensuring that BMDs that misbehave are investigated—nor can there be, as we argue below.

Let's summarize. If a machine alters votes on 5% of the ballots (enabling it to change the margin by 10%), and 10% of voters check their ballots carefully and 50% of the voters who check notice the error, then optimistically we might expect $5\% \times 10\% \times 50\%$ or 0.25% of the voters to request a new ballot and correct their vote.²⁰ This means that the machine will change the margin by 9.75% and get away with it.

In this scenario, 0.25% of the voters, one in every 400 voters, has requested a new ballot. You might think, "that's a form of *detection* of the hacking." But it isn't, as a practical matter: a few individual voters may have detected that there was a problem, but there's no procedure by which this translates into any action that election administrators can take to correct the outcome of the election. Polling-place procedures *cannot correct or deter hacking, or even reliably detect it*, as we discuss next. This is essentially the distinction between a system that is merely software independent and one that is contestable: a change to the software that alters the outcome might generate evidence for an alert, conscientious, individual voter, but it does not generate public evidence that an election official can rely on to conclude there is a problem.

Even if some voters notice that BMDs are altering votes, there's no way to correct the election outcome. That is, BMD voting systems are *not contestable, not defen-*

¹⁸You might think, "the voter can prove it by showing someone that the vote on the paper doesn't match the vote onscreen." But that won't work. On a typical BMD, by the time a paper record is printed and ejected for the voter to hold and examine, the touchscreen no longer shows the voter's choice. You might think, "BMDs should be designed so that the choices still show on the screen for the voter to compare with the paper." But a hacked BMD could easily alter the on-screen choices to match the paper, *after* the voter hits the "print" button.

¹⁹Voters should *certainly not* videorecord themselves voting! That would defeat the privacy of the secret ballot and is illegal in most jurisdictions.

²⁰This calculation assumes that the 10% of voters who check are in effect a random sample of voters: voters' propensity to check BMD printout is not associated with their political preferences.

sible (and therefore *not strongly defensible*), and *not strongly software independent*. Suppose a state election official wanted to detect whether the BMDs are cheating, and correct election results, based on actions by those few alert voters who notice the error. What procedures could possibly work against the manipulation we are considering?

1. How about, “If at least 1 in 400 voters claims that the machine misrepresented their vote, void the entire election.”²¹ No responsible authority would implement such a procedure. A few dishonest voters could collaborate to invalidate entire elections simply by falsely claiming that BMDs changed their votes.
2. How about, “If at least 1 in 400 voters claims that the machine misrepresented their vote, then investigate.” Investigations are fine, but then what? The only way an investigation can ensure that the outcome accurately reflects what voters expressed to the BMDs is to void an election in which the BMDs have altered votes and conduct a new election. But how do you know whether the BMDs have altered votes, except based the claims of the voters?²² Furthermore, the investigation itself would suffer from the same problem as above: how can one distinguish between voters who detected BMD hacking or bugs from voters who just want to interfere with an election?

This is the essential security flaw of BMDs: few voters will notice and promptly report discrepancies between what they saw on the screen and what is on the BMD printout, and even when they do notice, there’s nothing appropriate that can be done. Even if election officials are convinced that BMDs malfunctioned, *there is no way to determine who really won*.

Therefore, BMDs should not be used by most voters.

Why can’t we rely on pre-election and post-election logic and accuracy testing, or parallel testing? Most, if not all, jurisdictions perform some kind of *logic and accuracy testing* (LAT) of voting equipment before elections. LAT generally involves voting on the equipment using various combinations of selections, then checking whether the

²¹Note that in many jurisdictions, far fewer than 400 voters use a given machine on election day: BMDs are typically expected to serve fewer than 300 voters per day. (The vendor ES&S recommended 27,000 BMDs to serve Georgia’s 7 million voters, amounting to 260 voters per BMD [33].) Recall also that the rate 1 in 400 is tied to the amount of manipulation. What if the malware flipped only one vote in 50, instead of 1 vote in 20? That could still change the margin by 4%, but—in this hypothetical—would be noticed by only one voter in 1,000, rather than one in 400. The smaller the margin, the less manipulation it would have taken to alter the electoral outcome.

²²Forensic examination of the BMD might show that it *was* hacked or misconfigured, but it cannot prove that the BMD *was not* hacked or misconfigured.

equipment tabulated the votes correctly. As the Volkswagen/Audi “Dieselgate” scandal shows, devices can be programmed to behave properly when they are tested but misbehave in use [11]. Therefore, LAT can never prove that voting machines performed properly in practice.

Parallel or “live” testing involves pollworkers or election officials using some BMDs at random times on election day to mark (but not cast) ballots with test patterns, then check whether the marks match the patterns. The idea is that the testing is not subject to the “Dieselgate” problem, because the machines cannot “know” they are being tested on election day.²³ As a practical matter, the number of tests required to provide a reasonable chance of detecting outcome-changing errors is prohibitive: it would leave no time for actual voting [37]. Moreover, it would require additional staff, infrastructure, and other resources.

Suppose, counterfactually, that it was practical to perform enough parallel testing to guarantee a large chance of detecting a problem if BMD hacking or malfunction altered electoral outcomes. Suppose, counterfactually, that election officials were required to conduct that amount of parallel testing during every election, and that the required equipment, staffing, infrastructure, and other resources were provided. Even then, the system would not be *strongly defensible*; that is, if testing detected a problem, there would be no way to determine who really won. The only remedy would be a new election.

Don’t voters need to check hand-marked ballots, too? It is always a good idea to check one’s work, but there is a substantial body of research (e.g., [28]) suggesting that preventing error as a ballot is being marked is a fundamentally different cognitive task than detecting an error on a previously marked ballot. In cognitively similar tasks, such as proof reading for non-spelling errors, ten percent rates of error detection are common [28, pp 167ff], whereas by carefully attending to the task of correctly marking their ballots, voters apparently can largely avoid marking errors.

A fundamental difference between hand-marked paper ballots and ballot-marking devices is that, with hand-marked paper ballots, voters are responsible for catching and

²³BMDs do “know” their own settings and other aspects of each voting session, so malware can use that information to target sessions that use the audio interface, increase the font size, use the sip-and-puff interface, set the language to something other than English, or take much longer than average to vote. (Voters who use those settings might be less likely to be believed if they report that the equipment altered their votes.) For parallel testing to have a good chance of detecting all outcome-changing problems, the tests must have a large chance of probing *every* combination of settings and voting patterns that includes enough ballots to change any contest result. It is not practical.

correcting *their own errors*, while if BMDs are used, voters are also responsible for catching *machine errors, bugs, and hacking*. Voters are the *only* people who can detect such problems with BMDs—but, as explained above, if voters do find problems, there’s no way they can prove to poll workers or election officials that there were problems and no way to ensure that election officials take appropriate remedial action.

4 Other tradeoffs, BMDs versus hand-marked opscan

Supporters of ballot-marking devices advance several other arguments for their use.

- **Mark legibility.** A common argument is that a properly functioning BMD will generate clean, error-free, unambiguous marks, while hand-marked paper ballots may contain mistakes and stray marks that make it impossible to discern a voter’s intent. However appealing this argument seems at first blush, the data are not nearly so compelling. Experience with statewide recounts in Minnesota and elsewhere suggest that truly ambiguous handmade marks are very rare.²⁴ For instance, 2.9 million hand-marked ballots were cast in the 2008 Minnesota race between Al Franken and Norm Coleman for the U.S. Senate. In a manual recount, between 99.95% and 99.99% of ballots were unambiguously marked.^{25 26} In addition, usability studies of hand-marked bubble ballots—the kind in most common use in U.S. elections—indicate a *voter* error rate of 0.6%, much lower than the 2.5–3.7% error rate for machine-marked ballots [16].²⁷ Moreover, modern image-based opscan equipment (*digital scan machinery*) is better than older

²⁴States do need clear and complete regulations for interpreting voter marks.

²⁵“During the recount, the Coleman and Franken campaigns initially challenged a total of 6,655 ballot-interpretation decisions made by the human recounters. The State Canvassing Board asked the campaigns to voluntarily withdraw all but their most serious challenges, and in the end approximately 1,325 challenges remained. That is, approximately 5 ballots in 10,000 were ambiguous enough that one side or the other felt like arguing about it. The State Canvassing Board, in the end, classified all but 248 of these ballots as votes for one candidate or another. That is, approximately 1 ballot in 10,000 was ambiguous enough that the bipartisan recount board could not determine an intent to vote.” [1] See also [25]

²⁶We have found that some local election officials consider marks to be ambiguous if *machines* cannot read the marks. That is a different issue from *humans* being unable to interpret the marks. Errors in machine interpretation of voter intent can be dealt with by manual audits: if the reported outcome is wrong because machines misinterpreted handmade marks, a RLA has a known, large chance of correcting the outcome.

²⁷Better designed user interfaces (UI) might reduce the error rate for machine-marked ballots below the historical rate for DREs; however, UI improvements cannot keep BMDs from printing something other than what the voter is shown on the screen.

“marksense” machines at interpreting imperfect marks. Thus, mark legibility is not a good reason to adopt BMDs for all voters.

- **Undervotes, overvotes.** Another argument offered for BMDs is that the machines can alert voters to undervotes and prevent overvotes. That is true, but modern PCOS systems can also alert a voter to overvotes and undervotes, allowing a voter to eject the ballot and correct it.
- **Bad ballot design.** Ill-designed paper ballots, just like ill-designed touchscreen interfaces, may lead to unintentional undervotes [24]. For instance, the 2006 Sarasota, Florida, touchscreen ballot was badly designed. The 2018 Broward County, Florida, opscan ballot was badly designed: it violated three separate guidelines from the EAC’s 2007 publication, “Effective Designs for the Administration of Federal Elections, Section 3: Optical scan ballots.” [39] In both of these cases (touchscreens in 2006, hand-marked optical-scan in 2018), undervote rates were high. The solution is to follow standard, published ballot-design guidelines and other best practices, both for touchscreens and for hand-marked ballots [3, 24].
- **Low-tech paper-ballot fraud.** All paper ballots, however they are marked, are vulnerable to *loss*, *ballot-box stuffing*, *alteration*, and *substitution* between the time they are cast and the time they are recounted. That’s why it is so important to make sure that ballot boxes are always in multiple-person (preferably bipartisan) custody whenever they are handled, and that appropriate physical security measures are in place. Strong, verifiable chain-of-custody protections are essential.

Hand-marked paper ballots are vulnerable to alteration by anyone with a pen. Both hand-marked and BMD-marked paper ballots are vulnerable to substitution: anyone who has poorly supervised access to a legitimate BMD during election day can create fraudulent ballots, not necessarily to deposit them in the ballot box immediately (in case the ballot box is well supervised on election day) but with the hope of substituting it later in the chain of custody.²⁸

All those attacks (on hand-marked and on BMD-marked paper ballots) are fairly low-tech. There are also higher-tech ways of producing ballots indistinguishable from BMD-marked ballots for substitution into the ballot box if there is inadequate chain-of-custody protection.

- **Accessible voting technology.** When hand-marked paper ballots are used with PCOS, there is (as required by law) also an accessible voting technology available in the polling place for voters unable to mark a paper ballot with a pen. This

²⁸Some BMDs print a barcode indicating when and where the ballot was produced, but that does not prevent such a substitution attack against currently EAC-certified, commercially available BMDs. We understand that systems under development might make ballot-substitution attacks against BMDs more difficult.

is typically a BMD or a DRE. When the accessible voting technology is not the same as what most voters vote on—when it is used by very few voters—it may happen that the accessible technology is ill-maintained or even (in some polling places) not even properly set up by pollworkers. This is a real problem. One proposed solution is to require all voters to use the same BMD or all-in-one technology. But the failure of some election officials to properly maintain their accessible equipment is not a good reason to adopt BMDs for *all* voters. Among other things, it would expose all voters to the security flaws described above.²⁹ Other advocates object to the idea that disabled voters must use a different method of marking ballots, arguing that their rights are thereby violated. Both HAVA and ADA require reasonable accommodations for voters with physical and cognitive impairments, but neither law requires that those accommodations must be used by all voters. To best enable and facilitate participation by all voters, each voter should be provided with a means of casting a vote best suited to their abilities.

- **Ballot printing costs.** Preprinted optical-scan ballots cost 20–50 cents each.³⁰ Blank cards for BMDs cost up to 15 cents each, depending on the make and model of BMD.³¹ But optical-scan ballots must be preprinted for as many voters as *might* show up, whereas blank BMD cards are consumed in proportion to how many voters *do* show up. The Open Source Election Technology Institute (OSET) conducted an independent study of total life cycle costs³² for hand-marked paper ballots and BMDs in conjunction with the 2019 Georgia legislative debate regarding BMDs [26]. OSET concluded that, even in the most optimistic (i.e., lowest cost) scenario for BMDs and the most pessimistic (i.e., highest cost) scenario for hand-marked paper ballots and ballot-on-demand (BOD) printers—which can print unmarked ballots as needed—the total lifecycle costs for BMDs would be higher than the corresponding costs for hand-marked paper ballots.³³
- **Vote centers.** To run a vote center that serves many election districts with different ballot styles, one must be able to provide each voter a ballot containing

²⁹Also, some accessibility advocates argue that requiring disabled voters to use BMDs compromises their privacy since hand-marked ballots are easily distinguishable from machine marked ballots. That issue can be addressed without BMDs-for-all: Accessible BMDs are already available and in use that mark ballots with marks that cannot easily be distinguished from hand-marked ballots.

³⁰Single-sheet (one- or two-side) ballots cost 20-28 cents; double-sheet ballots needed for elections with many contests cost up to 50 cents.

³¹Ballot cards for ES&S ExpressVote cost about 15 cents. New Hampshire's (One4All / Prime III) BMDs used by sight-impaired voters use plain paper that is less expensive.

³²They include not only the cost of acquiring and implementing systems but also the ongoing licensing, logistics, and operating (purchasing paper stock, printing, and inventory management) costs.

³³BOD printers currently on the market arguably are best suited for vote centers, but less expensive options suited for polling places could be developed. Indeed, BMDs that print full-face ballots could be re-purposed as BOD printers for polling place use, with modest changes to the programming.

the contests that voter is eligible to vote in, possibly in a number of different languages. This is easy with BMDs, which can be programmed with all the appropriate ballot definitions. With preprinted optical-scan ballots, the PCOS can be programmed to *accept* many different ballot styles, but the vote center must still maintain *inventory* of many different ballots. BOD printers are another economical alternative for vote centers.³⁴

- **Paper/storage.** BMDs that print summary cards rather than full-face ballots can save paper and storage space. However, many BMDs print full-face ballots—so they do not save storage—while many BMDs that print summary cards (which could save storage) use thermal printers and paper that is fragile and can fade in a few months.³⁵

Advocates of hand-marked paper ballot systems advance these additional arguments.

- **Cost.** Using BMDs for all voters substantially increases the cost of acquiring, configuring, and maintaining the voting system. One PCOS can serve 1200 voters in a day, while one BMD can serve only about 260 [33]—though both these numbers vary greatly depending on the length of the ballot and the length of the day. OSET analyzed the relative costs of acquiring BMDs for Georgia’s nearly seven million registered voters versus a system of hand-marked paper ballots, scanners, and BOD printers [26]. A BMD solution for Georgia would cost taxpayers between 3 and 5 times more than a system based on hand-marked paper ballots. Open-source systems might eventually shift the economics, but current commercial universal-use BMD systems are more expensive than systems that use hand-marked paper ballots for most voters.
- **Mechanical reliability and capacity.** Pens are likely to have less downtime than BMDs. It is easy and inexpensive to get more pens and privacy screens when additional capacity is needed. If a precinct-count scanner goes down, people can still mark ballots with a pen; if the BMD goes down, voting stops. Thermal

³⁴Ballot-on-demand printers *may* require maintenance such as replacement of toner cartridges. This is readily accomplished at a vote center with a professional staff. Ballot-on-demand printers may be a less attractive option for many small precincts on election day, where there is no professional staff—but on the other hand, they are less necessary, since far fewer ballot styles will be needed in any one precinct.

³⁵The California Top-To-Bottom Review (TTBR) of voting systems found that thermal paper can also be covertly spoiled wholesale using common household chemicals <https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/red-diebold.pdf>, last visited 8 April 2019. The fact that thermal paper printing can fade or deteriorate rapidly might mean it does not satisfy the federal requirement to preserve voting materials for 22 months. <http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title52-section20701&num=0&edition=prelim>, last visited 8 April 2019.

printers used in DREs with VVPAT are prone to jams; those in BMDs might have similar flaws.

These secondary pros and cons of BMDs do not outweigh the primary security and accuracy concern: BMDs, if hacked or erroneously programmed, can change votes in a way that is not correctable. BMD voting systems are not contestable or defensible. Audits that rely on BMD printout cannot make up for this defect in the paper trail: they cannot reliably detect or correct problems that altered election outcomes.

Barcodes

A controversial feature of some BMDs allows them to print 1-dimensional or 2-dimensional barcodes on the paper ballots. A 1-dimensional barcode resembles the pattern of vertical lines used to identify products by their universal product codes. A 2-dimensional barcode or QR code is a rectangular area covered in coded image *modules* that encode more complex patterns and information. BMDs print barcodes on the same paper ballot that contains human-readable ballot choices. Voters using BMDs are expected to verify the human-readable printing on the paper ballot card, but the presence of barcodes with human-readable text poses some significant problems.

- **Barcodes are not human readable.** The whole purpose of a paper ballot is to be able to recount (or audit) the *voters'* votes in a way independent of any (possibly hacked or buggy) computers. If the official vote on the ballot card is the barcode, then it is impossible for the voters to verify that the official vote they cast is the vote they expressed. Therefore, before a state even *considers* using BMDs that print barcodes (and we do not recommend doing so), the State must ensure by statute that recounts and audits are based *only* on the human-readable portion of the paper ballot. Even so, audits based on untrustworthy paper trails suffer from the verifiability the problems outlined above.
- **Ballot cards with barcodes contain two different votes.** Suppose a state does ensure by statute that recounts and audits are based on the human-readable portion of the paper ballot. Now a BMD-marked ballot card with both barcodes and human-readable text contains two different votes in each contest: the barcode (used for electronic tabulation), and the human-readable selection printout (official for audits and recounts). In few (if any) states has there even been a discussion of the legal issues raised when the official markings to be counted differ between the original count and a recount.
- **Barcodes pose technical risks.** Any coded input into a computer system—including wired network packets, WiFi, USB thumbdrives, *and barcodes*—pose

the risk that the input-processing software can be vulnerable to attack via deliberately ill-formed input. Over the past two decades, many such vulnerabilities have been documented on *each* of these channels (including barcode readers) that, in the worst case, give the attacker complete control of a system.³⁶ If an attacker were able to compromise a BMD, the barcodes are an attack vector for the attacker to take over an optical scanner (PCOS or CCOS), too. Since it is good practice to close down all such unneeded attack vectors into PCOS or CCOS voting machines (e.g., don't connect your PCOS to the Internet!), it is also good practice to avoid unnecessary attack channels such as barcodes.

End-to-End Verifiable BMDs

In all BMD systems currently on the market, and in all BMD systems certified by the EAC, the printed ballot or ballot summary is the only channel by which voters can verify the correct recording of their ballots, independently of the computers. The analysis in this paper applies to all of those BMD systems.

There is a class of voting systems called “end-to-end verifiable” (E2E-V), which provide an alternate mechanism for voters to verify their votes [2]. Some E2E-V systems incorporate BMDs, for instance STAR-Vote³⁷ [5]. As we discuss above in Section 1, such systems are not contestable, defensible, or strongly software independent. In any event, no E2E-V system is currently certified by the EAC, nor to our knowledge is any such system under review for certification, nor are any of the 5 major voting-machine vendors offering such a system for sale.³⁸

³⁶An example of a barcode attack is based on the fact that many commercial barcode-scanner components (which system integrators use to build cash registers or voting machines) treat the barcode scanner using the same operating-system interface as if it were a keyboard device; and then some operating systems allow “keyboard escapes” or “keyboard function keys” to perform unexpected operations.

³⁷The STAR-Vote system is actually a DRE+VVPAT system with a smart ballot box, rather than a BMD system: voters interact with a device that captures their votes electronically and prints a paper record that voters can inspect, but the electronic votes are held “in limbo” until the paper ballot is deposited in the smart ballot box. The ballot box does not read the votes from the ballot; rather, depositing the ballot tells the system that it has permission to cast the vote that it had already recorded from the touchscreen.

³⁸Some vendors, notably Scytl, have sold systems advertised as E2E-V in other countries. Those systems were not in fact E2E-V. Moreover, serious security flaws have been found in their implementations. See, e.g., [21].

5 Insecurity of All-in-One BMDs

Some voting machines incorporate a BMD interface, printer, and optical scanner into the same cabinet. Other DRE+VVPAT voting machines incorporate ballot-marking, tabulation, and paper-printout retention, but without scanning. These are often called “all-in-one” voting machines. To use an all-in-one machine, the voter makes choices on a touchscreen or through a different accessible interface. When the selections are complete, the BMD prints the completed ballot for the voter to review and verify, before depositing the ballot in a ballot box attached to the machine.

Such machines are especially unsafe: like any BMD described in Section 3 they are not contestable or defensible, but in addition, if hacked they can print votes onto the ballot *after* the voter last inspects the ballot.

- The ES&S ExpressVote (in all-in-one mode) allows the voter to mark a ballot by touchscreen or audio interface, then prints a paper ballot card and ejects it from a slot. The voter has the opportunity to review the ballot, then the voter redeposits the ballot into the same slot, where it is scanned and deposited into a ballot box.
- The ES&S ExpressVoteXL allows the voter to mark a ballot by touchscreen or audio interface, then prints a paper ballot and displays it under glass. The voter has the opportunity to review the ballot, then the voter touches the screen to indicate “OK,” and the machine pulls paper ballot up (still under glass) and into the integrated ballot box.
- The Dominion ImageCast Evolution (ICE) allows the voter to deposit a hand-marked paper ballot, which it scans and drops into the attached ballot box. *Or*, a voter can use a touchscreen or audio interface to direct the marking of a paper ballot, which the voting machine ejects through a slot for review; then the voter redeposits the ballot into the slot, where it is scanned and dropped into the ballot box.

In all three of these machines, the ballot-marking printer is in the same paper path as the mechanism to deposit marked ballots into an attached ballot box. This opens up a very serious security vulnerability: the voting machine can mark the paper ballot (to add votes or spoil already-cast votes) after the last time the voter sees the paper, and then deposit that marked ballot into the ballot box without the possibility of detection.

Vote-stealing software could easily be constructed that looks for *undervotes* on the ballot, and marks those unvoted spaces for the candidate of the hacker’s choice. This is very straightforward to do on optical-scan bubble ballots (as on the Dominion ICE) where undervotes are indicated by no mark at all. On machines such as the ExpressVote

and ExpressVoteXL, the normal software indicates an undervote with the words NO SELECTION MADE on the ballot summary card. Hacked software could simply leave a blank space there (most voters wouldn't notice the difference), and then fill in that space and add a matching bar code after the voter has clicked "cast this ballot."

An even worse feature of the ES&S ExpressVote and the Dominion ICE is the *auto-cast* configuration setting (in the manufacturer's standard software) that allows the voter to indicate, "don't eject the ballot for my review, just print it and cast it without me looking at it." If fraudulent software were installed in the ExpressVote, it could change *all* the votes of any voter who selected this option, because the voting machine software would know *in advance of printing* that the voter had waived the opportunity to inspect the printed ballot. We call this auto-cast feature "permission to cheat" [4].

Regarding these all-in-one machines, we conclude:

- Any machine with ballot printing in the same paper path with ballot deposit is not *software independent*; it is *not* the case that "an error or fault in the voting system software or hardware cannot cause an undetectable change in election results." Therefore such all-in-one machines do not comply with the VVSG 2.0 (the Election Assistance Commission's Voluntary Voting Systems Guidelines). Such machines are not contestable or defensible, either.
- All-in-one machines on which all voters use the BMD interface to mark their ballots (such as the ExpressVote and ExpressVoteXL) *also* suffer from the same serious problem as ordinary BMDs: most voters do not review their ballots effectively, and elections on these machines are not contestable or defensible.
- The auto-cast option for a voter to allow the paper ballot to be cast without human inspection is particularly dangerous, and states must insist that vendors disable or eliminate this mode from the software. However, even disabling the auto-cast feature does not eliminate the risk of undetected vote manipulation.

Remark. The Dominion ImageCast Precinct ICP320 is a precinct-count optical scanner (PCOS) that also contains an audio+buttons ballot-marking interface for disabled voters. This machine can be configured to cast electronic-only ballots from the BMD interface, or an external printer can be attached to print paper optical-scan ballots from the BMD interface. When the external printer is used, that printer's paper path is *not* connected to the scanner+ballot-box paper path (a person must take the ballot from the printer and deposit it into the scanner slot). Therefore this machine is as safe to use as any PCOS with a separate external BMD.

6 Conclusion

Ballot-Marking Devices produce ballots that do not necessarily record the vote expressed by the voter when they enter their selections on the touchscreen: hacking, bugs, and configuration errors can cause the BMDs to print votes that differ from what the voter entered and verified electronically. Because outcome-changing errors in BMD printout do not produce public evidence, BMD systems are not *contestable*. Because there is no way to generate convincing public evidence that reported outcomes are correct despite any BMD malfunctions that might have occurred, BMD systems are not *defensible*. Therefore, BMDs should not be used by voters who can hand mark paper ballots.

All-in-one voting machines, which combine ballot-marking and ballot-box-deposit into the same paper path, are even worse. They have all the disadvantages of BMDs (they are not contestable or defensible), and they can mark the ballot after the voter has inspected it. Therefore they are not even *software independent*, and should not be used by those voters who are capable of marking, handling, and visually inspecting a paper ballot.

When computers are used to record votes, the original transaction (the voter's expression of the votes) is not documented in a verifiable way.³⁹ When pen-and-paper is used to record the vote, the original expression of the vote *is* documented in a verifiable way (if demonstrably secure chain of custody of the paper ballots is maintained). Audits of elections conducted with hand-marked paper ballots, counted by optical scanners, can ensure that reported election outcomes are correct. Audits of elections conducted with BMDs *cannot* ensure that reported outcomes are correct.

References

- [1] A.W. Appel. Optical-scan voting extremely accurate in Minnesota. *Freedom to Tinker*, January 2009. <https://freedom-to-tinker.com/2009/01/21/optical-scan-voting-extremely-accurate-minnesota/>.

³⁹It is conceivable that cryptographic protocols like those used in E2E-V systems could be used to create BMD-based systems that are contestable and defensible, but no such system exists, nor, to our knowledge, has such a design been worked out in principle. Existing E2E-V systems that use a computer to print (encrypted) selections are neither contestable nor defensible, as explained in Section 1.

- [2] A.W. Appel. End-to-end verifiable elections. *Freedom to Tinker*, November 2018. <https://freedom-to-tinker.com/2018/11/05/end-to-end-verifiable-elections/>.
- [3] A.W. Appel. Florida is the Florida of ballot-design mistakes. *Freedom to Tinker*, November 2018. <https://freedom-to-tinker.com/2018/11/14/florida-is-the-florida-of-ballot-design-mistakes/>.
- [4] A.W. Appel. Serious design flaw in ESS ExpressVote touchscreen: “permission to cheat”. *Freedom to Tinker*, September 2018. <https://freedom-to-tinker.com/2018/09/14/serious-design-flaw-in-ess-expressvote-touchscreen-permission-to-cheat/>.
- [5] J. Benaloh, M. Byrne, B. Eakin, P. Kortum, N. McBurnett, O. Pereira, P.B. Stark, , and D.S. Wallach. Star-vote: A secure, transparent, auditable, and reliable voting system. *JETS: USENIX Journal of Election Technology and Systems*, 1:18–37, 2013.
- [6] J. Benaloh, D. Jones, E. Lazarus, M. Lindeman, and P.B. Stark. SOBA: Secrecy-preserving observable ballot-level audits. In *Proceedings of the 2011 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE '11)*. USENIX, 2011.
- [7] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman. Can voters detect malicious manipulation of ballot marking devices? In *41st IEEE Symposium on Security and Privacy*, page (to appear). IEEE, 2020.
- [8] R. K. Bothwell, K.A. Deffenbacher, and J.C. Brigham. Correlation of eyewitness accuracy and confidence: Optimality hypothesis revisited. *Journal of Applied Psychology*, 72:691–695, 1987.
- [9] D. Chaum, A. Essex, R.T. Carback III, J. Clark, S. Popoveniuc, A.T. Sherman, and P. Vora. Scantegrity: End-to-end voter verifiable optical-scan voting. *IEEE Security & Privacy*, 6:40–46, 2008.
- [10] Election Assistance Commission. Voluntary voting systems guidelines 2.0, September 2017. https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf.
- [11] Moritz Contag, Guo Li, Andre Pawlowski, Felix Domke, Kirill Levchenko, Thorsten Holz, and Stefan Savage. How they did it: An analysis of emission defeat devices in modern automobiles. In *2017 IEEE Symposium on Security and Privacy*, pages 231–250. IEEE, 2017.

- [12] K. Deffenbacher. Eyewitness accuracy and confidence: Can we infer anything about their relation? *Law and Human Behavior*, 4:243–260, 1980.
- [13] R. DeMillo, R. Kadel, and M. Marks. What voters are asked to verify affects ballot verification: A quantitative analysis of voters’ memories of their ballots, November 2018. <https://ssrn.com/abstract=3292208>.
- [14] S.L. Desmarais, T.L. Nicholls, J. D. Read, and J. Brink. Confidence and accuracy in assessments of short-term risks presented by forensic psychiatric patients. *The Journal of Forensic Psychiatry & Psychology*, 21(1):1–22, 2010.
- [15] D. Dunning, D.W. Griffin, J.D. Milojkovic, and L. Ross. The overconfidence effect in social prediction. *Journal of Personality and Social Psychology*, 58:568–581, 1990.
- [16] S.P. Everett. *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection*. PhD thesis, Rice University, 2007.
- [17] A.J. Feldman, J.A. Halderman, and E.W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. In *2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 2007)*, August 2007.
- [18] Verified Voting Foundation. The verifier – polling place equipment – november 2018, November 2018. <https://www.verifiedvoting.org/verifier/>.
- [19] P. Johansson, L. Hall, and S. Sikstrom. From change blindness to choice blindness. *Psychologia*, 51:142–155, 2008.
- [20] D. Kahnemann. *Thinking, fast and slow*. Farrar, Straus and Giroux, 2011.
- [21] S. J. Lewis, O. Pereira, and V. Teague. Ceci n’est pas une preuve: The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system, 2019. <https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf>.
- [22] M. Lindeman and P.B. Stark. A gentle introduction to risk-limiting audits. *IEEE Security and Privacy*, 10:42–49, 2012.
- [23] National Academies of Sciences, Engineering, and Medicine. *Securing the Vote: Protecting American Democracy*. The National Academies Press, Washington, DC, September 2018.

- [24] L. Norden, M. Chen, D. Kimball, and W. Quesenbery. Better Ballots, 2008. Brennan Center for Justice, <http://www.brennancenter.org/publication/better-ballots>.
- [25] Office of the Minnesota Secretary of State. Minnesota’s historic 2008 election, 2009. <https://www.sos.state.mn.us/media/3078/minnesotas-historic-2008-election.pdf>.
- [26] E. Perez. Georgia state election technology acquisition: A reality check. OSET Institute Briefing, March 2019. https://trustthevote.org/wp-content/uploads/2019/03/06Mar19-OSETBriefing_GeorgiaSystemsCostAnalysis.pdf.
- [27] K. Rayner and M.S. Castelhana. Eye movements during reading, scene perception, and visual search, 2009. *Q J Experimental Psychology*, 2009, August 62(8), 1457-1506.
- [28] J. Reason. *Human Error (20th Printing)*. Cambridge University Press, New York, 2009.
- [29] R.L. Rivest and J.P. Wack. On the notion of software independence in voting systems, July 2006. <http://vote.nist.gov/SI-in-voting.pdf>.
- [30] Ronald L Rivest. On the notion of ‘software independence’ in voting systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 366(1881):3759–3767, 2008.
- [31] Ronald L Rivest and Madars Virza. Software independence revisited. In *Real-World Electronic Voting*, pages 19–34. Auerbach Publications, 2016.
- [32] P.Y.A. Ryan, D. Bismark amnd J. Heather, and S. Schneiderand Z. Xia. The prêt à voter verifiable election system. *IEEE Transactions on Information Forensics and Security*, 4:662–673, 2009.
- [33] Election Systems and Software. State of Georgia Electronic Request for Information New Voting System Event Number: 47800-SOS0000035, 2018. <http://sos.ga.gov/admin/files/ESS%20RFI%20-%20Final%20-%20Redacted.pdf>.
- [34] P.B. Stark. Conservative statistical post-election audits. *Annals of Applied Statistics*, 2:550–581, 2008.

- [35] P.B. Stark. Risk-limiting post-election audits: P -values from common probability inequalities. *IEEE Transactions on Information Forensics and Security*, 4:1005–1014, 2009.
- [36] P.B. Stark. An introduction to risk-limiting audits and evidence-based elections, 2018. Testimony prepared for the California Little Hoover Commission, <https://www.stat.berkeley.edu/~stark/Preprints/lhc18.pdf>.
- [37] P.B. Stark. There is no reliable way to detect hacked ballot-marking devices. <https://arxiv.org/abs/1908.08144>, 2019.
- [38] P.B. Stark and D.A. Wagner. Evidence-based elections. *IEEE Security and Privacy*, 10:33–41, 2012.
- [39] U. S. Election Assistance Commission. Effective designs for the administration of federal elections, June 2007. https://www.eac.gov/assets/1/1/EAC_Effective_Election_Design.pdf.
- [40] J.T. Wixted and G.L. Wells. The relationship between eyewitness confidence and identification accuracy: A new synthesis. *Psychological Science in the Public Interest*, 2017.

EXHIBIT 11 A

The State of Texas



Elections Division
P.O. Box 12060
Austin, Texas 78711-2060
www.sos.texas.gov

Phone: 512-463-5650
Fax: 512-475-2811
Dial 7-1-1 For Relay Services
(800) 252-VOTE (8683)

Ruth R. Hughes
Secretary of State

REPORT OF REVIEW OF DOMINION VOTING SYSTEMS DEMOCRACY SUITE 5.5-A

PRELIMINARY STATEMENT

On October 2-3, 2019, Dominion Voting Systems (“Dominion” or the “Vendor”) presented the Democracy Suite 5.5-A system for examination and certification. The examination was conducted in Austin, Texas. Pursuant to Sections 122.035(a) and (b) of the Texas Election Code, the Secretary of State appointed the following examiners:

1. Mr. Tom Watson, an expert in electronic data communication systems;
2. Mr. Brian Mechler, an expert in electronic data communication systems;
3. Mr. Brandon Hurley, an expert in election law and procedure; and
4. Mr. Charles Pinney, an expert in election law and procedure.

Pursuant to Section 122.035(a), the Texas Attorney General appointed the following examiners:

1. Dr. Jim Sneeringer, an expert in electronic data communication systems; and
2. Mr. Ryan Vassar, an employee of the Texas Attorney General.

On October 2, 2019, Mr. Pinney, Mr. Mechler, and Dr. Sneeringer witnessed the installation of the Democracy Suite 5.5-A software and firmware that the Office of the Texas Secretary of State (the “Office”) received directly from the Independent Testing Authority. The next day, Mr. Pinney examined the accessibility components of the ImageCast X Ballot Marking Device.

On October 3, 2019, the Vendor demonstrated the Democracy Suite 5.5-A system and answered questions presented by the examiners. Test ballots were then processed on each voting device. The results were accumulated and later verified for accuracy by staff of the Secretary of State.

Examiner reports regarding the Democracy Suite 5.5-A system are attached hereto and incorporated herein by this reference.

On December 27, 2019, pursuant to Section 122.0371 of the Texas Election Code, the Office held a public hearing for interested persons to express views for or against the certification of the Democracy Suite 5.5-A system.

BRIEF DESCRIPTION OF DEMOCRACY SUITE 5.5-A

The Democracy Suite 5.5-A system is an updated version of the Democracy Suite 5.5 system, which was denied certification by the Office on June 20, 2019. The Democracy Suite 5.5-A system includes certain software and hardware updates to the Suite 5.5 version.

Democracy Suite 5.5-A has been evaluated at an accredited independent voting system laboratory for conformance to the 2005 Voluntary Voting System Guidelines (VVSG). Democracy Suite 5.5-A was certified by the Election Assistance Commission (EAC) on January 30, 2019.

The components of Democracy Suite 5.5-A are as follows:

Component	Version	Description
EMS – Election Management System	5.5.12.1	Election Management System
ADJ – Adjudication	5.5.8.1	
ICC – ImageCast Central	5.5.3.0002	Central scanner
ICX – ImageCast X BMD	5.5.10.30	Ballot marking device
ICP – ImageCast Precinct	5.5.3-0002	Precinct scanner

FINDINGS

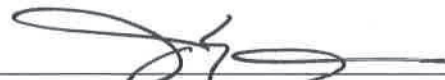
The following are the findings, based on written evidence submitted by the Vendor in support of its application for certification, oral evidence presented at the examination, and the findings of the voting system examiners as set out in their written reports.

The examiner reports identified multiple hardware and software issues that preclude the Office of the Texas Secretary of State from determining that the Democracy Suite 5.5-A system satisfies each of the voting-system requirements set forth in the Texas Election Code. Specifically, the examiner reports raise concerns about whether the Democracy Suite 5.5-A system is suitable for its intended purpose; operates efficiently and accurately; and is safe from fraudulent or unauthorized manipulation. Therefore, the Democracy Suite 5.5-A system and corresponding hardware devices do not meet the standards for certification prescribed by Section 122.001 of the Texas Election Code.

CONCLUSION

Accordingly, based upon the foregoing, I hereby deny certification of Dominion Voting Systems' Democracy Suite 5.5-A system for use in Texas elections.

Signed under my hand and seal of office, this 24th day of January 2020.



JOSE A. ESPARZA
DEPUTY SECRETARY OF STATE

EXHIBIT 11 B

The State of Texas



Elections Division
P.O. Box 12060
Austin, Texas 78711-2060
www.sos.texas.gov

Phone: 512-463-5650
Fax: 512-475-2811
Dial 7-1-1 For Relay Services
(800) 252-VOTE (8683)

Ruth R. Hughs
Secretary of State

REPORT OF REVIEW OF DOMINION VOTING SYSTEMS DEMOCRACY SUITE 5.5-A

PRELIMINARY STATEMENT

On October 2-3, 2019, Dominion Voting Systems (“Dominion” or the “Vendor”) presented the Democracy Suite 5.5-A system for examination and certification. The examination was conducted in Austin, Texas. Pursuant to Sections 122.035(a) and (b) of the Texas Election Code, the Secretary of State appointed the following examiners:

1. Mr. Tom Watson, an expert in electronic data communication systems;
2. Mr. Brian Mechler, an expert in electronic data communication systems;
3. Mr. Brandon Hurley, an expert in election law and procedure; and
4. Mr. Charles Pinney, an expert in election law and procedure.

Pursuant to Section 122.035(a), the Texas Attorney General appointed the following examiners:

1. Dr. Jim Sneeringer, an expert in electronic data communication systems; and
2. Mr. Ryan Vassar, an employee of the Texas Attorney General.

On October 2, 2019, Mr. Pinney, Mr. Mechler, and Dr. Sneeringer witnessed the installation of the Democracy Suite 5.5-A software and firmware that the Office of the Texas Secretary of State (the “Office”) received directly from the Independent Testing Authority. The next day, Mr. Pinney examined the accessibility components of the ImageCast X Ballot Marking Device.

On October 3, 2019, the Vendor demonstrated the Democracy Suite 5.5-A system and answered questions presented by the examiners. Test ballots were then processed on each voting device. The results were accumulated and later verified for accuracy by staff of the Secretary of State.

Examiner reports regarding the Democracy Suite 5.5-A system are attached hereto and incorporated herein by this reference.

BRIEF DESCRIPTION OF DEMOCRACY SUITE 5.5-A

The Democracy Suite 5.5-A system is an updated version of the Democracy Suite 5.5 system, which was denied certification by the Office on June 20, 2019. The Democracy Suite 5.5-A system includes certain software and hardware updates to the Suite 5.5 version.

Democracy Suite 5.5-A has been evaluated at an accredited independent voting system laboratory for conformance to the 2005 Voluntary Voting System Guidelines (VVSG). Democracy Suite 5.5-A was certified by the Election Assistance Commission (EAC) on January 30, 2019.

The components of Democracy Suite 5.5-A are as follows:

Component	Version	Description
EMS – Election Management System	5.5.12.1	Election Management System
ADJ – Adjudication	5.5.8.1	
ICC – ImageCast Central	5.5.3.0002	Central scanner
ICX – ImageCast X BMD	5.5.10.30	Ballot marking device
ICP – ImageCast Precinct	5.5.3-0002	Precinct scanner

FINDINGS


The following are the findings, based on written evidence submitted by the Vendor in support of its application for certification, oral evidence presented at the examination, and the findings of the voting system examiners as set out in their written reports.

The examiner reports identified multiple hardware and software issues that preclude the Office of the Texas Secretary of State from determining that the Democracy Suite 5.5-A system satisfies each of the voting-system requirements set forth in the Texas Election Code. Specifically, the examiner reports raise concerns about whether the Democracy Suite 5.5-A system is suitable for its intended purpose; operates efficiently and accurately; and is safe from fraudulent or unauthorized manipulation. Therefore, the Democracy Suite 5.5-A system and corresponding hardware devices do not meet the standards for certification prescribed by Section 122.001 of the Texas Election Code.

CONCLUSION

Accordingly, based upon the foregoing, I hereby deny certification of Dominion Voting Systems' Democracy Suite 5.5-A system for use in Texas elections.

Signed under my hand and seal of office, this 24th day of January, 2020.



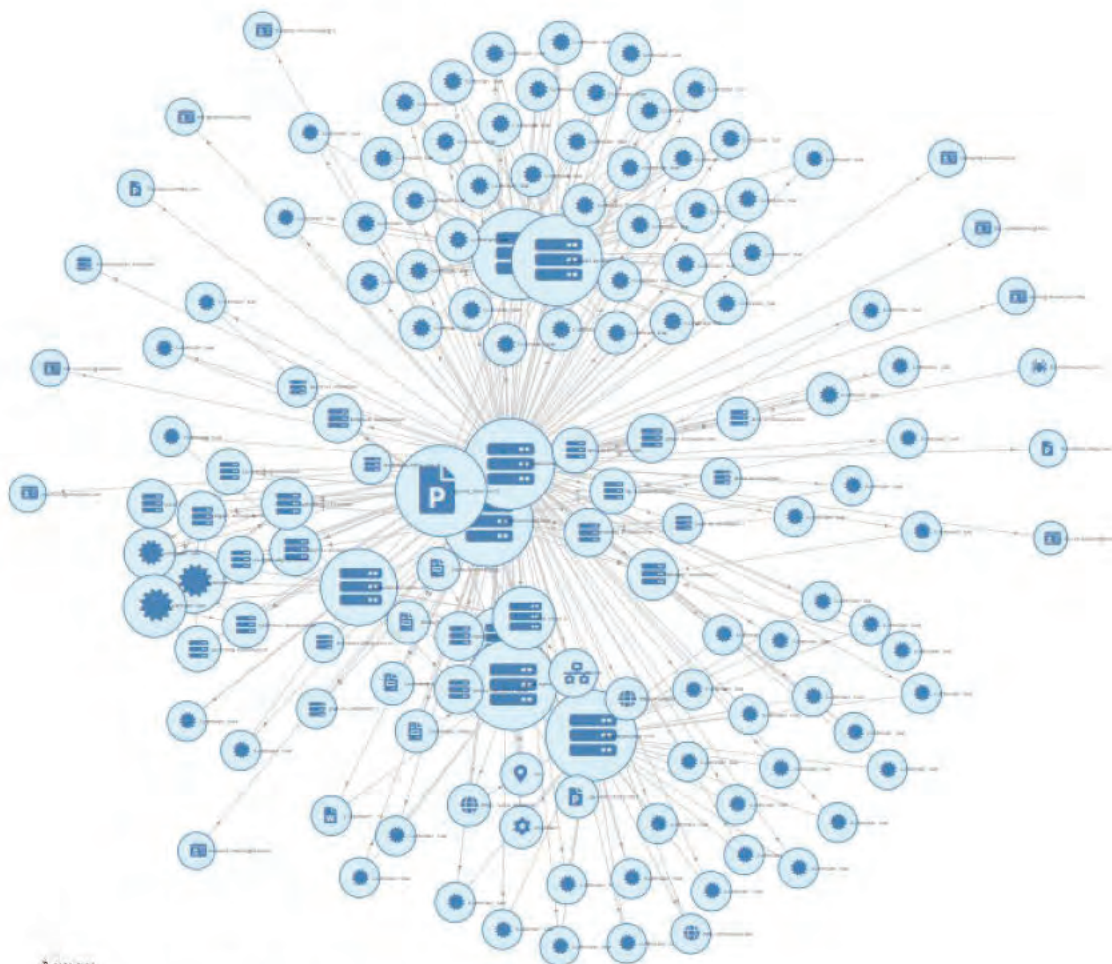
JOSE A. ESPARZA
DEPUTY SECRETARY OF STATE

EXHIBIT 12

Declaration of [REDACTED]

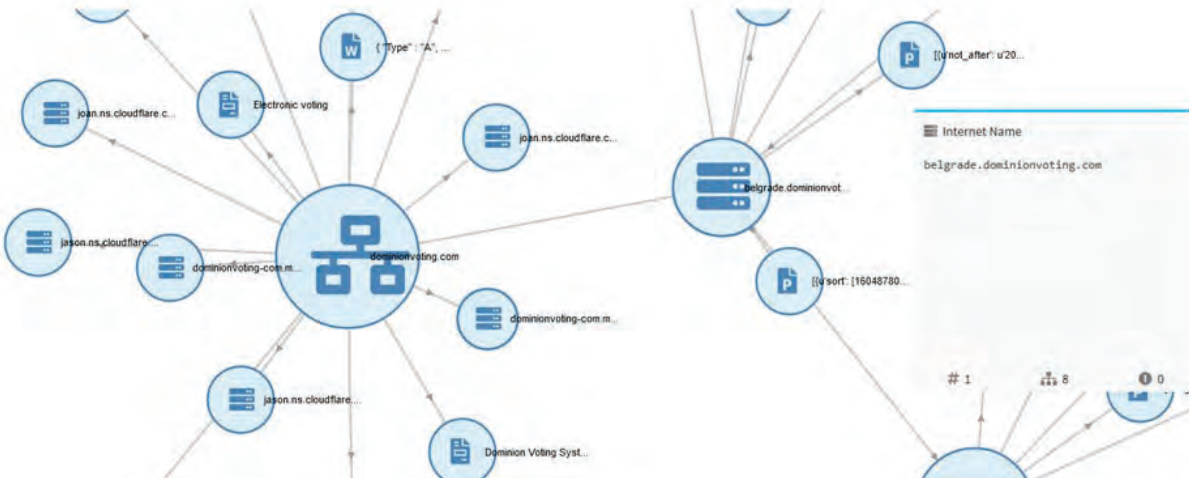
Pursuant to 28 U.S.C Section 1746, [REDACTED] make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I was an electronic intelligence analyst under 305th Military Intelligence with experience gathering SAM missile system electronic intelligence. I have extensive experience as a white hat hacker used by some of the top election specialists in the world. The methodologies I have employed represent industry standard cyber operation toolkits for digital forensics and OSINT, which are commonly used to certify connections between servers, network nodes and other digital properties and probe to network system vulnerabilities.
3. I am a US citizen and I reside [REDACTED] location in the United States of America.
4. Whereas the Dominion and Edison Research systems exist in the internet of things, and whereas this makes the network connections between the Dominion, Edison Research and related network nodes available for scanning,
5. And whereas Edison Research's primary job is to report the tabulation of the count of the ballot information as received from the tabulation software, to provide to Decision HQ for election results,
6. And whereas Spiderfoot and Robtex are industry standard digital forensic tools for evaluation network security and infrastructure, these tools were used to conduct public security scans of the aforementioned Dominion and Edison Research systems,
7. A public network scan of Dominionvoting.com on 2020-11-08 revealed the following inter-relationships and revealed 13 unencrypted passwords for dominion employees, and 75 hashed passwords available in TOR nodes:



```
Array
(
  [id] => 544167324
  [luser] => ian.macvicar
  [domain] => dominionvoting.com
  [password] => jamley
)
7
Array
(
  [id] => 599400504
  [luser] => jelena.tanaskovic
  [domain] => dominionvoting.com
)
```


8. The same public scan also showed a direct connection to the group in Belgrade as highlighted below:



robtex.com/dns-lookup/dominionvoting.com

8 results shown.

IP numbers of the name servers	Subdomains/Hostnames
2400:cb00:2049:1::adf5:3bb3	Domains or hostnames one step under this dom
2606:4700:50::adf5:3aad	barracuda.dominionvoting.com
2803:f800:50::6ca2:c0ad	belgrade.dominionvoting.com
2803:f800:50::6ca2:c1b3	webmail.dominionvoting.com
2a06:98c1:50::ac40:20ad	www.dominionvoting.com
108.162.192.173	4 results shown.
108.162.193.170	

9. A cursory search on LinkedIn of “dominion voting” on 11/19/2020 confirms the numerous employees in Serbia:

The image shows two LinkedIn profiles. The first profile is for Vukašin Đorđević, a 3rd-degree connection, who is a Software Developer at Dominion Voting Systems in Serbia. The second profile is for Edvan Sabanovic, also a 3rd-degree connection, who is a Senior Full-stack Web Developer in Belgrade, Serbia, and a former Senior Web Developer at Dominion Voting Systems.

10. An additional search of Edison Research on 2020-11-08 showed that Edison Research has an Iranian server seen here:



Inputting the Iranian IP into Robtex confirms the direct connection into the “edisonresearch” host from the perspective of the Iranian domain also. This means that it is not possible that the connection was a unidirectional reference.

QUICK INFO

Quick summary of the host name: edisonresearch.xn--mgb3a4fra.ir quick info

General	
FQDN	edisonresearch.xn--mgb3a4fra.ir
Host Name	edisonresearch
Domain Name	xn--mgb3a4fra.ir
Registry	ir
TLD	ir

SHARED

This section shows related hostnames and IP addresses:

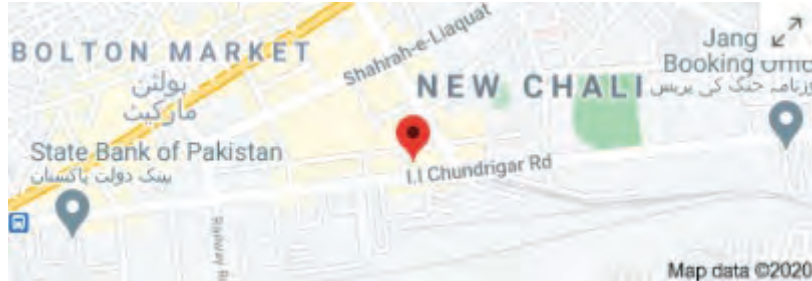
On other TLD:s and domains

This sub section show this name on other top level domains.

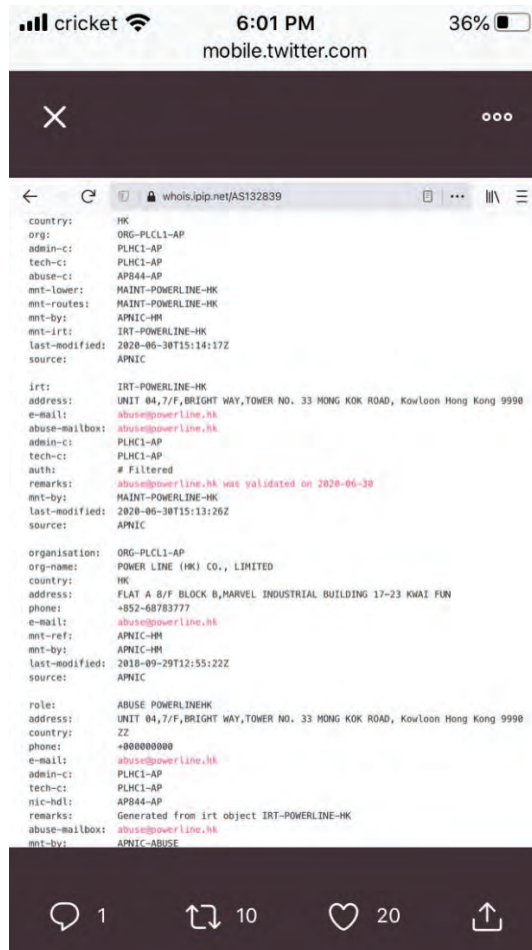
- xn--mgb3a4fra.com
- xn--mgb3a4fra.net
- xn--mgb3a4fra.tk

3 results shows.

A deeper search of the ownership of Edison Research “edisonresearch.com” shows a connection to BMA Capital Management, where shareofear.com and bmacapital.com are both connected to edisonresearch.com via a VPS or Virtual Private Server, as denoted by the “vps” at the start of the internet name:



Dominionvoting is also dominionvotingsystems.com, of which there are also many more examples, including access of the network from China. The records of China accessing the server are reliable.



CHINA UNICOM China169 Backbone - Fraud Risk

Low Risk

← Lowest Risk Highest Risk →

0 Fraud Score: 3 100

We consider **CHINA UNICOM China169 Backbone** to be a potentially low fraud risk ISP, by which we mean that web traffic from this ISP potentially poses a low risk of being fraudulent. Other types of traffic may pose a different risk or no risk. They operate 1,889,865 IP addresses, some of which are running

6 77 126

Domain Name: dominionvotingsystems.com
Registry Domain ID: 2530599738_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2020-05-26T15:48:58Z
Creation Date: 2020-05-26T15:48:57Z
Registrar Registration Expiration Date: 2021-05-26T15:48:57Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>
Domain Status: clientUpdateProhibited <http://www.icann.org/epp#clientUpdateProhibited>
Domain Status: clientRenewProhibited <http://www.icann.org/epp#clientRenewProhibited>
Domain Status: clientDeleteProhibited <http://www.icann.org/epp#clientDeleteProhibited>
Registrant Organization:
Registrant State/Province: Hunan
Registrant Country: CN
Registrant Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com>
Admin Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com>
Tech Email: Select Contact Domain Holder link at <https://www.godaddy.com/whois/results.aspx?domain=dominionvotingsystems.com>
Name Server: NS1.DNS.COM
Name Server: NS2.DNS.COM
DNSSEC: unsigned

Overview - [dominionvotingsystems.com](#)

DNS Records 4

Type	Value	OSH	Security score
A	45.195.162.194 - AS132839 - POWER LINE DATACENTER	2	15
NS	ns1.dns.com 27.152.186.193 - AS133776 - Quanzhou	9	100
	119.167.180.131 - AS4837 - CHINA UNICOM China169 Bac...	8	100
	218.96.111.202 - AS21859 - ZNET	14	100
NS	ns2.dns.com 181.253.57.193 - AS9808 - Guangdong Mobile Communic...	6	100
	121.12.104.65 - AS134763 - CHINANET Guangdong provin...	4	100
SOA	ns1.dns.com Hostname @ dnsadmin.dns.com		

[View all DNS Records](#)

Domains with same A records - [dominionvotingsystems.com](#)

1 Domains with same A records

Domain	Site Title	Alexa rank	DNS A	OSH	DNS CHAME
boanglobal.com	-	-	45.195.162.194 - AS132839 - POWER LINE DATACENTER	2	-

CVE - [dominionvotingsystems.com](#)

22 CVE

ID	Base Score	Severity	Vector	Source	Description
CVE-2018-20845	2.8	LOW	AV:N/A/C/M:N/C:N/P:N	45.195.162.194	In OpenSSH 7.8, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of, or an empty filename. The impact is modifying the permissions of the target directory on the client side.
CVE-2018-6384	6.9	MEDIUM	AV:N/A/C/M:N/C:C/C:A/C	45.195.162.194	Use-after-free vulnerability in the mon_answer_name_free_ctx function in monitor.c in sshd in OpenSSH before 7.8 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.
CVE-2018-1989	7.5	HIGH	AV:N/A/C/M:N/C:P/P:A/P	45.195.162.194	The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.
CVE-2018-18679	6.9	MEDIUM	AV:N/A/C/M:N/C:C/C:A/C	45.195.162.194	sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.
CVE-2018-6451	7.8	HIGH	AV:N/A/C/M:N/C:N/A/C	45.195.162.194	The auth_password function in auth_passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (excess CPU consumption) via a long string.
CVE-2018-5880	8.5	HIGH	AV:N/A/C/M:N/C:P/N/A/C	45.195.162.194	The libdfit_shm_cleanup function in auth-chall.c in sshd in OpenSSH through 8.8 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh-sshInteractiveDevices option, as demonstrated by a modified client that provides a different password for each item element on this list.
CVE-2018-6461	1.9	LOW	AV:N/A/C/M:N/C:P/N/A/P	45.195.162.194	The monitor component in sshd in OpenSSH before 7.8 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PAM_INT request, related to monitor_answer.c and monitor_answer.c.
CVE-2018-13319	5	MEDIUM	AV:N/A/C/M:N/C:P/N/A/N	45.195.162.194	Remotely observable behaviour in auth_gss.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users in a target system when GSSAPI is in use. NOTE: the discover status "is understood" from the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.
CVE-2020-19718	6.8	MEDIUM	AV:N/A/C/M:N/C:P/P:A/P	45.195.162.194	scp in OpenSSH through 8.3p1 allows command injection in the scp.c, tsversion function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument brackets" because that could "stand a great chance of breaking existing workflows."
CVE-2019-4140	4	MEDIUM	AV:N/A/C/M:N/C:P/P:A/P	45.195.162.194	In OpenSSH 7.8, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.
CVE-2016-10911	2.1	LOW	AV:L/A/C/M:N/C:P/N/A/P	45.195.162.194	authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of malloc on buffer contents, which might allow local users to obtain sensitive private key information by leveraging access to a privilege-separated child process.
CVE-2016-13981	7.2	HIGH	AV:N/A/C/M:N/C:C/C:A/C	45.195.162.194	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all consumers, which might allow local users to gain privileges by leveraging access to a conditioned privilege separation process, related to the m_block and m_ptrb data structures.
CVE-2018-5552	4.3	MEDIUM	AV:N/A/C/M:N/C:P/N/A/N	45.195.162.194	The x11_login_helper function in channels.c in ssh in OpenSSH before 6.8, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.
CVE-2018-6805	7.2	HIGH	AV:L/A/C/M:N/C:C/C:A/C	45.195.162.194	The do_setup_env function in session.c in sshd in OpenSSH through 7.3p1, when the local login feature is enabled and PAM is configured to read pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the AuthLogin program, as demonstrated by jail_LD_LIBRARY_PATH environment variable.
CVE-2016-10089	7.6	HIGH	AV:N/A/C/M:N/C:P/P:A/P	45.195.162.194	Untrusted search-path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PRCSHELL modules by leveraging control over a forwarded agent socket.
CVE-2018-20709	5	MEDIUM	AV:N/A/C/M:N/C:P/N/A/P	45.195.162.194	sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to key.c and packet.c.
CVE-2018-6189	4	MEDIUM	AV:N/A/C/M:N/C:P/N/A/P	45.195.162.194	An issue was discovered in OpenSSH 7.8. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_message() in progressmore.c.
CVE-2018-6210	4.3	MEDIUM	AV:N/A/C/M:N/C:P/N/A/N	45.195.162.194	sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.
CVE-2020-14149	4.2	MEDIUM	AV:N/A/C/M:N/C:P/N/A/N	45.195.162.194	The client side in OpenSSH 3.7 through 8.2 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows (in the middle attacker) to target initial connection attempts (before no host key for the server has been cached by the client).
CVE-2014-3113	5.9	MEDIUM	AV:N/A/C/M:N/C:P/P:A/P	45.195.162.194	Multiple CVE-7 function vulnerabilities in sessions.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticate1 and (2) session_x11_req functions.

11. BMA Capital Management is known as a company that provides Iran access to capital markets with direct links publicly discoverable on LinkedIn (found via google on 11/19/2020):

www.linkedin.com · muhammad-talha-a0759660

Muhammad Talha - BMA Capital Management Limited

Manager, Money Market & Fixed Income at **BMA Capital Management Limited**. **BMA Capital ...**

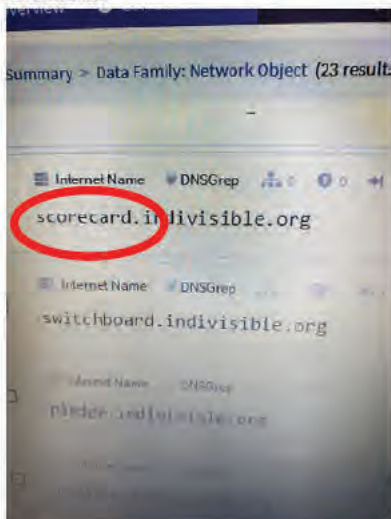
Manager-FMR at Pak Iran Joint Investment Company, Pakistan.

Pakistan · Manager, Money Market & Fixed Income · BMA Capital Management Limited

The same Robtex search confirms the Iranian address is tied to the server in the Netherlands, which correlates to known OSINT of Iranian use of the Netherlands as a remote server (See Advanced Persistent Threats: APT33 and APT34):



12. A search of the indivisible.org network showed a subdomain which evidences the existence of scorecard software in use as part of the Indivisible (formerly ACORN) political group for Obama:



13. Each of the tabulation software companies have their own central reporting “affiliate”. Edison Research is the affiliate for Dominion.

14. Beanfield.com out of Canada shows the connections via co-hosting related sites, including dvscorp.com:

This domain redirects to **beanfield.com**

DNS

View domain name system records, including but not limited to the A, CNAME, MX, and TXT records. View API →

A	96.45.195.194	5 Domains -
MX	10 barracuda.dominionvoting.com.	2 Domains -
NS	ns29.domaincontrol.com.	56,979,357 Domains -
	ns30.domaincontrol.com.	56,979,357 Domains -

Co-Hosted

There are 5 domains hosted on 96.45.195.194 (AS21949 Beanfield Technologies Inc.). [Show All →](#) View API →

guta.ca	ndbgroup.ca	dvscorp.com
aiyokuacardioulounge.com	grantdyer.com	

This Dominion partner domain “dvscopr” also includes an auto discovery feature, where new in-network devices automatically connect to the system. The following diagram shows some of the related dvscopr.com mappings, which mimic the infrastructure for Dominion and are an obvious typo derivation of the name. Typo derivations are commonly purchased to catch redirect traffic and sometimes are used as honeypots. The diagram shows that infrastructure spans multiple different servers as a methodology.

The screenshot shows a network analysis tool interface with the following data:

Data Element	Source Data Element
Similar Domain: TLD Searcher: dvscopr.ايران.ir	Internet Name: SpiderFoot UI: dvscopr.com
Similar Domain: Tool - DNSTwist: dv.scopr.com	Domain Name: SpiderFoot UI: dvscopr.com
Similar Domain: Tool - DNSTwist: dvscorp.com	Domain Name: SpiderFoot UI: dvscopr.com
Similar Domain: TLD Searcher: dvscopr.台湾	Internet Name: SpiderFoot UI: dvscopr.com
Similar Domain: TLD Searcher: dvscopr.fin.ci	Internet Name: SpiderFoot UI: dvscopr.com

<input type="checkbox"/> <p>Domain Name: DSVCORP.COM Registry Domain ID: 134773082_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.bookmyname.com Registrar URL: http://www.bookmyname.com <small>Updated Date: 2020-09-13T10:00:07Z</small></p>	dsvcorp.com
<input type="checkbox"/> <p>Similar Domain - Whois Whois 0 0 2 0 % This is the IRNIC Whois server v1.6.2. % Available on web at http://whois.nic.ir/ % Find the terms and conditions of use on http://www.nic.ir/ % <small>* This domain uses HTTP 302 to the specified for comments and parameters</small></p>	dsvcorp.ایران.ir
<input type="checkbox"/> <p>Similar Domain TLD Searcher 0 0 1 0 dsvcorp.caa.li</p>	dsvcorp.com
<input type="checkbox"/> <p>Similar Domain TLD Searcher 1 0 1 0 dsvcorp.hasura-app.io</p>	dsvcorp.com
<input type="checkbox"/> <p>Similar Domain TLD Searcher 0 0 1 0 dsvcorp.rackmaze.com</p>	dsvcorp.com
<input type="checkbox"/> <p>Similar Domain TLD Searcher 1 0 1 0 dsvcorp.devices.resinstaging.io</p>	dsvcorp.com
<input type="checkbox"/> <p>Similar Domain TLD Searcher 1 0 1 0 dsvcorp.cust.dev.thingdust.io</p>	dsvcorp.com

The above diagram shows how these domains also show the connection to Iran and other places, including the following Chinese domain, highlighted below:

<input type="checkbox"/> <p>Similar Domain TLD Searcher 0 0 1 0 dsvcorp.台湾 Chinese Domain</p>	
<input type="checkbox"/> <p>Similar Domain TLD Searcher 1 0 1 0 dsvcorp.fin.ci</p>	

15. The auto discovery feature allows programmers to access any system while it is connected to the internet once it's a part of the constellation of devices (see original Spiderfoot graph).
16. Dominion Voting Systems Corporation in 2019 sold a number of their patents to China (via HSBC Bank in Canada):

Assignment details for assignee "HSBC BANK CANADA, AS COLLATERAL AGENT"

Assignments (1 total)

Assignment 1

Reel/frame	Execution date	Date recorded	Pages
050500/0236	Sep 25, 2019	Sep 26, 2019	7

Conveyance

SECURITY AGREEMENT

Assignors	Correspondent	Attorney docket
DOMINION VOTING SYSTEMS CORPORATION	CHAPMAN & CUTLER LLP 1270 AVENUE OF THE AMERICAS, 30TH FLOOR ATTN: SOREN SCHWARTZ NEW YORK, NY 10020	

Assignee

HSBC BANK CANADA, AS COLLATERAL AGENT

4TH FLOOR, 70 YORK STREET

TORONTO M5J 1S9

CANADA

Properties (18)

Patent	Publication	Application	PCT	International registration
8844813	20130306724	13476836		
8913787	20130301873	13470091		
9202113	20150071501	14539684		
8195505	20050247783	11121997		
9870666	20120232963	13463536		
9710988	20120259680	13525187		
9870667	20120259681	13525208		
7111782	20040238632	10811969		
7422151	20070012767	11526028		
D599131		29324281		

[View all](#)

This searchable database contains all recorded Patent Assignment information from August 1980 to the present.

When the USPTO receives relevant information for its assignment database, the USPTO puts the information in the public record and does not verify the validity of the information. Recordation is a ministerial function--the USPTO neither makes a determination of the legality of the transaction nor the right of the submitting party to take the action.

Release 2.0.0 | [Release Notes](#) | [Send Feedback](#) | [Legacy Patent Assignment Search](#) | [Legacy Trademark Assignment Search](#)

Of particular interest is a section of the document showing aspects of the nature of the patents dealing with authentication:

Patent assignment 050500/0236

SECURITY AGREEMENT

Date recorded
Sep 26, 2019

Reel/frame
050500/0236

Pages
7

Assignors
DOMINION VOTING SYSTEMS CORPORATION

Execution date
Sep 25, 2019

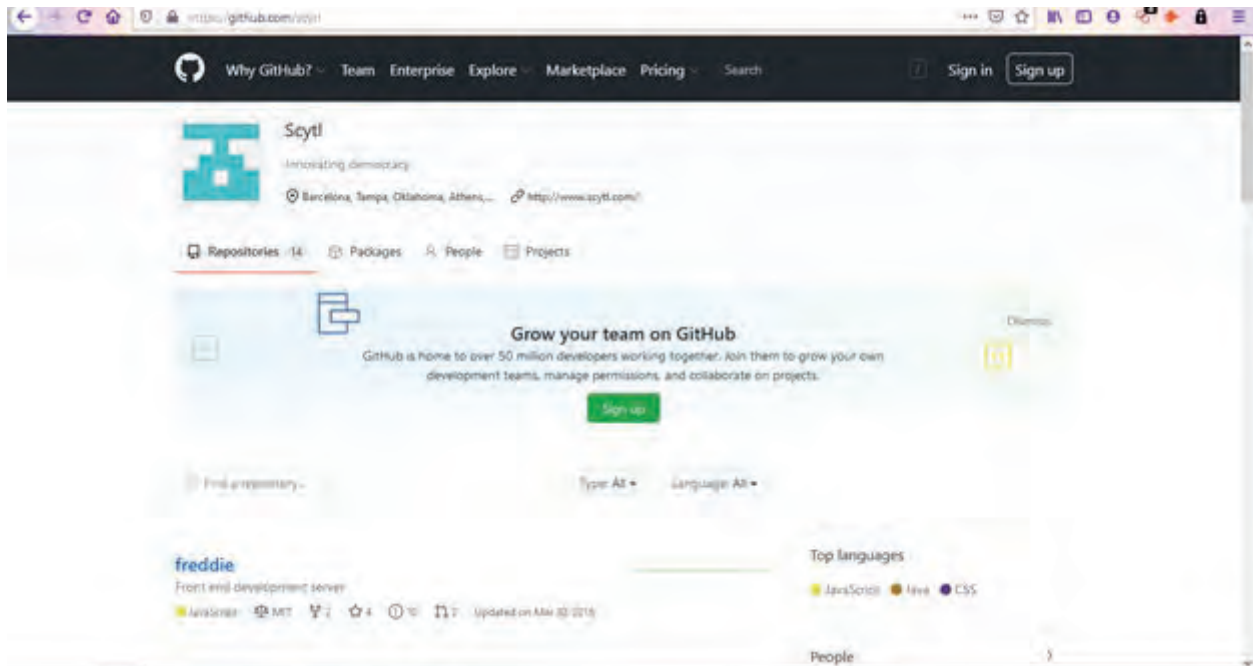
Assignee
HSBC BANK CANADA AS COLLATERAL AGENT
4TH FLOOR, 70 YORK STREET
TORONTO M5J 1S9
CANADA

Correspondent
CHAPMAN & CUTLER LLP
1270 AVENUE OF THE AMERICAS, 30TH FLOOR
ATTN: SOREN SCHWARTZ
NEW YORK, NY 10020

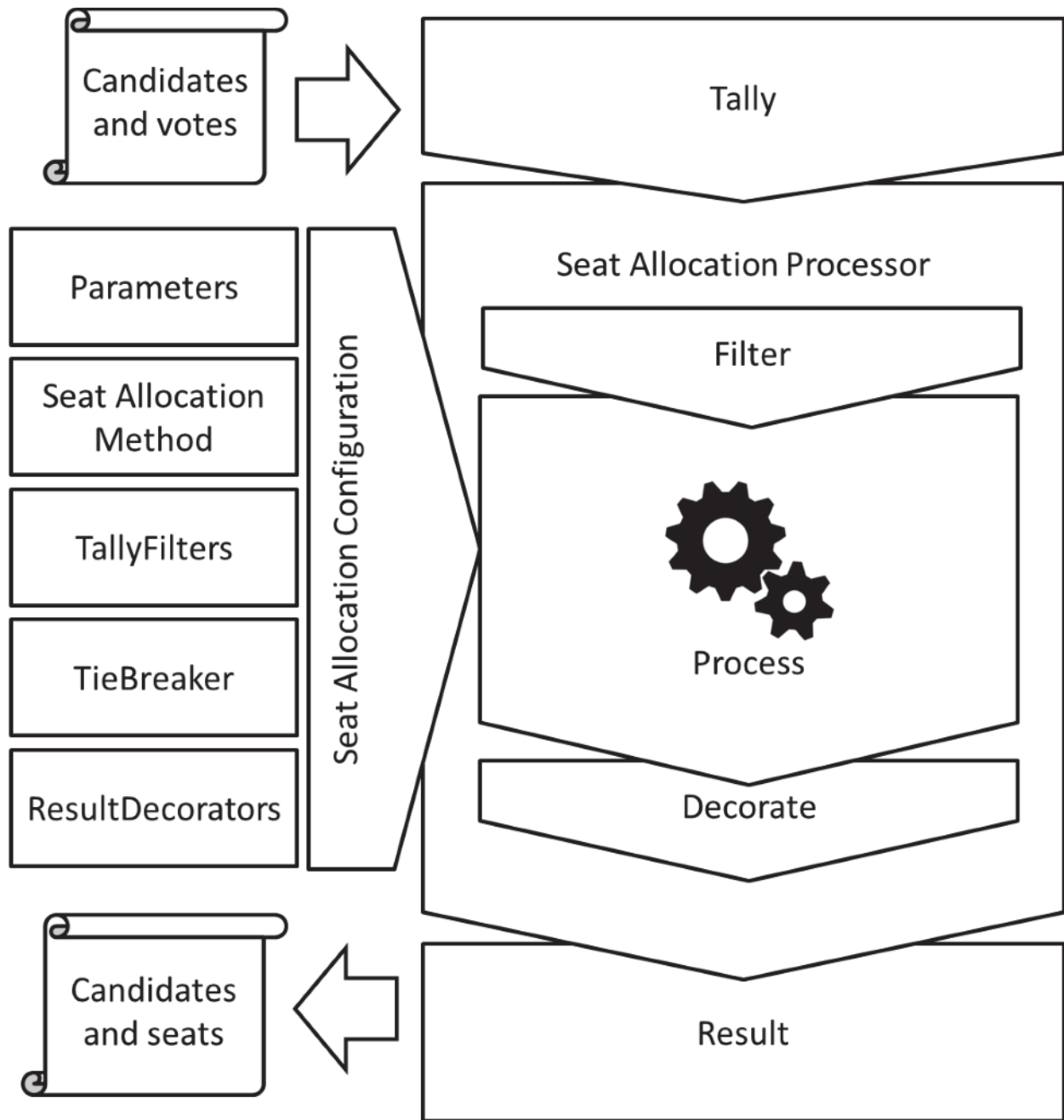
Properties (18 total)

Patent	Publication	Application
1. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7111782 Sep 26, 2006	20040238632 Dec 2, 2004	10811969 Mar 30, 2004
2. SYSTEM, METHOD AND COMPUTER PROGRAM FOR VOTE TABULATION WITH AN ELECTRONIC AUDIT TRAIL Inventors: JOHN DOULOS, JAMES HOOVER, NICK IKONOMAKIS, GORAN OBRADOVIC		
8195505 Jun 5, 2012	20050247783 Nov 10, 2005	11121997 May 5, 2005
3. SYSTEMS AND METHODS FOR PROVIDING SECURITY IN A VOTING MACHINE Inventors: JOHN PAUL HOMEWOOD, THOMAS E. KEELING, PAUL DAVID TERWILLIGER, MARC R. LATOUR		
7422151 Sep 9, 2008	20070012767 Jan 18, 2007	11526028 Sep 25, 2006
4. BALLOT LEVEL SECURITY FEATURES FOR OPTICAL SCAN VOTING MACHINE CAPABLE OF BALLOT IMAGE PROCESSING, SECURE BALLOT PRINTING, AND BALLOT LAYOUT AUTHENTICATION AND VERIFICATION Inventors: ERIC COOMER, LARRY KORB, BRIAN GLENN LIERMAN		

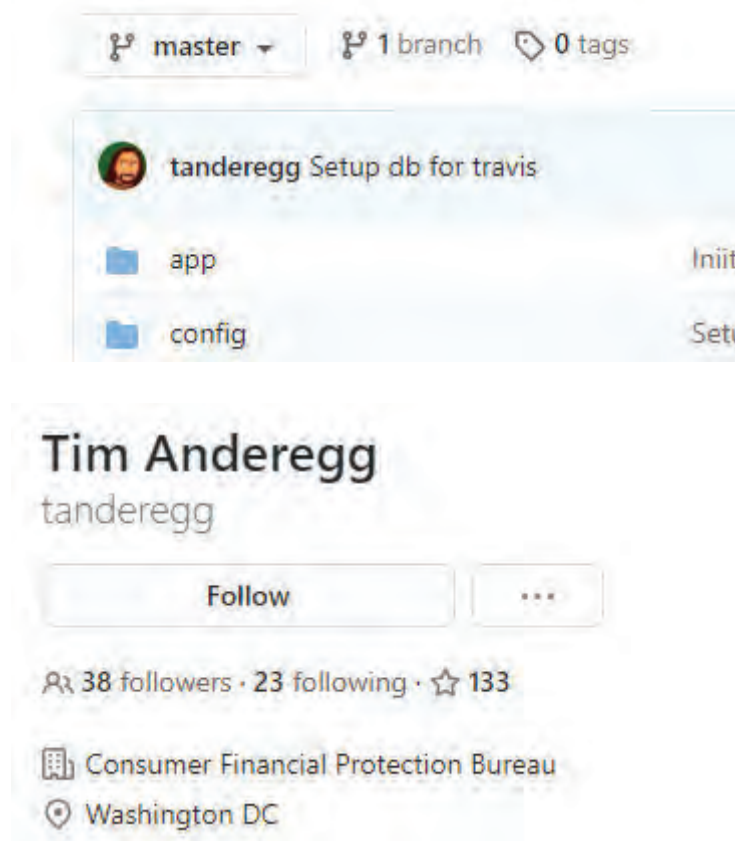
17. Smartmatic creates the backbone (like the cloud). SCYTL is responsible for the security within the election system.



18. In the GitHub account for Scytl, Scytl Jseats has some of the programming necessary to support a much broader set of election types, including a decorator process where the data is smoothed, see the following diagram provided in their source code:



19. Unrelated, but also a point of interest is CTCL or Center for Tech and Civic Life funded by Mark Zuckerberg. Within their github page (<https://github.com/ctcl>), one of the programmers holds a government position. The Bipcoop repo shows tanderegg as one of the developers, and he works at the Consumer Financial Protection Bureau:



20. As seen in included document titled

“AA20-304A-

Iranian_Advanced_Persistent_Threat_Actor_Identified_Obtaining_Voter_Registration_Data” that was authored by the Cybersecurity & Infrastructure Security Agency (CISA) with a Product ID of AA20-304A on a specified date of October 30, 2020, CISA and the FBI reports that Iranian APT teams were seen using ACUTENIX, a website scanning software, to find vulnerabilities within Election company websites, confirmed to be used by the Iranian APT teams buy seized cloud storage that I had personally captured and reported to higher authorities. These scanning behaviors showed that foreign agents of aggressor nations had access to US voter lists, and had done so recently.

21. In my professional opinion, this affidavit presents unambiguous evidence that Dominion Voter Systems and Edison Research have been accessible and were certainly compromised by rogue actors, such as Iran and China. By using servers and employees connected with rogue actors and hostile foreign influences combined with numerous easily discoverable leaked credentials, these organizations neglectfully allowed foreign adversaries to access data

and intentionally provided access to their infrastructure in order to monitor and manipulate elections, including the most recent one in 2020. This represents a complete failure of their duty to provide basic cyber security. This is not a technological issue, but rather a governance and basic security issue: if it is not corrected, future elections in the United States and beyond will not be secure and citizens will not have confidence in the results.

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge. Executed this November 23th, 2020.



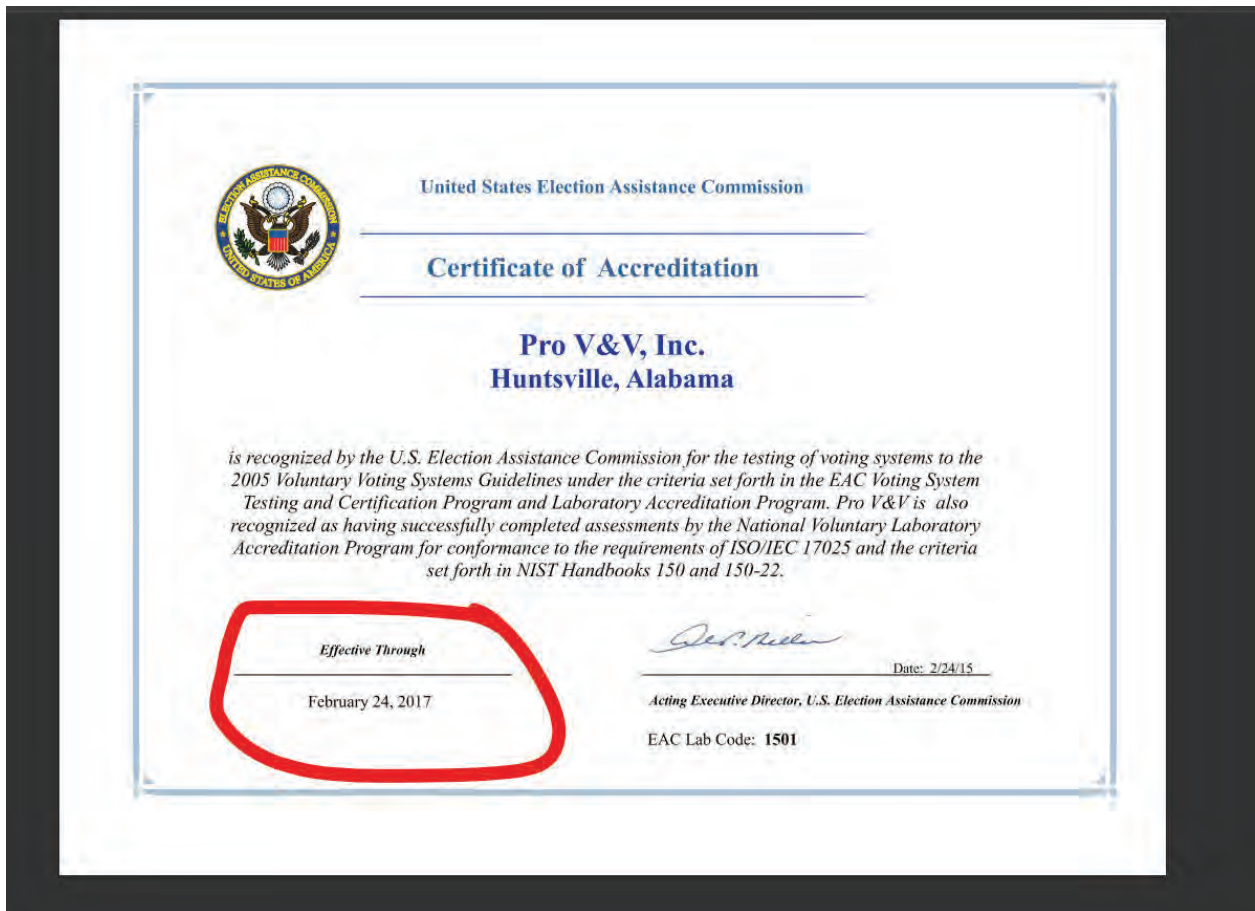
EXHIBIT 13

Declaration of [REDACTED]

Pursuant to 28 U.S.C Section 1746, I, [REDACTED], make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. I have been a private contractor with experience gathering and analyzing foreign intelligence and acted as a LOCALIZER during the deployment of projects and operations both OCONUS and CONUS. I am a trained Cryptolinguist, hold a completed degree in Molecular and Cellular Physiology and have FORMAL training in other sciences such as Computational Linguistics, Game Theory, Algorithmic Aspects of Machine Learning, Predictive Analytics among others.
3. I have operational experience in sources and methods of implementing operations during elections both CONUS and OCONUS
4. I am an amateur network tracer and cryptographer and have over two decades of mathematical modeling and pattern analysis.
5. In my position from 1999-2014 I was responsible for delegating implementation via other contractors sub-contracting with US or 9 EYES agencies identifying connectivity, networking and subcontractors that would manage the micro operations.
6. My information is my personal knowledge and ability to detect relationships between the companies and validate that with the cryptographic knowledge I know and attest to as well as evidence of these relationships.
7. In addition, I am WELL versed due to my assignments during my time as a private contractor of how elections OCONUS (for countries I have had an assignment at) and CONUS (well versed in HAVA ACT) and more.
8. On or about October 2017 I had reached out to the US Senate Majority Leader with an affidavit claiming that our elections in 2017 may be null and void due to lack of EAC certifications. In fact Sen. Wyden sent a letter to Jack Cobb on 31 OCT 2017 advising discreetly pointing out the importance of being CERTIFIED EAC had issued a certificate to

Pro V & V and that expired on Feb 24, 2017. No other certification has been located.



9. Section 231(b) of the Help America Vote Act (HAVA) of 2002 (42 U.S.C. §15371(b)) requires that the EAC provide for the accreditation and revocation of accreditation of independent, non-federal laboratories qualified to test voting systems to Federal standards. Generally, the EAC considers for accreditation those laboratories evaluated and recommended by the National Institute of Standards and Technology (NIST) pursuant to HAVA Section 231(b)(1). However, consistent with HAVA Section 231(b)(2)(B), the Commission may also vote to accredit laboratories outside of those recommended by NIST upon publication of an explanation of the reason for any such accreditation.



10.

11. VSTL's are VERY important because equipment vulnerabilities allow for deployment of algorithms and scripts to intercept, alter and adjust voting tallies.
12. There are only TWO accredited VSTLs (VOTING SYSTEM TEST LABORATORIES). In order to meet its statutory requirements under HAVA §15371(b), the EAC has developed the EAC's Voting System Test Laboratory Accreditation Program. The procedural requirements of the program are established in the proposed information collection, the EAC [Voting System Test Laboratory Accreditation Program Manual](#). Although participation in the program is voluntary, adherence to the program's procedural requirements is mandatory for participants. The procedural requirements of this Manual will supersede any prior laboratory accreditation requirements issued by the EAC. This manual shall be read in conjunction with the EAC's [Voting System Testing and Certification Program Manual](#) (OMB 3265-0019).

U.S. Election Assistance Commission



MICHIGAN

<i>State Participation:</i>	Requires Testing by an Independent Testing Authority. MI requires that voting systems are certified by an independent testing authority accredited by NASED and the board of state canvassers.
<i>Applicable Statute(s):</i>	“An electronic voting system shall not be used in an election unless it is approved by the board of state canvassers ... and unless it meets 1 of the following conditions: (a) Is certified by an independent testing authority accredited by the national association of state election directors and by the board of state canvassers. (b) In the absence of an accredited independent testing authority, is certified by the manufacturer of the voting system as meeting or exceeding the performance and test standards referenced in subdivision (a) in a manner prescribed by the board of state canvassers.” MICH. COMP. LAWS ANN § 168.795a (2009).
<i>Applicable Regulation(s):</i>	MI does not have a regulation regarding the federal certification process.
<i>State Certification Process:</i>	The Secretary of State accepts requests from persons/corporations wishing to have their voting system examined. The requestor must pay the Secretary of State an application fee of \$1,500.00, file a report listing all of the states in which the voting system has been approved and any reports that these states have made regarding the performance of the voting system. The Board of State Canvassers conducts a field test involving Michigan electors and election officials in simulated election day conditions. The Board of State Canvassers shall approve the voting system if it meets all of the state requirements. MICH. COMP. LAWS ANN § 168.795a (2009).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> http://www.michigan.gov/sos/0,1607,7-127-1633_8716_45458--,00.html

U.S. Election Assistance Commission



WISCONSIN

<i>State Participation:</i>	Requires Testing by a Federally Accredited Laboratory. WI requires that its voting systems receive approval from an independent testing authority accredited by NASED verifying that the voting systems meet all of the recommended FEC standards.
<i>Applicable Statute(s):</i>	“No ballot, voting device, automatic tabulating equipment or relating equipment and materials to be used in an electronic voting system may be utilized in this state unless it is approved by the board [of election commissioners].” WIS. STAT. ANN. § 5.91 (West 2009).
<i>Applicable Regulation(s):</i>	“An application for approval of an electronic voting system shall be accompanied by all of the following ... [r]eports from an independent testing authority accredited by the national association of state election directors (NASED) demonstrating that the voting system conforms to all the standards recommended by the federal elections commission.” WIS. ADMIN. CODE GAB § 7.01 (2009).
<i>State Certification Process:</i>	The Board of Election Commissioners accepts applications for the approval of electronic voting systems. Once the application is completed, the vendor must set up the voting system for three mock elections using: (1) offices, (2) referenda questions and (3) candidates. A panel of local election officials can assist the Board in the review of the voting system. The Board conducts the test using a mock election for the partisan primary, general election, and nonpartisan election. The Board may also require that the voting system be used in an actual election as a condition of the approval. WIS. ADMIN. CODE GAB §§ 7.01, 7.02 (2009).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> http://elections.state.wi.us/section.asp?linkid=643&locid=47

U.S. Election Assistance Commission



GEORGIA

State Participation: **Requires Federal Certification.** GA requires that its voting systems are tested to EAC standards by EAC accredited labs and certified by the EAC.

Applicable Statute(s): "Any person or organization owning, manufacturing, or selling, or being interested in the manufacture or sale of, any voting machine may request the Secretary of State to examine the machine. Any ten or more electors of this state may, at any time, request the Secretary of State to reexamine any voting machine previously examined and approved by him or her. Before any such examination or reexamination, the person, persons, or organization requesting such examination or reexamination shall pay to the Secretary of State the reasonable expenses of such examination; provided, however, that in the case of a request by ten or more electors the examination fee shall be \$ 250.00. The Secretary of State may, at any time, in his or her discretion, reexamine any voting machine." [GA CODE ANN. § 21-2-324](#) (2008).

Applicable Regulation(s): "Prior to submitting a voting system for certification by the State of Georgia, the proposed voting system's hardware, firmware, and software must have been issued Qualification Certificates from the EAC. These EAC Qualification Certificates must indicate that the proposed voting system has successfully completed the EAC Qualification testing administered by EAC approved ITAs. If for any reason, this level of testing is not available, the Qualification tests shall be conducted by an agency designated by the Secretary of State. In either event, the Qualification tests shall comply with the specifications of the *Voting Systems Standards* published by the EAC." [GA. COMP. R. & RES. 590-8-1-.01](#) (2009).

State Certification Process: After the voting system has passed EAC Qualification testing, the vendor of the voting system submits a letter to the Office of the Secretary of State requesting certification for the voting system along with a technical data package to the certification agent. An evaluation proposal is created by the certification agent after a preliminary view of the Technical Data Package and sent to the vendor. Any additional EAC ITA testing identified in the evaluation proposal is arranged by the vendor and the certification agent will perform all other tests identified in the evaluation proposal. The certification agent submits a report of their findings to the Secretary of State. Based on these findings the Secretary of State will make a final determination on whether to certify the voting system. [GA. COMP. R. & RES. 590-8-1-.01](#) (2009).

Fielded Voting Systems: *[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].*
<http://www.sos.georgia.gov/Elections/>

U.S. Election Assistance Commission

**PENNSYLVANIA**

<i>State Participation:</i>	Requires Testing by a Federally Accredited Laboratory. PA requires that its voting systems are approved by a federally recognized independent testing laboratory as meeting federal voting system standards.
<i>Applicable Statute(s):</i>	“Any person or corporation owning, manufacturing or selling, or being interested in the manufacture or sale of, any electronic voting system, may request the Secretary of the Commonwealth to examine such system if the voting system has been examined and approved by a federally recognized independent testing authority and if it meets any voting system performance and test standards established by the Federal Government.” <u>25 PA. CONS. STAT. ANN. Code § 3031.5</u> (West 2008).
<i>Applicable Regulation(s):</i>	PA does not have a regulation regarding the federal certification process.
<i>State Certification Process:</i>	The Secretary of State examines voting systems, upon request, once the voting systems have received approval by a federally recognized independent testing authority. The person(s) requesting the examination of the voting system are responsible for the cost of the examination. After the examination, the Secretary of State issues a report stating whether or not the voting systems are safe and compliant with state and federal requirements. If the voting systems are deemed safe and compliant by the Secretary of State then the systems may be adopted and approved for use in elections by each county through a majority vote of its qualified electors. <u>25 PA. CONS. STAT. ANN. Code §§ 3031.5, 3031.2</u> (West 2008).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> http://www.votespa.com/HowtoVote/tabid/74/language/en-US/Default.aspx

U.S. Election Assistance Commission

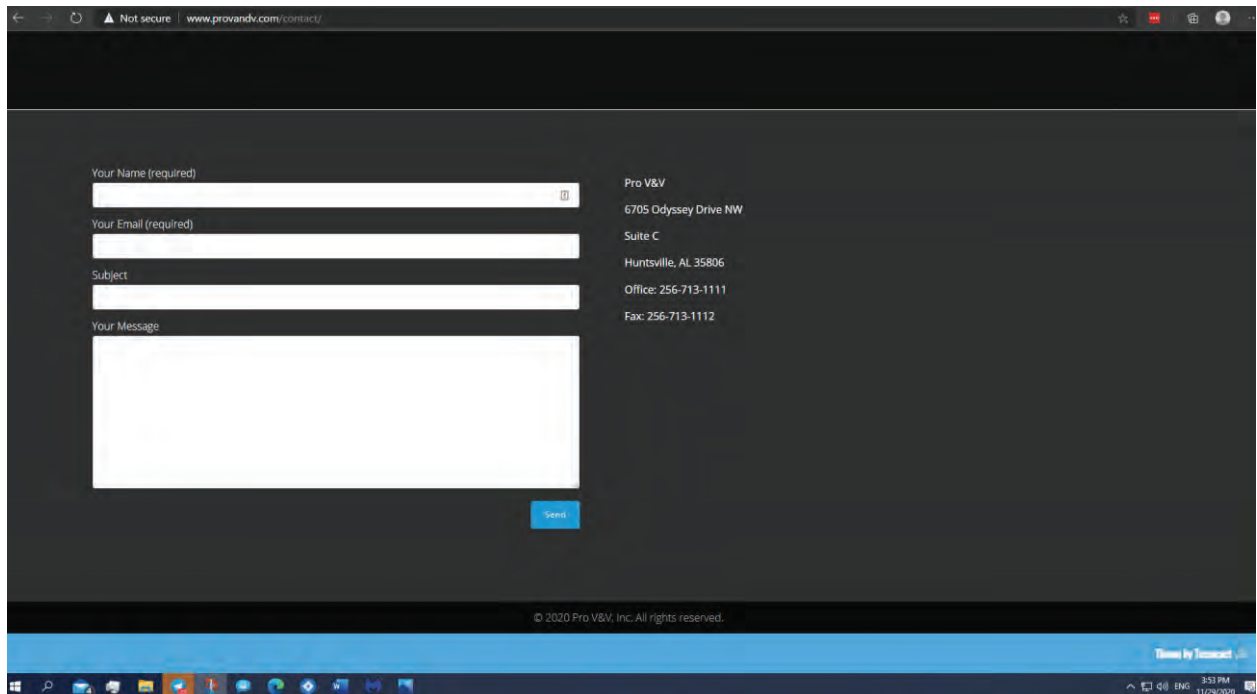
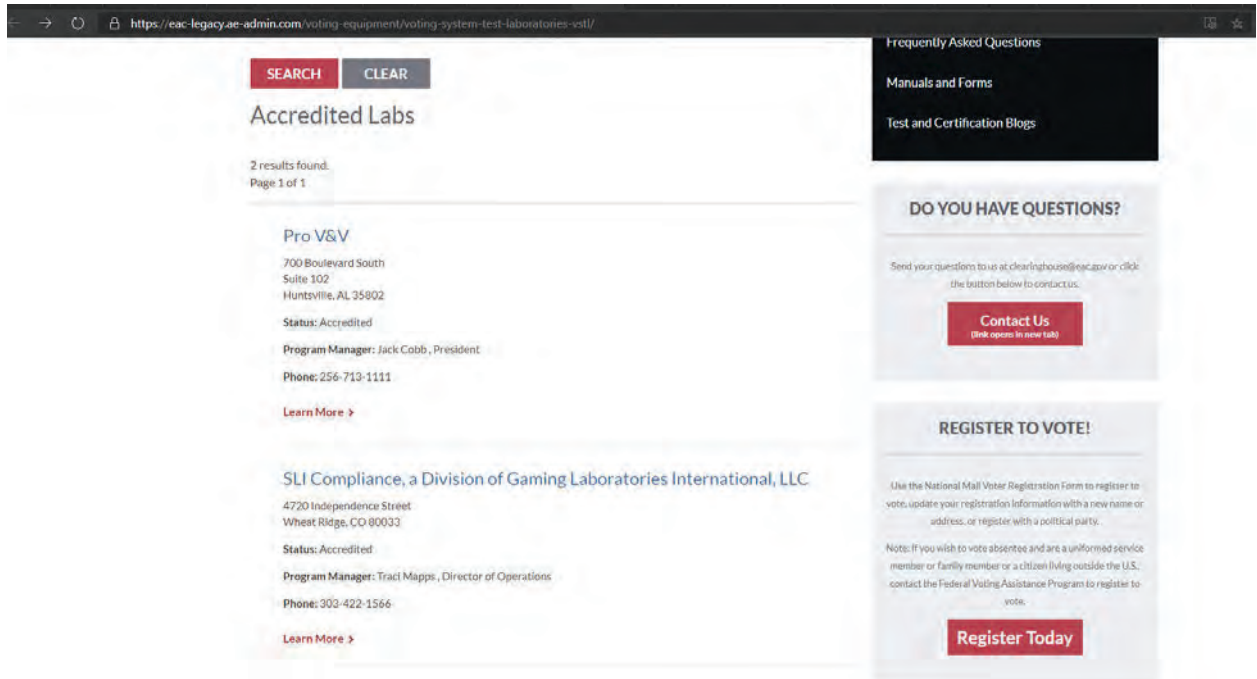


ARIZONA

<i>State Participation:</i>	Requires Testing by a Federally Accredited Laboratory. AZ requires that its voting systems are HAVA compliant and approved by a laboratory that is accredited pursuant to HAVA.
<i>Applicable Statute(s):</i>	"On completion of acquisition of machines or devices that comply with HAVA, machines or devices used at any election for federal, state or county offices may only be certified for use in this state and may only be used in this state if they comply with HAVA and if those machines or devices have been tested and approved by a laboratory that is accredited pursuant to HAVA." ARIZ. REV. STAT. § 16-442(B) (2008).
<i>Applicable Regulation(s):</i>	AZ does not have a regulation regarding the federal certification process.
<i>State Certification Process:</i>	The Secretary of State appoints a committee of three people that test different voting systems. This committee is required to submit their recommendations to the Secretary of State who then makes the final decision on which voting system(s) to adopt. ARIZ. REV. STAT. § 16-442(A) and (C) (2008).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> http://www.azsos.gov/election/equipment/default.htm

- 17.
18. **Pro V& V** and **SLI Gaming** both lack evidence of EAC Accreditation as per the Voting System Testing and Certification Manual.

19. **Pro V& V** is owned and Operated by Jack Cobb. Real name is Ryan Jackson Cobb. The company ProV&V was founded and run by Jack Cobb who formerly worked under the entity of Wyle Laboratories which is an AEROSPACE DEFENSE CONTRACTING ENTITY. The address information on the EAC, NIST and other entities for Pro V& V are different than that of what is on ProV&V website. The [EAC](#) and NIST (ISO CERT) issuers all have another address.



20. VSTLs are the most important component of the election machines as they examine the use of COTS (Commercial Off-The-Shelf)
21. “Wyle became involved with the testing of electronic voting systems in the early 1990’s and has tested over 150 separate voting systems. Wyle was the first company to obtain accreditation by the National Association of State Election Directors (NASSED). Wyle is accredited by the Election Assistance Commission (EAC) as a Voting System Testing Laboratory (VSTL). Our scope of accreditation as a VSTL encompasses all aspects of the hardware and software of a voting machine. Wyle also received NVLAP accreditation to ISO/IEC 17025:2005 from NIST.” [Testimony](#) of Jack Cobb 2009
22. COTS are preferred by many because they have been tried and tested in the open market and are most economic and readily available. COTS are also the SOURCE of vulnerability therefore VSTLs are VERY important. COTS components by voting system machine manufacturers can be used as a “Black Box” and changes to their specs and hardware make up change continuously. Some changes can be simple upgrades to make them more efficient in operation, cost efficient for production, end of life (EOL) and even complete reworks to meet new standards. The key issue in this is that MOST of the COTS used by Election Machine Vendors like Dominion, ES&S, Hart Intercivic, Smartmatic and others is that such manufacturing for COTS have been outsourced to China which if implemented in our Election Machines make us vulnerable to BLACK BOX antics and backdoors due to hardware changes that can go undetected. This is why VSTL’s are VERY important.
23. The proprietary voting system software is done so and created with cost efficiency in mind and therefore relies on 3rd party software that is AVAILABLE and HOUSED on the HARDWARE. This is a vulnerability. Exporting system reporting using software like Crystal Reports, or PDF software allows for vulnerabilities with their constant updates.
24. As per the COTS hardware components that are fixed, and origin may be cloaked under proprietary information a major vulnerability exists since once again third-party support software is dynamic and requires FREQUENT updates. The hardware components of the computer components, and election machines that are COTS may have slight updates that can be overlooked as they may be like those designed that support the other third -party software. COTS origin is important and the US Intelligence Community report in 2018 verifies that.
25. The Trump Administration made it clear that there is an absence of a major U.S. alternative to foreign suppliers of networking equipment. This highlights the growing dominance of

Chinese manufacturers like Huawei that are the world's LARGEST supplier of telecom and other equipment that endangers national security.

26. China, is not the only nation involved in COTS provided to election machines or the networking but so is Germany via a LAOS founded Chinese linked cloud service company that works with SCYTL named Akamai Technologies that have offices in China and are linked to the server that Dominion Software.

28 046 Madrid

Asian offices

Akamai Technologies - India

111, Brigade Court
Koramangala Industrial Area
Bangalore 560 095, India

Telephone: 91-80-575-99222
Fax: 91-80-575-99209
Regional Manager: Stuart Spiteri

Akamai Technologies - China

Suite 1560, 15th Floor
NCI Tower
12A Jianguomenwai Avenue
Chaoyang District,
Beijing 100022
China

Telephone: 86-10-8523-3097
Fax: 86-10-8523-3001
Regional Manager: Stuart Spiteri

Akamai Japan K.K.

The Executive Centre Japan K.K.
15F Tokyo Ginko Kyokai building
1-3-1 Marunouchi, Chiyoda-ku, Tokyo 100-0005

Telephone: 81-3-3216-7200 (Centre)
81-3-3216-7300 (Akamai direct)
Fax: 81-3-3216-7390 (Centre)
Regional Manager: Stuart Spiteri

Akamai Technologies - Singapore

Akamai, Regus Centre, 36-01 UOB Plaza 1
80 Raffles Place
Singapore 048624
[Driving directions](#)

Telephone: +65 6248 4614
Fax: +65 6248-4501
Regional Manager: Stuart Spiteri

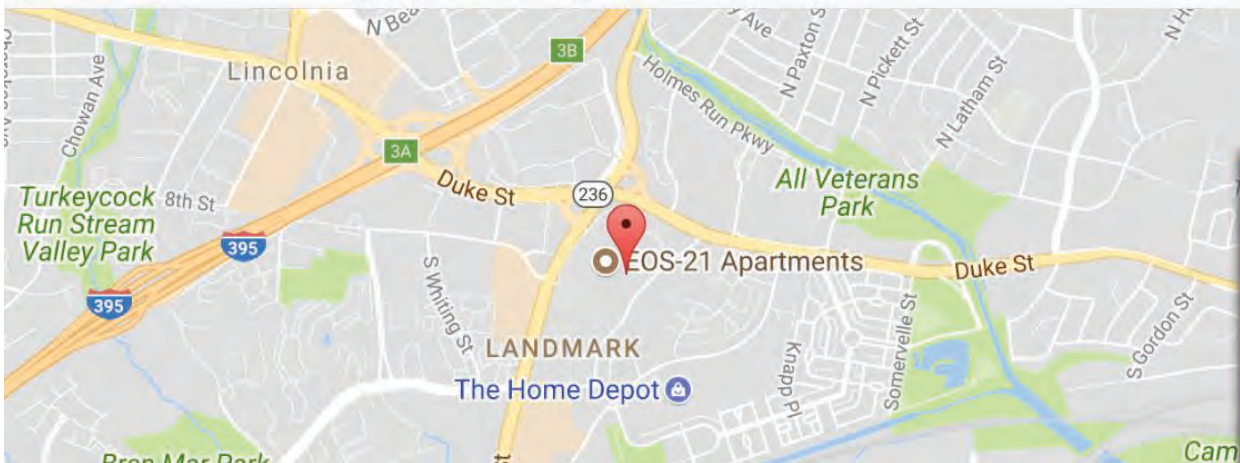
Akamai Technologies - Australia and New Zealand

201 Sussex St
Tower 2, Level 20
Sydney, NSW 2000, Australia
info@au.akamai.com

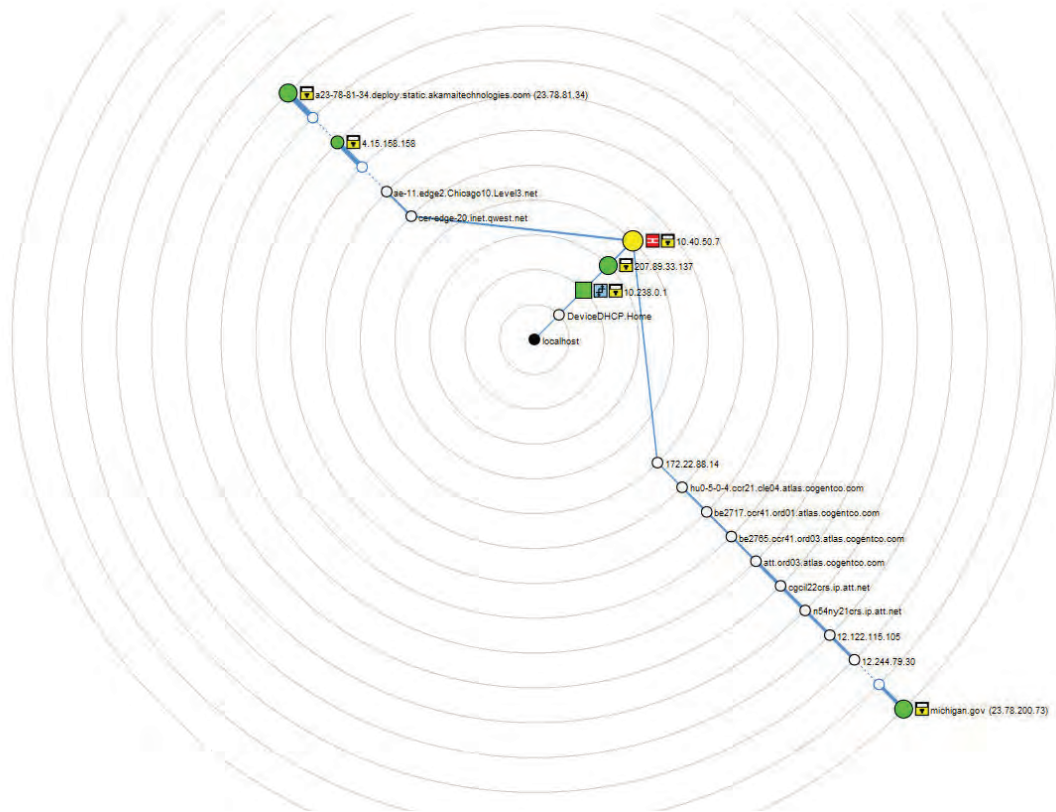
Telephone: 61 2 9006 1325
Fax: 61 2 9475 0343
Regional Manager: Stuart Spiteri

ptt.gov resolves to 4.30.228.74. According to our data this IP address belongs to Level 3 Communications and is located in Alexandria, Virginia, United States. Please have a look at the information provided below for further details.

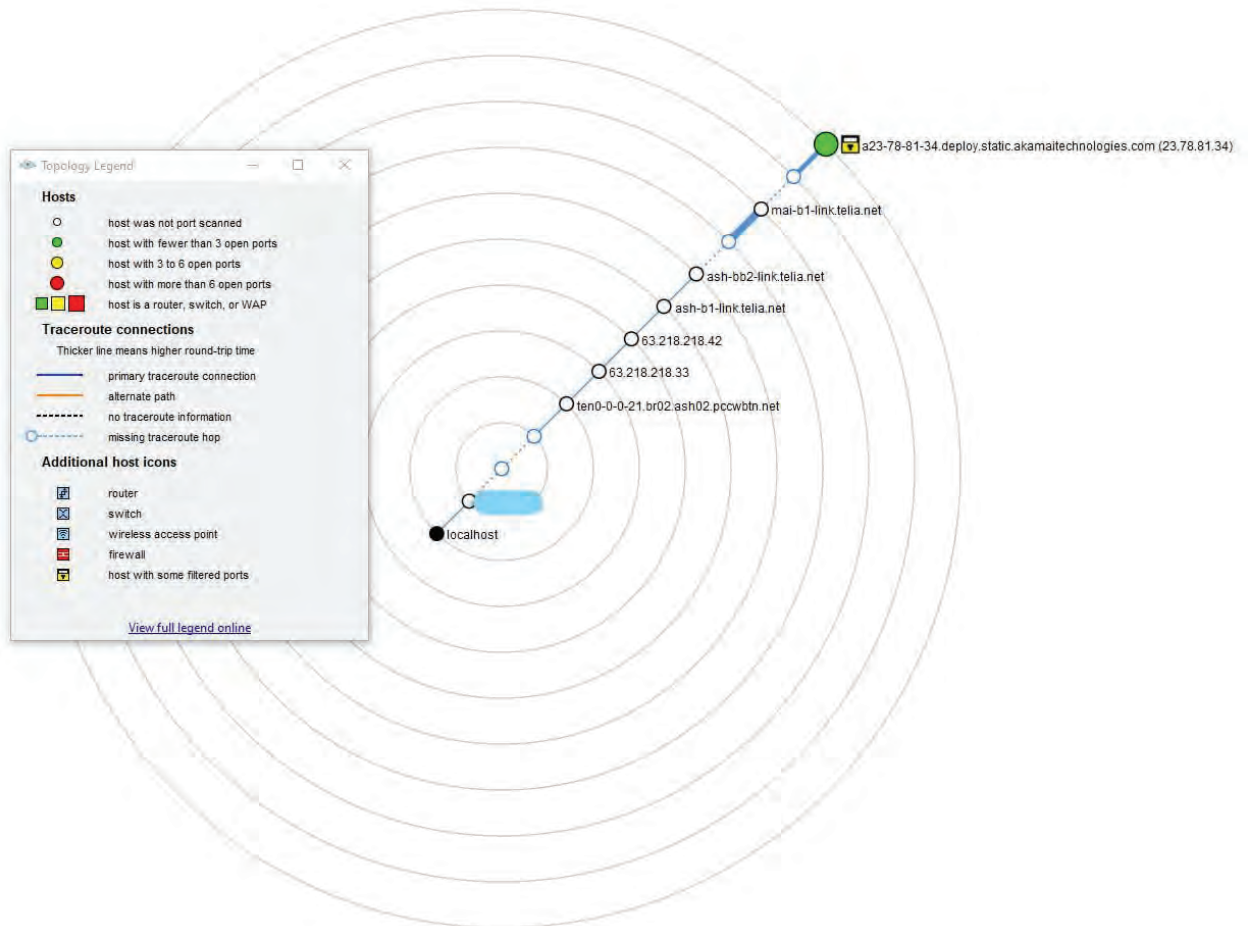
🇺🇸 4.30.228.74	
ISP/Organization	Level 3 Communications
Location	Alexandria 22304, Virginia (VA), 🇺🇸 United States (US)
Latitude	38.8115 / 38°48'41" N
Longitude	-77.1285 / 77°7'42" W
Timezone	America/New_York
Local Time	Thu, 12 Jul 2018 19:27:40 -0400



- 27.
28. L3 Level Communications is federal contractor that is partially owned by foreign lobbyist George Soros. An article that AP ran in 2010 – spoke out about the controversy of this that has been removed. ([LINK](#)) “As for the company’s other political connections, it also appears that none other than George Soros, the billionaire funder of the country’s liberal political infrastructure, owns 11,300 shares of OSI Systems Inc., the company that owns Rapiscan. Not surprisingly, OSI’s stock has appreciated considerably over the course of the year. Soros certainly is a savvy investor.” Washington Examiner re-write.



29.



30.

31. **L-3 Communication Systems-East** designs, develops, produces and integrates communication systems and support equipment for space, air, ground, and naval applications, including C4I systems and products; integrated Navy communication systems; integrated space communications and RF payloads; recording systems; secure communications, and information security systems. In addition, their site claims that MARCOM is an integrated communications system and The Marcom® is the foundation of the Navy's newest digital integrated voice / data switching system for affordable command and control equipment supporting communications and radio room automation. The MarCom® uses the latest **COTS** digital technology and open systems standards to offer the command and control user a low cost, user friendly, solution to the complex voice, video and data communications needs of present and future joint / allied missions. Built in reliability, rugged construction, and fail-safe circuits ensure your call and messages will go through. Evidently a HUGE vulnerability.

- 32. Michigan’s government site is thumped off Akamai Technologies servers which are housed on **TELIA AB** a foreign server located in Germany.
- 33. Scytl, who is contracted with AP that receives the results tallied BY Scytl on behalf of Dominion – During the elections the AP reporting site had a disclaimer.
AP – powered by SCYTL.

Advertisements	Basic Tracking Info
	<p>Domain: Michigan.gov [Whois Lookup - Domain Country - Domain To IP]</p> <p>IP Address: 23.78.81.34 IP Blacklist Check</p> <p>Reverse DNS: 34.81.78.23.in-addr.arpa</p> <p>Hostname: a23-78-81-34.deploy.static.akamaitechnologies.com</p> <p>a12-67.akam.net >> 184.26.160.67 a11-66.akam.net >> 84.53.139.66 a1-35.akam.net >> 193.108.91.35</p> <p>Nameservers: a5-66.akam.net >> 95.100.168.66 a18-64.akam.net >> 95.101.36.64 a24-65.akam.net >> 2.16.130.65</p>
	Location For an IP: Michigan.gov
	<p>Continent: North America (NA)</p> <p>Country: United States (US)</p> <p>Capital: Washington</p> <p>State: Unknown</p> <p>City: Unknown</p> <p>Location: Unknown</p> <p>ISP: Akamai Technologies</p> <p>Organization: Akamai Technologies</p> <p>AS Number: AS1299 Telia Company AB</p> <p>something went wrong! something went wrong!</p>
	Geolocation on IP Map
	<p>Time Zone: America/North_Dakota/Center</p> <p>Local Time: 13:48:46</p> <p>Timezone: -21600</p> <p>GMT offset: -21600</p> <p>Sunrise / Sunset: 07:27 / 17:12</p>
	Extra Information for an IP: Michigan.gov
	<p>Continent Lat/Lon: 46.07305 / -100.546</p> <p>Country Lat/Lon: 38 / -98</p> <p>City Lat/Lon: (37.751) / (-97.822)</p> <p>IP Language: English</p>

34. “Scytl was selected by the Federal Voting Assistance Program of the U.S. Department of Defense to provide a secure online ballot delivery and onscreen marking systems under a program to support overseas military and civilian voters for the 2010 election cycle and beyond. Scytl was awarded 9 of the 20 States that agreed to participate in the program (New York, Washington, Missouri, Nebraska, Kansas, New Mexico, South Carolina, Mississippi and Indiana), making it the provider with the highest number of participating States.” [PDF](#)
35. According to DOMINION : 1.4.1 Software and Firmware The software and firmware employed by Dominion D-Suite 5.5-A consists of 2 types, custom and commercial off the shelf (COTS). COTS applications were verified to be pristine or were subjected to source code review for analysis of any modifications and verification of meeting the pertinent standards.
36. The concern is the HARDWARE and the NON – ACCREDITED VSTLs as by their own admittance use COTS.
37. The purpose of VSTL’s being accredited and their importance in ensuring that there is no foreign interference/ bad actors accessing the tally data via backdoors in equipment software. The core software used by ALL SCYTL related Election Machine/Software manufacturers ensures “anonymity” .
38. Algorithms within the area of this “shuffling” to maintain anonymity allows for setting values to achieve a desired goal under the guise of “encryption” in the trap-door.
39. The actual use of trapdoor commitments in Bayer-Groth proofs demonstrate the implications for the verifiability factor. This means that no one can SEE what is going on during the process of the “shuffling” therefore even if you deploy an algorithms or manual scripts to fractionalize or distribute pooled votes to achieve the outcome you wish – you cannot prove they are doing it! See STUDY : [“The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system”](#)
40. **Key Terms**
41. **UNIVERSAL VERIFIABILITY:** Votes cast are the votes counted and integrity of the vote is verifiable (the vote was tallied for the candidate selected) . **SCYTL FAILS UNIVERSAL VERIFIABILITY** because no mathematical proofs can determine if any votes have been manipulated.
42. **INDIVIDUAL VERIFIABILITY:** Voter cannot verify if their ballot got correctly counted. Like, if they cast a vote for ABC they want to verify it was ABC. That notion clearly discounts the need for anonymity in the first place.

43. To understand what I observed during the 2020 I will walk you through the process of one ballot cast by a voter.
44. STEP 1 |Config Data | All non e-voting data is sent to Scytl (offshore) for configuration of data. All e-voting is sent to CONFIGURATION OF DATA then back to the e-voting machine and then to the next phase called CLEANSING. **CONCERNS:** Here we see an “OR PROOF” as coined by mathematicians – an “or proof” is that votes that have been pre-tallied parked in the system and the algorithm then goes back to set the outcome it is set for and seeks to make adjustments if there is a partial pivot present causing it to fail demanding manual changes such as block allocation and narrowing of parameters or self-adjusts to ensure the predetermined outcome is achieved.
45. STEP 2|CLEANSING | The Process is when all the votes come in from the software run by Dominion and get “cleansed” and put into 2 categories: invalid votes and valid votes.
46. STEP 3|Shuffling /Mixing | This step is the most nefarious and exactly where the issues arise and carry over into the decryption phase. Simply put, the software takes all the votes, literally mixes them a and then re-encrypts them. This is where if ONE had the commitment key- TRAPDOOR KEY – one would be able to see the parameters of the algorithm deployed as the votes go into this mixing phase, and how algorithm redistributes the votes.
47. This published PAPER FROM University College London depicts how this shuffle works. In essence, when this mixing/shuffling occurs, then one doesn’t have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes when mixed.

48.

Background - ElGamal encryption

- Setup: Group \mathcal{G} of prime order q with generator g
- Public key: $pk = y = g^x$
- Encryption: $\mathcal{E}_{pk}(m; r) = (g^r, y^r m)$
- Decryption: $\mathcal{D}_x(u, v) = vu^{-x}$
- Homomorphic:

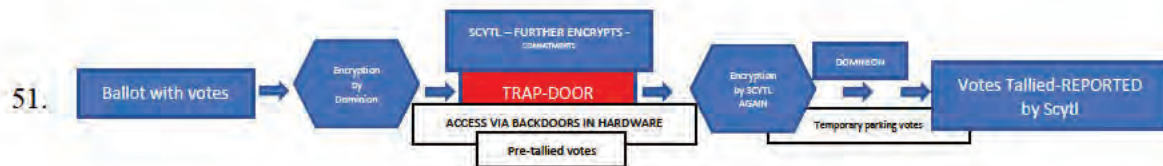
$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(M; R) = \mathcal{E}_{pk}(mM; r + R)$$

- Re-encryption:

$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(1; R) = \mathcal{E}_{pk}(m; r + R)$$



49. When this mixing/shuffling occurs, then one doesn't have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes.
50. When the votes are sent to ScytI via Dominion Software EMS (Election Management System) the Trap Door is accessed by ScytI or TRAP DOOR keys (Commitment Parameters).



52. The encrypted data is shifted into ScytI's platform in the form of ciphertexts – this means it is encrypted and a key based on commitments is needed to read the data. The ballot data can only be read if the person has a key that is set on commitments.
53. A false sense of security is provided to both parties that votes are not being “REPLACED” during the mixing phase. Basically, ScytI re-encrypts the ballot data that comes in from Dominion (or any other voting software company) as ciphertexts. ScytI is supposed to prove that votes A, B, C are indeed X, Y, Z under their new re-encryption when sending back the votes that are tallied coding them respectively. This is done by ScytI and the Election Software company that agrees to certain

“Generators” and therefore together build “commitments.”

```
public CommitmentParams(final ZpSubgroup group, final int n) {
    group = group;
    h = GroupTools.getRandomElement(group);
    commitmentlength = n;
    g = GroupTools.getVectorRandomElement(group,
    this.commitmentlength);
}

// from getRandomElement(group)
Exponent randomExponent = ExponentTools.getRandomExponent(group.getQ());
return group.getGenerator().exponentiate(randomExponent);
```

54. Scytl and Dominion have an agreement – only the two would know the parameters. This means that access is able to occur through backdoors in hardware if the parameters of the commitments are known in order to alter the range of the algorithm deployed to satisfy the outcome sought in the case of algorithm failure.
55. Trapdoor is a cryptotech term that describes a state of a program that knows the commitment parameters and therefore is able change the value of the commitments however it likes. In other words, Scytl or anyone that knows the commitment parameters can take all the votes and give them to any one they want. If they have a total of 1000 votes an algorithm can distribute them among all races as it deems necessary to achieve the goals it wants. (Case Study: Estonia)

Commitment_{CRYPT} = CM_C

Scytl sets commitment-simple math ↓

$$CM_C(\vec{a}; r) = H \prod_i^n G_i^{a_i} = 1 \cdot G_i^{a_i}$$

$$CM_C(\vec{a}; r) = H \left[r + \sum_{i=1}^n (a_i - z_i) e_i \right] \prod_{i=1}^n H^{z_i e_i}$$

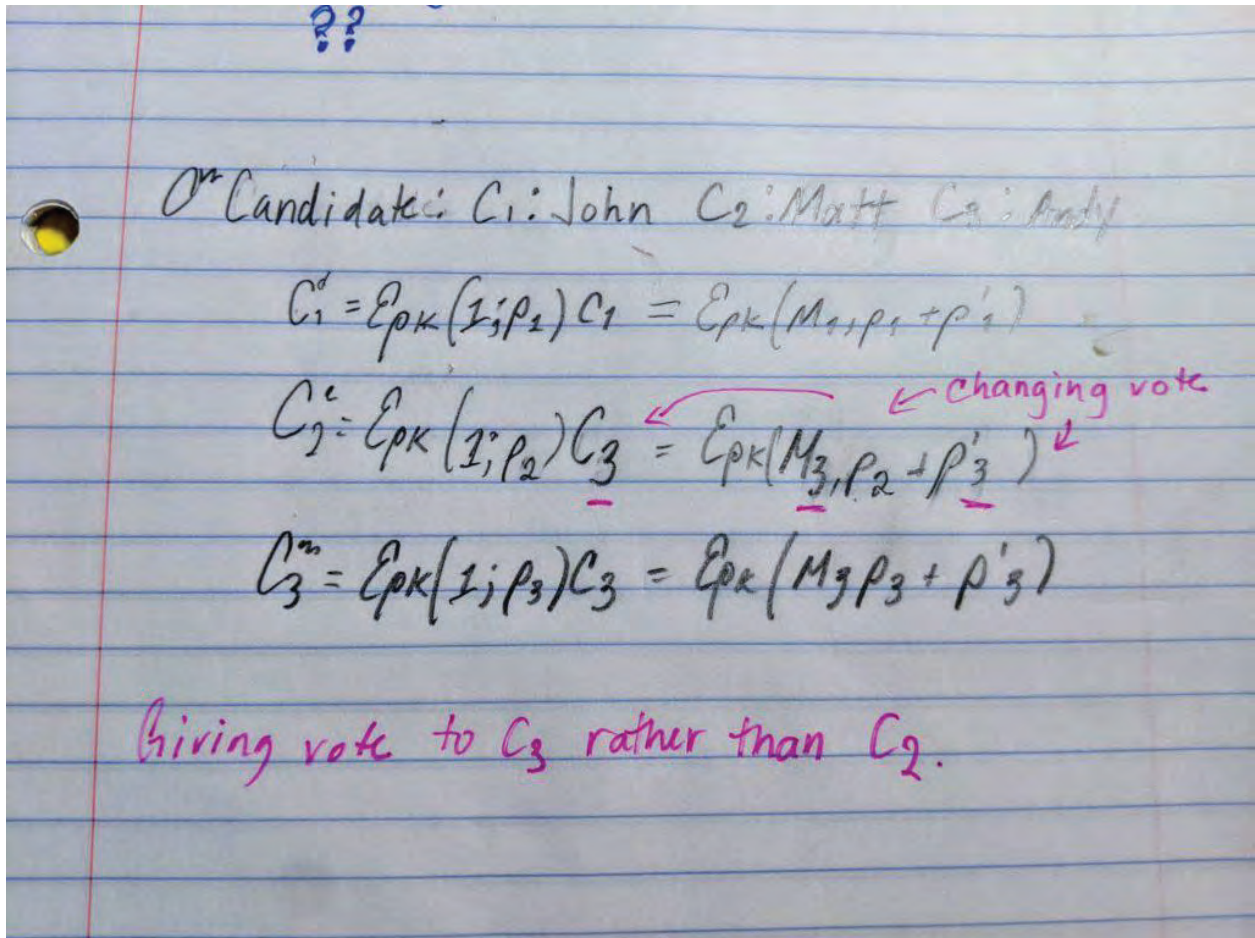
$$CM_C(\vec{a}; r) = CM_C(\vec{z}; r')$$

$$r' = r + \sum_{i=1}^n e_i (a_i - z_i).$$

56.

57. Within the trapdoor this is how the algorithm behaves to move the goal posts in elections without being detected by this proof . During the mixing phase this is the algorithm you would use to

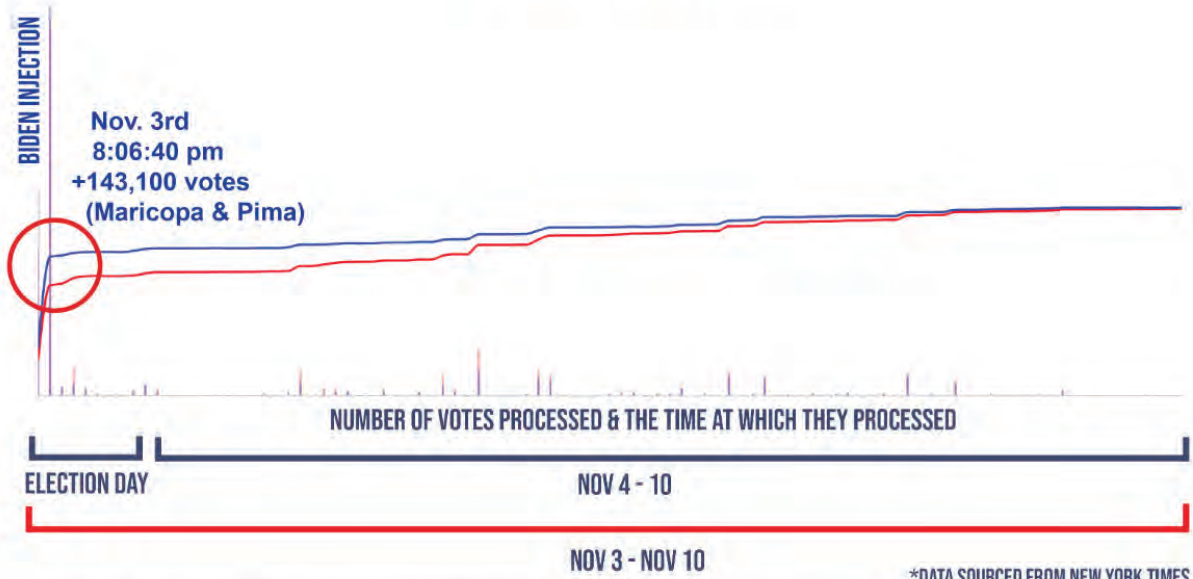
“reallocate” votes via an algorithm to achieve the goal set.



58. STEP 4|Decryption would be the decryption phase and temporary parking of vote tallies before reporting. In this final phase before public release the tallies are released from encrypted format into plain text. As previously explained, those that know the trapdoor can easily change any votes that the randomness is applied and used to generate the tally vote ciphertext. Thus in this case, Scytl who is the mixer can collude with their vote company clients or an agency (-----) to change votes and get away with it. This is because the receiver doesn't have the decryption key so they rely solely on Scytl to be *honest* or free from any foreign actors within their backdoor or the Election Company (like Dominion) that can have access to the key.
59. In fact, a study from the University of Bristol made claim that interference can be seen when there is a GREAT DELAY in reporting and finalizing numbers University of Bristol : [How not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios](#)
60. “Zero-knowledge proofs of knowledge allow a prover to convince a verifier that she holds information satisfying some desirable properties without revealing anything else.” David Bernhard, Olivier Pereira, and Bogdan Warinschi.

61. Hence, you can't prove anyone manipulated anything. The TRAP DOOR KEY HOLDERS can offer you enough to verify to you what you need to see without revealing anything and once again indicating the inability to detect manipulation. **ZERO PROOF of INTEGRITY OF THE VOTE.**
62. Therefore, if decryption is challenged, the administrator or software company that knows the trap door key can provide you proof that would be able to pass verification (blind). This was proven to be factually true in the case study by The University of Melbourne in March. White Hat Hackers purposely altered votes by knowing the parameters set in the commitments and there was no way to prove they did it – or any way to prove they didn't.
63. IT'S THE PERFECT THREE CARD MONTY. That's just how perfect it is. They fake a proof of ciphertexts with KNOWN "RANDOMNESS". This rolls back to the integrity of the VOTE. The vote is not safe using these machines not only because of the method used for ballot "cleansing" to maintain anonymity but the EXPOSURE to foreign interference and possible domestic bad actors.
64. In many circumstances, manipulation of the algorithm is NOT possible in an undetectable fashion. This is because it is one point heavy. Observing the elections in 2020 confirm the deployment of an algorithm due to the BEHAVIOR which is indicative of an algorithm in play that had no pivoting parameters applied.
65. The behavior of the algorithm is that one point (B) is the greatest point within the allocated set. It is the greatest number within the A B points given. Point A would be the smallest. Any points outside the A B points are not necessarily factored in yet can still be applied.
66. The points outside the parameters can be utilized to a certain degree such as in block allocation.
67. The algorithm geographically changed the parameters of the algorithm to force blue votes and ostracize red.
68. Post block allocation of votes the two points of the algorithm were narrowed ensuring a BIDEN win hence the observation of NO Trump Votes and some BIDEN votes for a period of time.

ARIZONA "FIXING" THE VOTE

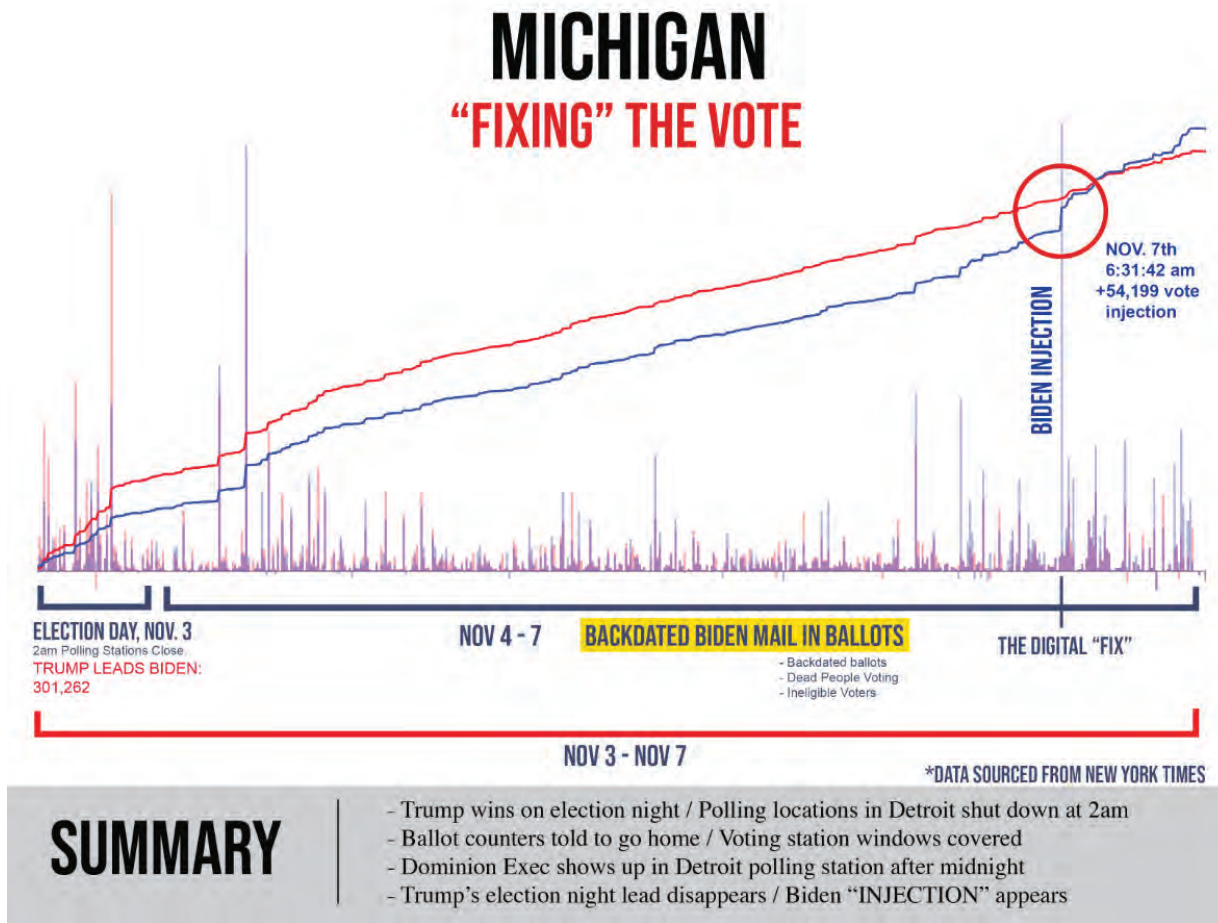


*DATA SOURCED FROM NEW YORK TIMES

SUMMARY

- Mathematical evidence of the seeding "injection" of votes at the beginning
- A spike means that a large number of votes were injected into the totals
- A normal vote pattern would look like a natural progression – smooth without extreme jumps

70. Gaussian Elimination without pivoting explains how the algorithm would behave and the election results and data from Michigan confirm FAILURE of algorithm.



71. The "Digital Fix" observed with an increased spike in VOTES for Joe Biden can be determined as evidence of a pivot. Normally it would be assumed that the algorithm had a Complete Pivot. Wilkinson's demonstrated the guarantee as :

$$\frac{\|U\|_{\infty}}{\|A\|_{\infty}} \leq n^{\frac{1}{2} \log(n)}$$

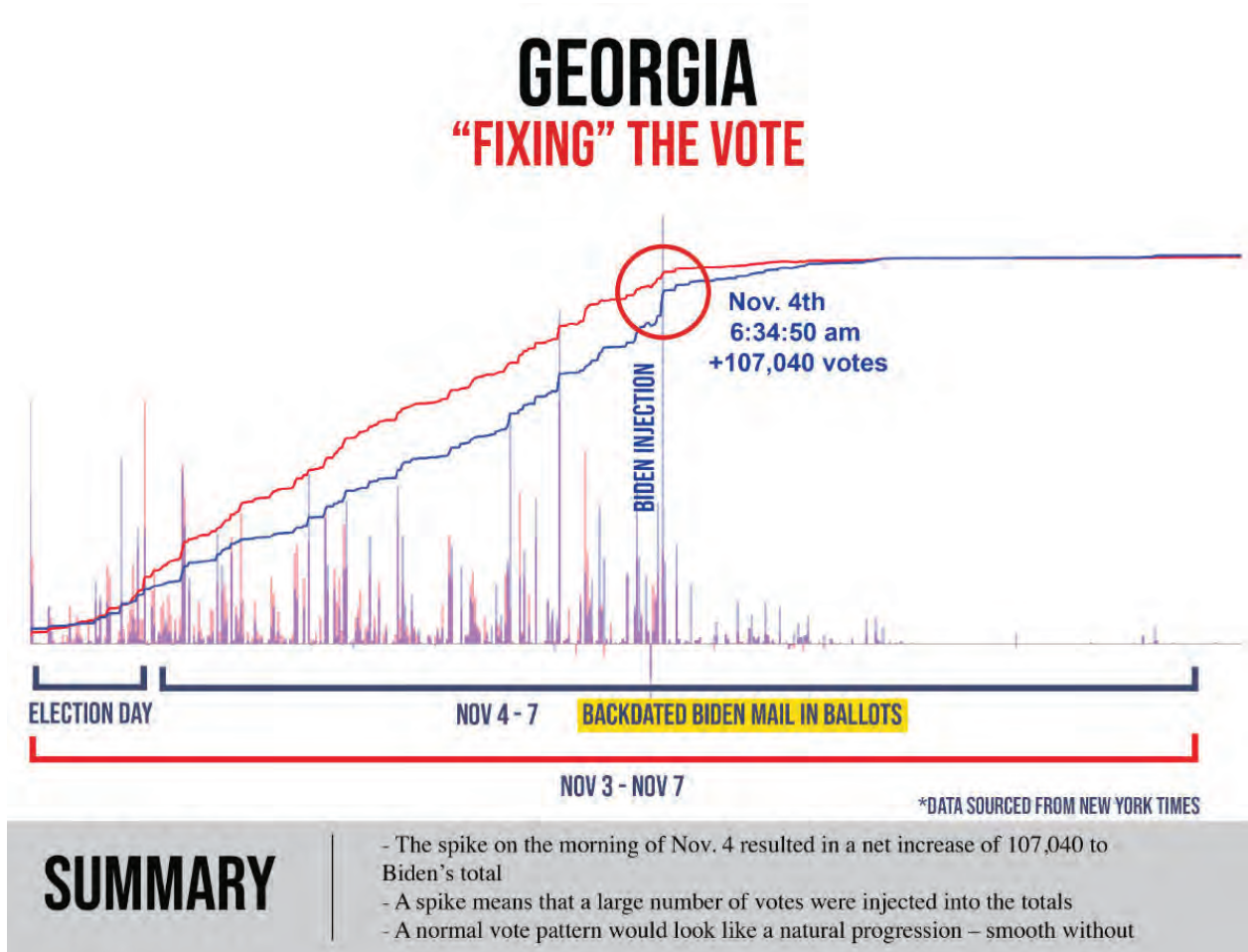
72.

73. Such a conjecture allows the growth factor the ability to be upper bound by values closer to n. Therefore, complete pivoting can't be observed because there would be too many floating points. Nor can partial as the partial pivoting would overwhelm after the "injection" of votes. Therefore, external factors were used which is evident from the "DIGITAL FIX"

74. Observing the elections, after a review of Michigan's data a spike of 54,199 votes to Biden. Because it is pushing and pulling and keeping a short distance between the 2 candidates; but then a spike, which is how an algorithm presents; - and this spike means there was a pause and an insert was made, where they insert an algorithm. Block spikes in votes for JOE BIDEN were NOT paper

ballots being fed or THUMB DRIVES. The algorithm block adjusted itself and the PEOPLE were creating the evidence to BACK UP the block allocation.

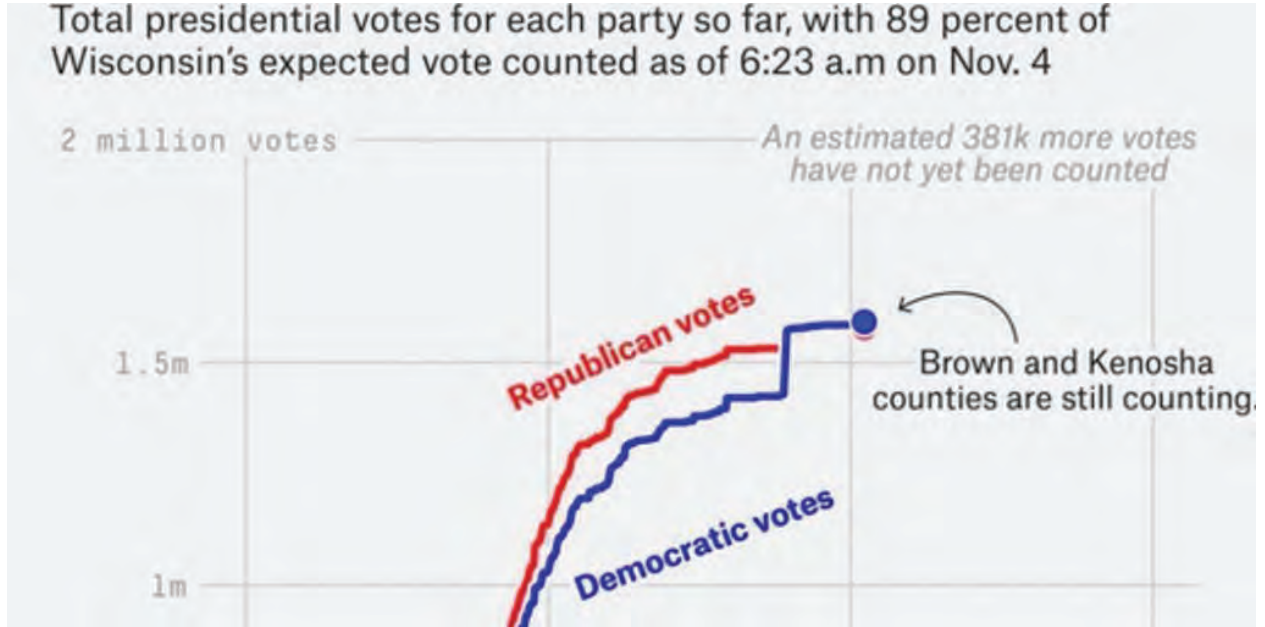
- 75. I have witnessed the same behavior of the election software in countries outside of the United States and within the United States. In -----, the elections conducted behaved in the same manner by allocating BLOCK votes to the candidate “chosen” to win.
- 76. Observing the data of the contested states (and others) the algorithm deployed is identical to that which was deployed in 2012 providing Barack Hussein Obama a block allocation to win the 2012 Presidential Elections.
- 77. The algorithm looks to have been set to give Joe Biden a 52% win even with an initial 50K+ vote block allocation was provided initially as tallying began (as in case of Arizona too). In the am of November 4, 2020 the algorithm stopped working, therefore another “block allocation” to remedy the failure of the algorithm. This was done manually as ALL the SYSTEMS shut down NATIONWIDE to avoid detection.



- 78.
- 79. In Georgia during the 2016 Presidential Elections a failed attempt to deploy the scripts to block allocate votes from a centralized location where the “trap-door” key lay an attempt by someone using

the DHS servers was detected by the state of GA. The GA leadership assumed that it was “Russians” but later they found out that the IP address was that of DHS.

80. In the state of Wisconsin, we observed a considerable BLOCK vote allocation by the algorithm at the SAME TIME it happened across the nation. All systems shut down at around the same time.



81.

82. In Wisconsin there are also irregularities in respect to BALLOT requests. (names AND address Hidden for privacy)

F	G	H	V	W	X	Y	AB	AC	AD	AG	AH	AI	AJ	AK	AL	AM
active	Registered	Military	Brown County	11/01/2020	Online	Military		Official	Active	Not Returned	Online	11/01/2020				
active	Registered	Regular	Brown County	10/23/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	10/23/2020	10/23/2020			
active	Registered	Military	Brown County	11/01/2020	Online	Military		Official	Active	Not Returned	Online	11/01/2020				
active	Registered	Regular	Brown County	11/01/2020	Online											
active	Registered	Regular	Brown County	11/01/2020	Email	Regular		Official	Active	Returned	Mail	10/31/2020	11/02/2020			
active	Registered	Regular	Brown County	11/01/2020	Email	Regular		Official	Active	Returned	Mail	10/31/2020	11/02/2020			
active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020			
active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020			
active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020			
active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020			
active	Registered	Regular	Brown County	11/02/2020	Voted in Person	Regular		Official	Active	Returned	Voted In Person	11/02/2020	11/02/2020			
active	Registered	Regular	Brown County	11/02/2020	Online											
active	Registered	Regular	Brown County	11/02/2020	Received in Person	Hospitaliz		Official	Active	Returned	Appointed Agent	11/02/2020	11/02/2020			
active	Registered	Regular	Brown County	11/02/2020	Email	Hospitaliz		Official	Active	Returned	Appointed Agent	11/02/2020	11/02/2020			
active	Registered	Military	Brown County	11/02/2020	Mail											
active	Registered	Regular	Brown County	11/02/2020	Mail	Regular		Official	Active	Returned	Appointed Agent	11/02/2020	11/02/2020			
active	Registered	Regular	Brown County	11/02/2020	Mail	Regular		Official	Active	Returned	Appointed Agent	11/02/2020	11/02/2020			
active	Registered	Military	Brown County	11/02/2020	Online	Military		Official	Active	Not Returned	Online	11/02/2020				
active	Registered	Military	Brown County	11/02/2020	Online	Military		Official	Active	Not Returned	Online	11/02/2020				
active	Registered	Regular	Brown County	11/02/2020	FPCA	Military		Official	Active	Not Returned	Mail	11/02/2020				
active	Registered	Military	Brown County	11/02/2020	FPCA	Military		Official	Active	Returned	Mail	11/02/2020	11/03/2020			
active	Registered	Regular	Brown County	11/03/2020	Voted in Person	Regular		Official	Inactive	Voter Spoiled	Voted In Person	11/03/2020	11/03/2020			
active	Registered	Military	Brown County	11/03/2020	Mail	Military	Certification insufficient	Federal Absent	Active	Returned, to be Rejected	Mail	11/03/2020	11/03/2020			
active	Registered	Military	Brown County	11/03/2020	Mail	Military		Official	Active	Not Returned	Mail	11/03/2020				
active	Registered	Military	Brown County	11/03/2020	Online											
active	Registered	Regular	Brown County	11/03/2020	Online											
active	Registered	Regular	Brown County	11/04/2020	Online											
active	Registered	Regular	Brown County	11/04/2020	Online											
active	Registered	Regular	Brown County	11/04/2020	Online											
active	Registered	Regular	Brown County	11/04/2020	Online											
active	Registered	Regular	Brown County	11/04/2020	Online											
active	Registered	Regular	Brown County	11/04/2020	Online											
active	Registered	Regular	Brown County	11/04/2020	Online											
active	Registered	Regular	Brown County	11/04/2020	Online											

83.

active	Registered	Regular	Brown County	11/03/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/04/2020	Online
active	Registered	Regular	Brown County	11/05/2020	Online
active	Registered	Regular	Brown County	11/05/2020	Online
active	Registered	Regular	Brown County	11/05/2020	Online
active	Registered	Regular	Brown County	11/05/2020	Online
active	Registered	Regular	Brown County	11/05/2020	Online
active	Registered	Regular	Brown County	11/05/2020	Online
active	Registered	Regular	Brown County	11/05/2020	Online
active	Registered	Regular	Brown County	11/05/2020	Online
active	Registered	Regular	Brown County	11/05/2020	Online
active	Registered	Regular	Brown County	11/05/2020	Online
active	Registered	Regular	Brown County	11/06/2020	Online
active	Registered	Regular	Brown County	11/06/2020	Online

- 84.
- 85. I can personally attest that in 2013 discussions by the Obama / Biden administration were being had with various agencies in the deployment of such election software to be deployed in ----- in 2013.
- 86. On or about April 2013 a one year plan was set to fund and usher elections in -----.
- 87. Joe Biden was designated by Barack Hussein Obama to ensure the ----- accepted assistance.
- 88. John Owen Brennan and James (Jim) Clapper were responsible for the ushering of the intelligence surrounding the elections in -----.
- 89. Under the guise of Crisis support the US Federal Tax Payers funded the deployment of the election software and machines in ----- signing on with Scytl.

The White House
Office of the Press Secretary

For Immediate Release

April 21, 2014

SHARE THIS:



FACT SHEET: U.S. Crisis Support Package for Ukraine

President Obama and Vice President Biden have made U.S. support for Ukraine an urgent priority as the Ukrainian government works to establish security and stability, pursue democratic elections and constitutional reform, revive its economy, and ensure government institutions are transparent and accountable to the Ukrainian people. Ukraine embarks on this reform path in the face of severe challenges to its sovereignty and territorial integrity, which we are working to address together with Ukraine and our partners in the international community. The United States is committed to ensuring that Ukrainians alone are able to determine their country's future without intimidation or coercion from outside forces. To support Ukraine, we are today announcing a new package of assistance totaling \$50 million to help Ukraine pursue political and economic reform and strengthen the partnership between the United States and Ukraine.

90.

91. Right before the ----- elections it was alleged that CyberBerkut a pro-Russia group infiltrated --- central election computers and **deleted key files**. These actions supposedly rendered the vote-tallying system inoperable.
92. In fact, the KEY FILES were the Commitment keys to allow Scytl to tally the votes rather than the election machines. The group had disclosed emails and other documents proving that their election was rigged and that they tried to avoid a fixed election.
93. The elections were held on May 25, 2014 but in the early AM hours the election results were BLOCKED and the final tally was DELAYED flipping the election in favor of -----.
94. The claim was that there was a DDoS attack by Russians when in actual fact it was a mitigation of the algorithm to inject block votes as we observed was done for Joe Biden because the KEYS were unable to be deployed. In the case of -----, the trap-door key was “altered”/deleted/ rendered ineffective. In the case of the US elections, representatives of Dominion/ ES&S/ Smartmatic/ Hart Intercivic would have to manually deploy them since if the entry points into the systems seemed to have failed.
95. The vote tallying of all states NATIONWIDE stalled and hung for days – as in the case of Alaska that has about 300K registered voters but was stuck at 56% reporting for almost a week.
96. This “hanging” indicates a failed deployment of the scripts to block allocate remotely from one location as observed in ----- on May 26, 2014.
97. This would justify the presence of the election machine software representatives making physical appearances in the states where the election results are currently being contested.
98. A Dominion Executive appeared at the polling center in Detroit after midnight.
99. Considering that the hardware of the machines has NOT been examined in Michigan since 2017 by Pro V& V according to Michigan’s own reporting. COTS are an avenue that hackers and bad actors seek to penetrate in order to control operations. Their software updates are the reason vulnerabilities to foreign interference in all operations exist.
100. The importance of VSTLs is underrated to protect up from foreign interference by way of open access via COTS software. Pro V& V who’s EAC certification EXPIRED on 24 FEB 2017 was contracted with the state of WISCONSIN.
101. In the United States each state is tasked to conduct and IV& V (Independent Verification and Validation) to provide assurance of the integrity of the votes.
102. If the “accredited” non-federal entities have NOT received EAC accreditation this is a failure of the states to uphold their own states standards that are federally regulated.
103. In addition, if the entities had NIST certificates they are NOT sufficing according the HAVA ACT 2002 as the role of NIST is clear.
104. Curiously, both companies PRO V&V and SLI GAMING received NIST certifications OUTSIDE the 24 month scope.

105. PRO V& V received a NIST certification on 26MAR2020 for ONE YEAR. Normally the NIST certification is good for two years to align with that of EAC certification that is good for two years.



106.

107. The last PRO V& V EAC accreditation certificate (Item 8) of this declaration expired in February 2017 which means that the IV & V conducted by Michigan claiming that they were accredited is false.

108. The significance of VSTLs being accredited and examining the HARDWARE is key. COTS software updates are the avenues of entry.

109. As per DOMINION'S own petition, the modems they use are COTS therefore failure to have an accredited VSTL examine the hardware for points of entry by their software is key.

*Compact Flash Cards	<p>***SanDisk Ultra: SDCFHS-004G SDCFHS-008G</p> <p>RiData: CFC-14A RDF8G-233XMCB2-1 RDF16G-233XMCB2-1 RDF32G-233XMCB2-1</p> <p>SanDisk Extreme: SDCFX-016G SDCFX-032G</p> <p>SanDisk: SDFAA-008G</p>		Memory device for ICP and ICE tabulators.
*Modems	<p>Verizon USB Modem Pantech UMW190NCD</p> <p>USB Modem MultiTech MT9234MU</p> <p>CellGo Cellular Modem E-Device 3GPUSUS</p> <p>AT&T USB Modem MultiTech GSM MTD- H5</p> <p>Fax Modem US Robotics 56K V.92.</p>		Analog and wireless modems for transmitting unofficial election night results.

110.

111. For example and update of Verizon USB Modem Pantech undergoes multiple software updates a year for it's hardware. That is most likely the point of entry into the systems.

112. During the 2014 elections in ---- it was the modems that gave access to the systems where the commitment keys were deleted.

113. SLI Gaming is the other VSTL "accredited" by the EAC BUT there is no record of their accreditation. In fact, SLI was NIST ISO Certified 27 days before the election which means that PA IV&V was conducted without NIST cert for SLI being valid.



- 114.
115. In fact SLI was NIST ISO Certified for less than 90 days.
116. I can personally attest that high-level officials of the Obama/Biden administration and large private contracting firms met with a software company called GEMS which is ultimately the software ALL election machines run now running under the flag of DOMINION.
117. GEMS was manifested from SOE software purchased by SCYTL developers and US Federally Funded persons to develop it.
118. The only way GEMS can be deployed across ALL machines is IF all counties across the nation are housed under the same server networks.
119. GEMS was tasked in 2009 to a contractor in Tampa, Fl.
120. GEMS was also fine-tuned in Latvia, Belarus, Serbia and Spain to be localized for EU deployment as observed during the Swissport election debacle.
121. John McCain's campaign assisted in FUNDING the development of GEMS web monitoring via WEB Services with 3EDC and Dynology.

Image# 13941014755

**SCHEDULE B-P
ITEMIZED DISBURSEMENTS**

Use separate schedule(s) for each category of the Detailed Summary Page

FOR LINE NUMBER: (check only one)

PAGE 7358 / 8595

<input checked="" type="checkbox"/> 23	<input type="checkbox"/> 24	<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27a
<input type="checkbox"/> 27b	<input type="checkbox"/> 28a	<input type="checkbox"/> 28b	<input type="checkbox"/> 28c	<input type="checkbox"/> 29

Any information copied from such Reports and Statements may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes, other than using the name and address of any political committee to solicit contributions from such committee.

NAME OF COMMITTEE (in Full)
JOHN MCCAIN 2008, INC.

Full Name (Last, First, Middle Initial) A. 3EDC LLC		Date of Disbursement MM / DD / YYYY 03 / 17 / 2008
Mailing Address 211 NORTH UNION ST STE 200		Transaction ID : SB23.10515
City ALEXANDRIA	State VA	
Zip Code 22314	Purpose of Disbursement WEB SERVICE	Amount of Each Disbursement this Period 399916.09
Candidate Name	Category/ Type	
Office Sought: <input type="checkbox"/> House <input type="checkbox"/> Senate <input type="checkbox"/> President	Disbursement For: 2008 <input checked="" type="checkbox"/> Primary <input type="checkbox"/> General <input type="checkbox"/> Other (specify) ▼	
State: District:		
Full Name (Last, First, Middle Initial) B. A FARE EXTRAORDINAIRE		Date of Disbursement MM / DD / YYYY 03 / 17 / 2008
Mailing Address 2035 MARSHALL		Transaction ID : SB23.10049
City HOUSTON	State TX	
Zip Code 77098	Purpose of Disbursement FACILITY RENTAL/CATERING	Amount of Each Disbursement this Period 23697.69
Candidate Name	Category/ Type	
Office Sought: <input type="checkbox"/> House <input type="checkbox"/> Senate <input type="checkbox"/> President	Disbursement For: 2008 <input checked="" type="checkbox"/> Primary <input type="checkbox"/> General <input type="checkbox"/> Other (specify) ▼	
State: District:		
Full Name (Last, First, Middle Initial) C. ADMINISTAFF		Date of Disbursement MM / DD / YYYY 03 / 05 / 2008
Mailing Address PO BOX 203332		Transaction ID : SB23.10117
City HOUSTON	State TX	
Zip Code 77216	Purpose of Disbursement INSURANCE	Amount of Each Disbursement this Period 483.68
Candidate Name	Category/ Type	
Office Sought: <input type="checkbox"/> House <input type="checkbox"/> Senate <input type="checkbox"/> President	Disbursement For: 2008 <input checked="" type="checkbox"/> Primary <input type="checkbox"/> General <input type="checkbox"/> Other (specify) ▼	
State: District:		
Subtotal Of Receipts This Page (optional).....		424097.46
Total This Period (last page this line number only).....		

122.

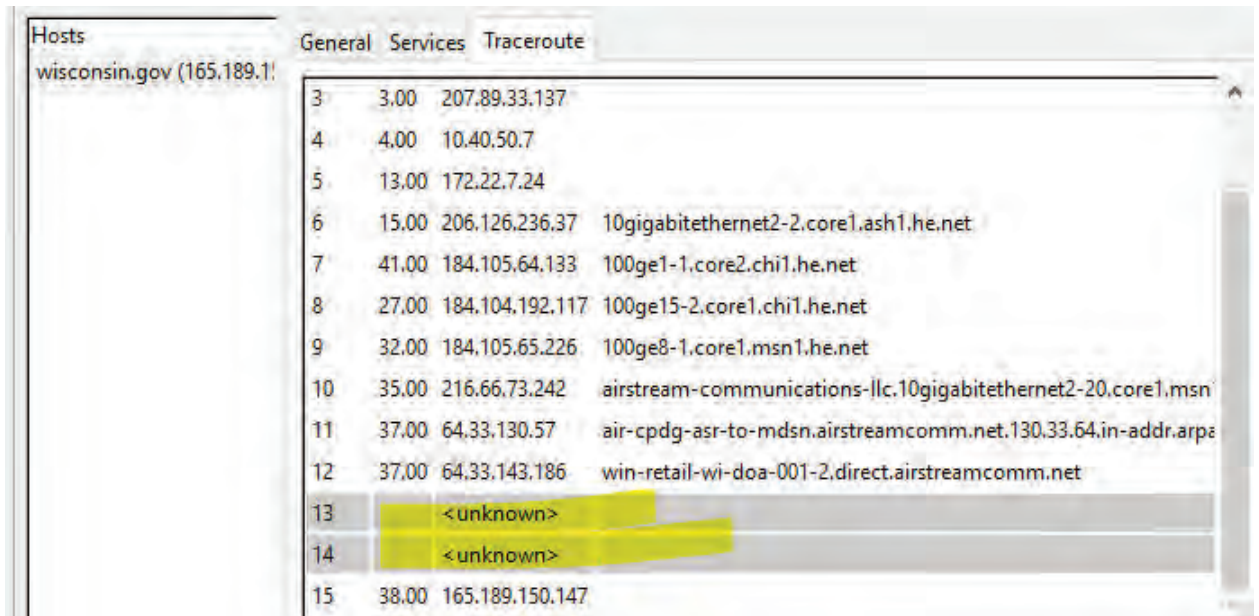
123.

124. AKAMAI Technologies services SCYTL.

- 125. AKAMAI Technologies Houses ALL foreign government sites. (Please see White Paper by Akamai.)
- 126. AKAMAI Technologies houses ALL .gov state sites. (ref Item 123 Wisconsin.gov Example)



- 127.
- 128. Wisconsin has EDGE GATEWAY port which is AKAMAI TECHNOLOGIES based out of GERMANY.
- 129. Using AKAMAI Technologies is allowing .gov sites to obfuscate and mask their systems by way of HURRICANE ELECTRIC (he.net) Kicking it to anonymous (AKAMAI Technologies) offshore servers.



- 130.
- 131. AKAMAI Technologies has locations around the world.
- 132. AKAMAI Technologies has locations in China (ref item 22)
- 133. AKAMAI Technologies has locations in Iran as of 2019.
- 134. AKAMAI Technologies merged with UNICOM (CHINESE TELECOMM) in 2018.
- 135. AKAMAI Technologies house all state .gov information in GERMANY via TELIA AB.

136. In my professional opinion, this affidavit presents unambiguous evidence:
137. That there was Foreign interference, complicit behavior by the previous administrations from 1999 up until today to hinder the voice of the people and US persons knowingly and willingly colluding with foreign powers to steer our 2020 elections that can be named in a classified setting.
138. Foreign interference is present in the 2020 election in various means namely,
139. Foreign nationals assisted in the creation of GEMS (Dominion Software Foundation)
140. Akamai Technologies merged with a Chinese company that makes the COTS components of the election machines providing access to our electronic voting machines.
141. Foreign investments and interests in the creation of the GEMS software.
142. US persons holding an office and private individuals knowingly and willingly oversaw fail safes to secure our elections.
143. The EAC failed to abide by standards set in HAVA ACT 2002.
144. The IG of the EAC failed to address complaints since their appointment regarding vote integrity
145. Christy McCormick of the EAC failed to ensure that EAC conducted their duties as set forth by HAVA ACT 2002
146. Both Patricia Layfield (IG of EAC) and Christy McCormick (Chairwoman of EAC) were appointed by Barack Hussein Obama and have maintained their positions since then.
147. The EAC failed to have a quorum for over a calendar year leading to the inability to meet the standards of the EAC.
148. AKAMAI Technologies and Hurricane Electric raise serious concerns for NATSEC due to their ties with foreign hostile nations.
149. For all the reasons above a complete failure of duty to provide safe and just elections are observed.
150. For the people of the United States to have confidence in their elections our cybersecurity standards should not be in the hands of foreign nations.
151. Those responsible within the Intelligence Community directly and indirectly by way of procurement of services should be held accountable for assisting in the development, implementation and promotion of GEMS.
152. GEMS ----- General Hayden.
153. In my opinion and from the data and events I have observed ----- with the assistance of SHADOWNET under the guise of L3-Communications which is MPRI. This is also confirmed by [us.army.mil](https://www.us.army.mil) making the statement that shadownet has been deployed to 30 states which all

happen to be using Dominion Machines.

FAIRFAX, Va. -The Virginia National Guard's Bowling Green-based 91st Cyber Brigade completed the nationwide rollout of its ShadowNet enterprise solution July 19, 2019, with the integration of the 125th Cyber Protection Battalion into the solution's virtual private network. ShadowNet is a custom-built private cloud-based out of the brigade's data center in Fairfax, Virginia, that uses VPN connectivity to provide its aligned units with 24-hour, seven-days-a-week remote access to critical cyber training at both the collective and individual levels. The brigade successfully integrated its three other cyber protection battalions - the 123rd, 124th, and 126th Cyber Protection Battalions - into the ShadowNet platform last January.

"I'm extremely proud to announce that the Soldiers of the 91st Cyber Brigade have completed the construction and rollout of ShadowNet, a world-class enterprise solution designed to propel operational innovation in the field of cyber training," said Col. Adam C. Volant, commander of the 91st Cyber Brigade. "ShadowNet will allow us to leverage the expertise of cyber professionals across our four cyber protection battalions to build Soldier-centric programs and collective training environments that deliver breakthroughs in exercise complexity and cost efficiency. Its robust

OCTOBER 26, 2020

U.S. Army STAND-TO! | Army Readiness Training

SEPTEMBER 12, 2019

September 2017 Nominative Sergeant Major Assignments

SEPTEMBER 12, 2019

DA ANNOUNCES ROTATIONAL DEPLOYMENTS

154. Based on my research of voter data – it appears that there are approximately 23,000 residents of a Department of Corrections Prison with requests for absentee ballot in Wisconsin. We are currently reviewing and verifying the data and will supplement.

	23230	Gutierrez	Mary	Jane		(202)994-9050	
23231	23231	Hansen	Luann	M		(262)994-9050	
23232	23232	Neberman	John	C		(262)994-9050	
23233	23233	Reynolds	Devi	J		(262)994-9050	
23234	23234	Rieckhoff	Kathryn	Susan		(262)994-9050	
23235	23235	Edwards	Mark	Landon		(262)994-9050	
23236	23236	Pfeiffer	Joseph	Patrick		(262)994-9050	
23237	23237	Hines	Dianna	K		(262)994-9050	
23238	23238	Beachem	Janice	F		(262)994-9050	
23239	23239	Blackstone	Thomas	Wayne		(262)994-9050	
23240	23240	Braun	Patricia	Ann		(262)994-9050	
23241	23241	Smith	Raymond	L		(262)994-9050	
23242	23242	Meyer	Steven	R		(262)994-9050	
23243	23243	Vincent	Herbert			(262)994-9050	
23244	23244	Guajardo	Juan	P		(262)994-9050	
23245	23245	Wallace	Kirk	R		(262)994-9050	
23246	23246	Kaplan	Bernard	L		(262)994-9050	
23247	23247	Bahrs	Michelle	M		(262)994-9050	
23248	23248	Shattuck	Elizabeth	L		(262)994-9050	
23249	23249	Munoz	Rosalio	S	JR	(262)994-9050	
23250	23250	Strunk	Amy	C		(262)994-9050	
23251	23251	Schendel	Michael	P	JR	(262)994-9050	
23252	23252	Mack	Kimberly	N		(262)994-9050	
23253	23253	Spikes	Debra	A		(262)994-9050	
23254	23254	Busarow	Suzanne	M		(262)994-9050	
23255	23255	Oliver	Timmy			(262)994-9050	
23256	23256	Wember	Jimmy	Dean		(262)994-9050	
23257	23257	Kosterman	Michael	Richard		(262)994-9050	
23258	23258	Szaradowski	Paul	M		(262)994-9050	
23259	23259	Oliver	Dale			(262)994-9050	
23260	23260	Derango	Nancy			(262)994-9050	
23261	23261	Smith	Arthur	J		(262)994-9050	SMITH24.3059@YAHOO
23262	23262	Brown	Michael	Edward		(262)994-9050	

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge.

Executed this November 29th, 2020.

A large black rectangular redaction box covering the signature area.A short black horizontal redaction bar.

EXHIBIT 14

DECLARATION OF RONALD WATKINS

I, Ronald Watkins, hereby state the following:

1. My name is Ronald Watkins. I am a United States citizen currently residing in Japan.
2. I am an adult of sound mind. All statements in this declaration are based on my personal knowledge and are true and correct. I am making this statement voluntarily and on my own initiative. I have not been promised, nor do I expect to receive, anything in exchange for my testimony and giving this statement. I have no expectation of any profit or reward and understand that there are those who may seek to harm me for what I say in this statement.
3. I make this declaration because I want to alert the public and let the world know the truth about the insecurity of actual voting tabulation software used in various states for administering the 2020 Presidential and other elections. The software is designed, whether with malicious intent or through plain incompetence, in such a way so as to facilitate digital ballot stuffing via simple vote result manipulation and abuse of the digital adjudication manual review system. Specifically, the Dominion Democracy Suite both enables voter fraud by unethical officials out to undermine the will of the people and facilitates tabulation errors by honest officials making simple, nearly untraceable mistakes.
4. I believe voting is a fundamental manifestation of our right to self-government, including our right to free speech. Under no circumstance should we allow a conspiracy of people and companies to subvert and destroy our most sacred rights.
5. I am a network and information security expert with nine years of experience as a network and information defense analyst and a network security engineer. In my nine years of network and information security experience, I have successfully defended large websites and complex networks against powerful cyberattacks. I have engaged in extensive training and education and learned through experience how to secure websites and networks.
6. In preparation for making this declaration, I have reviewed extensive technical materials relating to the Dominion Voting Democracy Suite, including those cited herein.
7. The Dominion Voting Systems ImageCast Central system is a software and hardware workstation system designed to work with just a common “Windows 10 Pro”¹² computer

¹ Dominion Voting, *Democracy Suite®ImageCast® Central User Guide*, p3, [online document], <https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-documentation/UG-ICC-UserGuide-5-11-CO.pdf> (Accessed November 23, 2020) <https://web.archive.org/web/20201019175854/https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> [archive]

² Georgia State Certification Testing, *Dominion Voting Systems D-Suite 5.5-A Voting System*, p5, table 2-1, [online document] https://sos.ga.gov/admin/uploads/Dominion_Test_Cert_Report.pdf (accessed November, 23,

paired via data cable³ to an off-the-shelf document scanner⁴ “for high speed scanning and counting of paper ballots.”⁵

8. When bulk ballot scanning and tabulation begins, the “ImageCast Central” workstation operator will load a batch of ballots into the scanner feed tray and then start the scanning procedure within the software menu.⁶ The scanner then begins to scan the ballots which were loaded into the feed tray while the “ImageCast Central” software application

2020),
https://web.archive.org/web/20201106055006/https://sos.ga.gov/admin/uploads/Dominion_Test_Cert_Report.pdf [archive].

³ Dominion Voting, *Democracy Suite®ImageCast® Central User Guide*, p2, s2.1, [online document, <https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> (Accessed November 23, 2020) <https://web.archive.org/web/20201019175854/https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> [archive].

⁴ Michigan.gov, DOMINION VOTING SYSTEMS CONTRACT No. 071B7700117, p6, 1.1.E.1, [online document],
https://www.michigan.gov/documents/sos/071B7700117_Dominion_Exhibit_2_to_Sch_A_Tech_Req_555357_7.pdf (accessed November 23, 2020),
https://web.archive.org/web/20201115084004/https://www.michigan.gov/documents/sos/071B7700117_Dominion_Exhibit_2_to_Sch_A_Tech_Req_555357_7.pdf [archive]

⁵ Commonwealth of Pennsylvania Department of State, Report Concerning the Examination Results of Dominion Voting Systems Democracy Suite 5.5A p6, s2.4, [online document],
<https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/Dominion%20Democracy%20Suite%205.5-A/Dominion%20Democracy%20Suite%20Final%20Report%20scanned%20with%20signature%20011819.pdf> (accessed November 23, 2020),
<https://web.archive.org/web/20201016161321/https://www.dos.pa.gov/VotingElections/Documents/Voting%20Systems/Dominion%20Democracy%20Suite%205.5-A/Dominion%20Democracy%20Suite%20Final%20Report%20scanned%20with%20signature%20011819.pdf> [archive]

⁶ Dominion Voting, *ImageCast Central*, p2, [online document],
<https://www.edcgov.us/Government/Elections/Documents/ImageCast%20Central%20Brochure%202018%20FINAL.pdf> (accessed November 23, 2020)
<https://web.archive.org/web/20201017175507/https://www.edcgov.us/Government/Elections/Documents/ImageCast%20Central%20Brochure%202018%20FINAL.pdf> [archive]

tabulates votes in real-time. Information about scanned ballots can be tracked inside the “ImageCast Central” software application.⁷

9. After all of the ballots loaded into the scanner’s feed tray have been through the scanner, the “ImageCast Central” operator will remove the ballots from the tray and then will have the option to “Accept Batch” on the scanning menu.⁸ Accepting the batch saves the results into the local file system within the “Windows 10 Pro” machine.⁹ Any “problem ballots” that may need to be examined or adjudicated at a later time can be found as ballot scans saved as image files into a standard Windows folder named “NotCastImages”.¹⁰ These “problem ballots” are automatically detected during the scanning phase and digitally set aside for manual review based on exception criteria.¹¹ Examples of exceptions may include: overvotes, undervotes, blank contests, blank ballots, write-in selections, and marginal

⁷ Dominion Voting, Democracy Suite®ImageCast® Central User Guide, p25, s4.1.2, [online document], <https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> (Accessed November 23, 2020), <https://web.archive.org/web/20201019175854/https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> [archive].

⁸ Dominion Voting, ImageCast Central, [website], <https://www.dominionvoting.com/imagecast-central/> (Accessed November 23, 2020) <https://web.archive.org/web/20201101203418/https://www.dominionvoting.com/imagecast-central/> [archive].

⁹ Dominion Voting, Democracy Suite®ImageCast® Central User Guide, p25, s4.1.2, [online document], <https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> (Accessed November 23, 2020), <https://web.archive.org/web/20201019175854/https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> [archive].

¹⁰ Dominion Voting, Democracy Suite®ImageCast® Central User Guide, p25, s4.1.2, [online document], <https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> (Accessed November 23, 2020), <https://web.archive.org/web/20201019175854/https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> [archive].

¹¹ Michigan.gov, DOMINION VOTING SYSTEMS CONTRACT No. 071B7700117, p21, 1.3.B.6, [online document], https://www.michigan.gov/documents/sos/071B7700117_Dominion_Exhibit_2_to_Sch_A_Tech_Req_555357_7.pdf (accessed November 23, 2020), https://web.archive.org/web/20201115084004/https://www.michigan.gov/documents/sos/071B7700117_Dominion_Exhibit_2_to_Sch_A_Tech_Req_555357_7.pdf [archive].

marks.”¹² Customizable outstack conditions and marginal mark detection lets [Dominion's Customers] decide which ballots are sent for Adjudication.¹³

10. During the ballot scanning process, the “ImageCast Central” software will detect how much of a percent coverage of the oval was filled in by the voter.¹⁴ The Dominion customer determines the thresholds of which the oval needs to be covered by a mark in order to qualify as a valid vote.¹⁵ If a ballot has a marginal mark which did not meet the specific thresholds set by the customer, then the ballot is considered a “problem ballot” and may be set aside into a folder named “NotCastImages.”¹⁷ “The ImageCast Central's advanced

¹² [11] MASTER SOLUTION PURCHASE AND SERVICES AGREEMENT BY AND BETWEEN DOMINION VOTING SYSTEMS, INC. as Contractor, and SECRETARY OF STATE OF THE STATE OF GEORGIA as State, p52, s1.3, [online document], <https://georgiaelections.weebly.com/uploads/1/0/8/5/108591015/contract.pdf> (Accessed November 23, 2020), <https://web.archive.org/web/20201122213728/https://georgiaelections.weebly.com/uploads/1/0/8/5/108591015/contract.pdf> [archive].

¹³ Dominion Voting, ImageCast Central, [website], <https://www.dominionvoting.com/imagecast-central/> (Accessed November 23, 2020) <https://web.archive.org/web/20201101203418/https://www.dominionvoting.com/imagecast-central/> [archive].

¹⁴ Michigan.gov, DOMINION VOTING SYSTEMS CONTRACT No. 071B7700117, p3, 1.1.A.22, [online document], https://www.michigan.gov/documents/sos/071B7700117_Dominion_Exhibit_2_to_Sch_A_Tech_Req_555357_7.pdf (accessed November 23, 2020), https://web.archive.org/web/20201115084004/https://www.michigan.gov/documents/sos/071B7700117_Dominion_Exhibit_2_to_Sch_A_Tech_Req_555357_7.pdf [archive].

¹⁵ Calhoun County, MI, ImageCast Central (ICC) 5.5 Operations, p19, [online document], https://cms5.revize.com/revize/calhouncountymi/Clerk%20&%20Register%20of%20Deeds/local%20clerk%20resources/5_5_icc_operations_manual.pdf (accessed November 23, 2020), https://web.archive.org/web/20200802003507/https://cms5.revize.com/revize/calhouncountymi/Clerk%20&%20Register%20of%20Deeds/local%20clerk%20resources/5_5_icc_operations_manual.pdf [archive].

¹⁶ IMAGECAST® CENTRAL Brochure, [website], <https://www.edcgov.us/Government/Elections/Documents/ImageCast%20Central%20Brochure%202018%20FINAL.pdf> (accessed November 23, 2020), <https://web.archive.org/web/20201017175507/https://www.edcgov.us/Government/Elections/Documents/ImageCast%20Central%20Brochure%202018%20FINAL.pdf> [archive].

¹⁷ Dominion Voting, Democracy Suite®ImageCast® Central User Guide, p25, s4.1.2, [online document], <https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> (Accessed November 23, 2020), <https://web.archive.org/web/20201019175854/https://www.sos.state.co.us/pubs/>

settings allow for adjustment of the scanning properties to “[set] the clarity levels at which the ballot should be scanned at.” Levels can be set as a combination of brightness and contrast values, or as a gamma value.”¹⁸

11. Based on my review of these materials, I conclude the system is designed in such a way that it allows a dishonest or otherwise unethical election administrator to creatively tweak the oval coverage threshold settings and advanced settings on the ImageCast Central scanners to set thresholds in such a way that a non-trivial amount of properly-marked ballots are marked as “problem ballots” and sent to the “NotCastImages” folder.
12. The administrator of the ImageCast Central work-station may view all images of scanned ballots which were deemed “problem ballots” by simply navigating via the standard “Windows File Explorer” to the folder named “NotCastImages” which holds ballot scans of “problem ballots.”¹⁹²⁰ Under this system, it is possible for an administrator of the “ImageCast Central” workstation to view and delete any individual ballot scans from the “NotCastImages” folder by simply using the standard Windows delete and recycle bin functions provided by the Windows 10 Pro operating system. Adjudication is “the process of examining voted ballots to determine, and, in the judicial sense, adjudicate voter intent.”²¹

elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide- 5-11-CO.pdf [archive].

¹⁸ Dominion Voting, Democracy Suite®ImageCast® Central User Guide, pp20-21, s3.22, [online document], <https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide-5-11-CO.pdf> (Accessed November 23, 2020), <https://web.archive.org/web/20201019175854/https://www.sos.state.co.us/pubs/elections/VotingSystems/DVS-DemocracySuite511/documentation/UG-ICC-UserGuide- 5-11-CO.pdf> [archive].

¹⁹ Dominion Voting, Democracy Suite® Use Procedures, p433, F.3.11, [online document] <https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds510-use-proc-jan.pdf> (Accessed November 23, 2020), <https://web.archive.org/web/20201101173723/https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds510-use-proc-jan.pdf> [archive].

²⁰ Calhoun County, MI, ImageCast Central (ICC) 5.5 Operations, p27, [online document], https://cms5.revize.com/revize/calhouncountymi/Clerk%20&%20Register%20of%20Deeds/local%20clerk%20resources/5_5_icc_operations_manual.pdf (accessed November 23, 2020), https://web.archive.org/web/20200802003507/https://cms5.revize.com/revize/calhouncountymi/Clerk%20&%20Register%20of%20Deeds/local%20clerk%20resources/5_5_icc_operations_manual.pdf [archive].

²¹ Dominion Voting, Democracy Suite® Use Procedures, p9, [online document] <https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds510-use-proc-jan.pdf> (Accessed November 23, 2020),

13. Based on my review of these materials, I conclude that a biased poll worker without sufficient and honest oversight could abuse the adjudication system to fraudulently switch votes for a specific candidate.
14. After the tabulation process, the ImageCast Central software saves a copy of the tabulation results locally to the “Windows 10 Pro” machine’s internal storage. The results data is located in an easy-to-find path which is designed to easily facilitate the uploading of tabulation results to flash memory cards. The upload process is just a simple copying of a “Results” folder containing vote tallies to a flash memory card connected to the “Windows 10 Pro” machine. The copy process uses the standard drag-and-drop or copy/paste mechanisms within “Windows File Explorer.”²² It is my conclusion that while this is a simple procedure, the report results process is subject to user errors and is very vulnerable to corrupt manipulation by a malicious administrator. It is my conclusion that, before delivering final tabulation results to the county, it is possible for an administrator to mistakenly copy the wrong “Results” folder or even maliciously copy a false “Results” folder, which could contain a manipulated data set, to the flash memory card and deliver those false “Results” as the outcome of the election.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed in Japan on November 24, 2020.

Ronald Watkins

<https://web.archive.org/web/20201101173723/https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds510-use-proc-jan.pdf> [archive].

²² Calhoun County, MI, ImageCast Central (ICC) 5.5 Operations, pp25-28, [online document], https://cms5.revize.com/revize/calhouncountymi/Clerk%20&%20Register%20of%20Deeds/local%20clerk%20resources/5_5_icc_operations_manual.pdf (accessed November 23, 2020), https://web.archive.org/web/20200802003507/https://cms5.revize.com/revize/calhouncountymi/Clerk%20&%20Register%20of%20Deeds/local%20clerk%20resources/5_5_icc_operations_manual.pdf [archive].

EXHIBIT 15

Congress of the United States

Washington, DC 20515

October 6, 2006

Henry M. Paulson, Jr.
Secretary
Department of the Treasury
1500 Pennsylvania Ave., N.W.
Washington, D.C. 20220

Dear Mr. Secretary:

I am writing to follow up on my letter of May 4, 2006, to Secretary Snow, seeking review by the Committee on Foreign Investment in the United States of the acquisition of Sequoia Voting Systems by Smartmatic, a foreign-owned company. I believe this transaction raises exactly the sort of foreign ownership issues that CFIUS is best positioned to examine for national security concerns. As discussed below, publicly reported information about Smartmatic's ownership and about the vulnerability of electronic voting machines to tampering raises serious concerns. I strongly urge CFIUS to independently verify the information provided to American officials and the public by Sequoia/Smartmatic, and to take all appropriate measures to safeguard our national security.

It is undisputed that Smartmatic is foreign-owned and it has acquired Sequoia, one of the three major voting machine companies doing business in the U.S. According to a Sequoia press release in May 2006 (copy attached) Sequoia voting machines were used to record over 125 million votes during the 2004 Presidential election in the United States. As we confront another election, Americans deserve to know that the Administration has made sure that any foreign ownership of voting machines poses no national security threat.

Although many press reports have tried, it appears that it is not possible to discern the true owners of Smartmatic from information available to the public. Smartmatic now acknowledges that Antonio Mugica, a Venezuelan businessman, has a controlling interest in Smartmatic, but the company has not revealed who all the other Smartmatic owners are. According to the press, Smartmatic's owners are hidden through a web of off-shore private entities. (See attached articles.)

The opaque nature of Smartmatic's ownership is particularly troubling since Smartmatic has been associated by the press with the Venezuelan government led by Hugo Chavez, which is openly hostile to the United States. According to press reports, Smartmatic shared a founder, officers, directors and a principal place of business with Bizta, a company in which, according to Smartmatic, the Venezuelan government previously held a 28% stake. Mugica is also a director of Bizta.

Henry M. Paulson, Jr.
October 6, 2006
Page 2

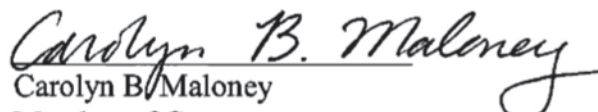
According to Smartmatic press releases, (copies attached) Smartmatic and Bizta were part of the consortium that received the government contract to provide the voting machines for the 2004 referendum election to recall Chavez as Venezuela's president, and have since been awarded other contracts by the Venezuelan government.

Smartmatic's possible connection to the Venezuelan government poses a potential national security concern in the context of its acquisition of Sequoia because electronic voting machines are susceptible to tampering and insiders are in the best position to engage in such tampering. The 2005 Government Accountability Office Report on electronic voting, GAO-05-956, and other private sector studies consistently support this conclusion. Thus, the reports that Sequoia brought Venezuelan nationals to the United States to work on the Chicago 2006 primary election raises questions about whether these individuals are subject to direction from a foreign interest that might pose a threat to the integrity of the election. Similarly, the use of Smartmatic software and machines developed in Venezuela, such as the HAAT software that was at issue in Chicago, raises questions as to whether this software is susceptible to manipulation by its unknown creators. Reportedly, Smartmatic may soon be introducing into the United States the type of electronic voting machines that were used (with Bizta software) in the controversial 2004 Venezuelan recall election, under the label AVC Edge II Plus.

In reviewing the Smartmatic acquisition of Sequoia, it is important that CFIUS understand the products and services that are of Venezuelan origin and evaluate Smartmatic's ownership to determine who could have influence and control over these and other Sequoia products and services that are in use or intended for use in U.S. elections. In light of Smartmatic's failure fully to answer these questions to date, this issue demands the most thorough independent investigation by CFIUS.

Thank you for your consideration of this letter.

Sincerely,


Carolyn B. Maloney
Member of Congress

Attachments

EXHIBIT 16

Congress of the United States

Washington, DC 20510

December 6, 2019

Sami Mnaymneh
Founder and Co-Chief Executive Officer
H.I.G. Capital, LLC

Tony Tamer
Founder and Co-Chief Executive Officer
H.I.G. Capital, LLC

Dear Messrs. Mnaymneh and Tamer:

We are writing to request information regarding H.I.G. Capital's (H.I.G.) investment in Hart InterCivic Inc. (Hart InterCivic) one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko.¹ For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies,"² owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimmed on security in favor of convenience," leaving voting systems across the country "prone to security problems."³ In light of these concerns, we request that you provide information about your firm, the portfolio

¹ Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, <https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/>; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, <https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html>.

² ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It.," Jessica Huseman, October 28, 2019, <https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it>.

³ Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, <https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c>.

companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early 2000s, almost twenty vendors competed in the election technology market.⁴ Today, three large vendors—Election Systems & Software, Dominion Voting Systems, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States.⁵ Private equity firms reportedly own or control each of these vendors, with very limited “information available in the public domain about their operations and financial performance.”⁶ While experts estimate that the total revenue for election technology vendors is about \$300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.⁷

Concentration in the election technology market and the fact that vendors are often “more seasoned in voting machine and technical services contract negotiations” than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems—leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.⁸ In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider “the cost to purchase or lease, operate, and maintain a voting system over its life span ... [and to] know how the vendor(s) plan to be profitable” when signing contracts, because vendors typically make their profits by ensuring “that they will be around to maintain it after the sale.” The EAC has warned election officials that “[i]f you do not manage the vendors, they will manage you.”⁹

Election security experts have noted for years that our nation’s election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States’ election infrastructure as “critical infrastructure” in order to prioritize the protection of our elections and to more effectively assist state and local election

⁴ Bloomberg, “Private Equity Controls the Gatekeepers of American Democracy,” Anders Melin and Reade Pickert, November 3, 2018, <https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy>.

⁵ Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

⁶ Id.

⁷ Id.

⁸ Brennan Center for Justice, “America’s Voting Machines at Risk,” Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf; Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

⁹ U.S. Election Assistance Commission, “Ten Things to Know About Selecting a Voting System,” October 14, 2017, <https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/>.

officials in addressing these risks.¹⁰ However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk.¹¹ In 2015, election officials in at least 31 states, representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state “using some machines that are no longer manufactured.”¹² Moreover, even when state and local officials work on replacing antiquated machines, many continue to “run on old software that will soon be outdated and more vulnerable to hackers.”¹³

In 2018 alone “voters in South Carolina [were] reporting machines that switched their votes after they’d inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana.”¹⁴ In addition, researchers recently uncovered previously undisclosed vulnerabilities in “nearly three dozen backend election systems in 10 states.”¹⁵ And, just this year, after the Democratic candidate’s electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county’s Republican Chairwoman said, “[n]othing went right on Election Day. Everything went wrong. That’s a problem.”¹⁶ These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

H.I.G. reportedly owns or has had investments in Hart InterCivic, a major election technology vendor. In order to help us understand your firm’s role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

1. Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the *Stop Wall Street Looting Act*.¹⁷
2. Which election technology companies, including all affiliates or related entities, does H.I.G. have a stake in or own? Please provide the name of and a brief description of the services each company provides.

¹⁰ Department of Homeland Security, “Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector,” January 6, 2017,

<https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>.

¹¹ AP News, “US election integrity depends on security-challenged firms,” Frank Bajak, October 29, 2018, <https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c>; Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

¹² Brennan Center for Justice, “America’s Voting Machines at Risk,” Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

¹³ Associated Press, “AP Exclusive: New election systems use vulnerable software,” Tami Abdollah, July 13, 2019, <https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1>.

¹⁴ Vice, “Here’s Why All the Voting Machines Are Broken and the Lines Are Extremely Long,” Jason Koebler and Matthew Gault, November 6, 2018, https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long.

¹⁵ Vice, “Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials,” Kim Zetter, August 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.

¹⁶ New York Times, “A Pennsylvania Country’s Election Day Nightmare Underscores Voting Machine Concerns,” Nick Corasaniti, November 30, 2019, <https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html>.


¹⁷ Stop Wall Street Looting Act, S.2155, <https://www.congress.gov/bill/116th-congress/senate-bill/2155>.

- a. Which election technology companies, including all affiliates or related entities, has H.I.G. had a stake in or owned in the past twenty years? Please provide the name of and a brief description of the services each company provides or provided.
 - b. For each election technology company H.I.G. had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
 - i. The name of the company
 - ii. Ownership stake
 - iii. Total revenue
 - iv. Net income
 - v. Percentage of revenue dedicated to research and development
 - vi. Total number of employees
 - vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
 - viii. Other private-equity firms that own a stake in the company
3. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.
 4. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.
 5. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.
 6. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.

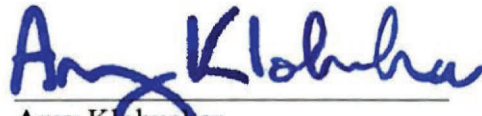
7. Has any election technology company, including all affiliates or related entities, in which H.I.G. has an ownership stake or has had an ownership stake in the past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or breach of contract? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.

Sincerely,



Elizabeth Warren
United States Senator



Amy Klobuchar
United States Senator



Ron Wyden
United States Senator




Mark Pocan
Member of Congress

Congress of the United States
Washington, DC 20510

December 6, 2019

Michael McCarthy
Chairman
McCarthy Group, LLC



Dear Mr. McCarthy:

We are writing to request information regarding McCarthy Group, LLC's (McCarthy Group) investment in Election Systems & Software (ES&S), one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko.¹ For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies,"² owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimmed on security in favor of convenience," leaving voting systems across the country "prone to security problems."³ In light of these concerns, we request that you provide information about your firm, the portfolio companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early

¹ Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, <https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/>; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, <https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html>.

² ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It.," Jessica Huseman, October 28, 2019, <https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it>.

³ Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, <https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c>.

2000s, almost twenty vendors competed in the election technology market.⁴ Today, three large vendors—ES&S, Dominion Voting Systems, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States.⁵ Private equity firms reportedly own or control each of these vendors, with very limited “information available in the public domain about their operations and financial performance.”⁶ While experts estimate that the total revenue for election technology vendors is about \$300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.⁷

Concentration in the election technology market and the fact that vendors are often “more seasoned in voting machine and technical services contract negotiations” than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems—leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.⁸ In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider “the cost to purchase or lease, operate, and maintain a voting system over its life span ... [and to] know how the vendor(s) plan to be profitable” when signing contracts, because vendors typically make their profits by ensuring “that they will be around to maintain it after the sale.” The EAC has warned election officials that “[i]f you do not manage the vendors, they will manage you.”⁹

Election security experts have noted for years that our nation’s election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States’ election infrastructure as “critical infrastructure” in order to prioritize the protection of our elections and to more effectively assist state and local election officials in addressing these risks.¹⁰ However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our

⁴ Bloomberg, “Private Equity Controls the Gatekeepers of American Democracy,” Anders Melin and Reade Pickert, November 3, 2018, <https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy>.

⁵ Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

⁶ Id.

⁷ Id.

⁸ Brennan Center for Justice, “America’s Voting Machines at Risk,” Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf; Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

⁹ U.S. Election Assistance Commission, “Ten Things to Know About Selecting a Voting System,” October 14, 2017, <https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/>.

¹⁰ Department of Homeland Security, “Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector,” January 6, 2017, <https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>.

elections at avoidable and increased risk.¹¹ In 2015, election officials in at least 31 states, representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state “using some machines that are no longer manufactured.”¹² Moreover, even when state and local officials work on replacing antiquated machines, many continue to “run on old software that will soon be outdated and more vulnerable to hackers.”¹³

In 2018 alone “voters in South Carolina [were] reporting machines that switched their votes after they’d inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana.”¹⁴ In addition, researchers recently uncovered previously undisclosed vulnerabilities in “nearly three dozen backend election systems in 10 states.”¹⁵ And, just this year, after the Democratic candidate’s electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county’s Republican Chairwoman said, “[n]othing went right on Election Day. Everything went wrong. That’s a problem.”¹⁶ These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

McCarthy Group reportedly owns or has had investments in ES&S, a major election technology vendor. In order to help us understand your firm’s role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

1. Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the *Stop Wall Street Looting Act*.¹⁷
2. Which election technology companies, including all affiliates or related entities, does McCarthy Group have a stake in or own? Please provide the name of and a brief description of the services each company provides.
 - a. Which election technology companies, including all affiliates or related entities, has McCarthy Group had a stake in or owned in the past twenty

¹¹ AP News, “US election integrity depends on security-challenged firms,” Frank Bajak, October 29, 2018, <https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c>; Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

¹² Brennan Center for Justice, “America’s Voting Machines at Risk,” Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

¹³ Associated Press, “AP Exclusive: New election systems use vulnerable software,” Tami Abdollah, July 13, 2019, <https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1>.

¹⁴ Vice, “Here’s Why All the Voting Machines Are Broken and the Lines Are Extremely Long,” Jason Koebler and Matthew Gault, November 6, 2018, https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long.

¹⁵ Vice, “Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials,” Kim Zetter, August 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.

¹⁶ New York Times, “A Pennsylvania Country’s Election Day Nightmare Underscores Voting Machine Concerns,” Nick Corasaniti, November 30, 2019, <https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html>.

¹⁷ Stop Wall Street Looting Act, S.2155, <https://www.congress.gov/bill/116th-congress/senate-bill/2155>.

years? Please provide the name of and a brief description of the services each company provides or provided.

- b. For each election technology company McCarthy Group had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
 - i. The name of the company
 - ii. Ownership stake
 - iii. Total revenue
 - iv. Net income
 - v. Percentage of revenue dedicated to research and development
 - vi. Total number of employees
 - vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
 - viii. Other private-equity firms that own a stake in the company
3. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.
4. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.
5. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.
6. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.
7. Has any election technology company, including all affiliates or related entities, in which McCarthy Group has an ownership stake or has had an ownership stake in the

past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or breach of contract? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.

Sincerely,



Elizabeth Warren
United States Senator



Amy Klobuchar
United States Senator



Ron Wyden
United States Senator



Mark Pocan
Member of Congress

Congress of the United States


Washington, DC 20510

December 6, 2019

Stephen D. Owens
Managing Director
Staple Street Capital Group, LLC



Hootan Yaghoobzadeh
Managing Director
Staple Street Capital Group, LLC



Dear Messrs. Owens and Yaghoobzadeh:

We are writing to request information regarding Staple Street Capital Group, LLC's (Staple Street) investment in Dominion Voting System (Dominion) one of three election technology vendors responsible for developing, manufacturing and maintaining the vast majority of voting machines and software in the United States, and to request information about your firm's structure and finances as it relates to this company.

Some private equity funds operate under a model where they purchase controlling interests in companies and implement drastic cost-cutting measures at the expense of consumers, workers, communities, and taxpayers. Recent examples include Toys "R" Us and Shopko.¹ For that reason, we have concerns about the spread and effect of private equity investment in many sectors of the economy, including the election technology industry—an integral part of our nation's democratic process. We are particularly concerned that secretive and "trouble-plagued companies,"² owned by private equity firms and responsible for manufacturing and maintaining voting machines and other election administration equipment, "have long skimmed on security in favor of convenience," leaving voting systems across the country "prone to security problems."³ In light of these concerns, we request that you provide information about your firm, the portfolio

¹ Atlantic, "The Demise of Toys 'R' Us Is a Warning," Bryce Covert, July/August 2018 issue, <https://www.theatlantic.com/magazine/archive/2018/07/toys-r-us-bankruptcy-private-equity/561758/>; Axios, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," Dan Primack, "How workers suffered from Shopko's bankruptcy while Sun Capital made money," June 11, 2019, <https://www.axios.com/shopko-bankruptcy-sun-capital-547b97ba-901c-4201-92cc-6d3168357fa3.html>.

² ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It.," Jessica Huseman, October 28, 2019, <https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it>.

³ Associated Press News, "US Election Integrity Depends on Security-Challenged Firms," Frank Bajak, October 28, 2019, <https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c>.

companies in which it has invested, the performance of those investments, and the ownership and financial structure of your funds.

Over the last two decades, the election technology industry has become highly concentrated, with a handful of consolidated vendors controlling the vast majority of the market. In the early 2000s, almost twenty vendors competed in the election technology market.⁴ Today, three large vendors—Election Systems & Software, Dominion, and Hart InterCivic—collectively provide voting machines and software that facilitate voting for over 90% of all eligible voters in the United States.⁵ Private equity firms reportedly own or control each of these vendors, with very limited “information available in the public domain about their operations and financial performance.”⁶ While experts estimate that the total revenue for election technology vendors is about \$300 million, there is no publicly available information on how much those vendors dedicate to research and development, maintenance of voting systems, or profits and executive compensation.⁷

Concentration in the election technology market and the fact that vendors are often “more seasoned in voting machine and technical services contract negotiations” than local election officials, give these companies incredible power in their negotiations with local and state governments. As a result, jurisdictions are often caught in expensive agreements in which the same vendor both sells or leases, and repairs and maintains voting systems—leaving local officials dependent on the vendor, and the vendor with little incentive to substantially overhaul and improve its products.⁸ In fact, the Election Assistance Commission (EAC), the primary federal body responsible for developing voluntary guidance on voting technology standards, advises state and local officials to consider “the cost to purchase or lease, operate, and maintain a voting system over its life span ... [and to] know how the vendor(s) plan to be profitable” when signing contracts, because vendors typically make their profits by ensuring “that they will be around to maintain it after the sale.” The EAC has warned election officials that “[i]f you do not manage the vendors, they will manage you.”⁹

Election security experts have noted for years that our nation’s election systems and infrastructure are under serious threat. In January 2017, the U.S. Department of Homeland Security designated the United States’ election infrastructure as “critical infrastructure” in order to prioritize the protection of our elections and to more effectively assist state and local election

⁴ Bloomberg, “Private Equity Controls the Gatekeepers of American Democracy,” Anders Melin and Reade Pickert, November 3, 2018, <https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy>.

⁵ Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

⁶ Id.

⁷ Id.

⁸ Brennan Center for Justice, “America’s Voting Machines at Risk,” Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf; Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

⁹ U.S. Election Assistance Commission, “Ten Things to Know About Selecting a Voting System,” October 14, 2017, <https://www.eac.gov/documents/2017/10/14/ten-things-to-know-about-selecting-a-voting-system-cybersecurity-voting-systems-voting-technology/>.

officials in addressing these risks.¹⁰ However, voting machines are reportedly falling apart across the country, as vendors neglect to innovate and improve important voting systems, putting our elections at avoidable and increased risk.¹¹ In 2015, election officials in at least 31 states, representing approximately 40 million registered voters, reported that their voting machines needed to be updated, with almost every state “using some machines that are no longer manufactured.”¹² Moreover, even when state and local officials work on replacing antiquated machines, many continue to “run on old software that will soon be outdated and more vulnerable to hackers.”¹³

In 2018 alone “voters in South Carolina [were] reporting machines that switched their votes after they’d inputted them, scanners [were] rejecting paper ballots in Missouri, and busted machines [were] causing long lines in Indiana.”¹⁴ In addition, researchers recently uncovered previously undisclosed vulnerabilities in “nearly three dozen backend election systems in 10 states.”¹⁵ And, just this year, after the Democratic candidate’s electronic tally showed he received an improbable 164 votes out of 55,000 cast in a Pennsylvania state judicial election in 2019, the county’s Republican Chairwoman said, “[n]othing went right on Election Day. Everything went wrong. That’s a problem.”¹⁶ These problems threaten the integrity of our elections and demonstrate the importance of election systems that are strong, durable, and not vulnerable to attack.

Staple Street reportedly owns or has had investments in Dominion, a major election technology vendor. In order to help us understand your firm’s role in this sector, we ask that you provide answers to the following questions no later than December 20, 2019.

1. Please provide the disclosure documents and information enumerated in Sections 501 and 503 of the *Stop Wall Street Looting Act*.¹⁷
2. Which election technology companies, including all affiliates or related entities, does Staple Street have a stake in or own? Please provide the name of and a brief description of the services each company provides.

¹⁰ Department of Homeland Security, “Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector,” January 6, 2017,

<https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical>.

¹¹ AP News, “US election integrity depends on security-challenged firms,” Frank Bajak, October 29, 2018, <https://apnews.com/f6876669cb6b4e4c9850844f8e015b4c>; Penn Wharton Public Policy Initiative, “The Business of Voting,” July 2018, <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>.

¹² Brennan Center for Justice, “America’s Voting Machines at Risk,” Lawrence Norden and Christopher Famighetti, 2015, https://www.brennancenter.org/sites/default/files/publications/Americas_Voting_Machines_At_Risk.pdf.

¹³ Associated Press, “AP Exclusive: New election systems use vulnerable software,” Tami Abdollah, July 13, 2019, <https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1>.

¹⁴ Vice, “Here’s Why All the Voting Machines Are Broken and the Lines Are Extremely Long,” Jason Koebler and Matthew Gault, November 6, 2018, https://www.vice.com/en_us/article/59vzgn/heres-why-all-the-voting-machines-are-broken-and-the-lines-are-extremely-long.

¹⁵ Vice, “Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials,” Kim Zetter, August 8, 2019, https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials.

¹⁶ New York Times, “A Pennsylvania Country’s Election Day Nightmare Underscores Voting Machine Concerns,” Nick Corasaniti, November 30, 2019, <https://www.nytimes.com/2019/11/30/us/politics/pennsylvania-voting-machines.html>.

¹⁷ Stop Wall Street Looting Act, S.2155, <https://www.congress.gov/bill/116th-congress/senate-bill/2155>.

- a. Which election technology companies, including all affiliates or related entities, has Staple Street had a stake in or owned in the past twenty years? Please provide the name of and a brief description of the services each company provides or provided.
 - b. For each election technology company Staple Street had a stake in or owned in the past twenty years, including all affiliates or related entities, please provide the following information for each year that the firm has had a stake in or owned this company and the five years preceding the firm's investment.
 - i. The name of the company
 - ii. Ownership stake
 - iii. Total revenue
 - iv. Net income
 - v. Percentage of revenue dedicated to research and development
 - vi. Total number of employees
 - vii. A list of all state and local jurisdictions with which the company has a contract to provide election related products or services
 - viii. Other private-equity firms that own a stake in the company
3. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with the EAC's Voluntary Voting System Guidelines? If so, please provide a copy of each EAC noncompliance notice received by the company and a description of what steps the company took to resolve each issue.
 4. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, been found to have been in noncompliance with any state or local voting system guidelines or practices? If so, please provide a list of all such instances and a description of what steps the company took to resolve each issue.
 5. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, been found to have violated any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such violations.
 6. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the last twenty years, reached a settlement with any federal or state law enforcement entity related to a potential violation of any federal or state laws or regulations? If so, please provide a complete list, including the date and description, of all such settlements.

7. Has any election technology company, including all affiliates or related entities, in which Staple Street has an ownership stake or has had an ownership stake in the past twenty years, reached a settlement with any state or local jurisdiction related to a potential violation of or breach of contract? If so, please provide a complete list, including the date and description, of all such settlements.

Thank you for your attention to this matter.


Sincerely,



Elizabeth Warren
United States Senator



Amy Klobuchar
United States Senator



Ron Wyden
United States Senator



Mark Pocan
Member of Congress

EXHIBIT 17

Declaration of Russell James Ramsland, Jr.

1. My name is Russell James Ramsland, Jr., and I am a resident of Dallas County, Texas. I submit this declaration pursuant to 28 USC sec 1746. I am over 18 years of age. I hold an MBA from Harvard University, and a political science degree from Duke University. I have worked with the National Aeronautics and Space Administration (NASA) and the Massachusetts Institute of Technology (MIT), among other organizations, and have run businesses all over the world, many of which are highly technical in nature. I have served on technical government panels.
2. I am part of the management team of Allied Security Operations Group, LLC, (ASOG). ASOG is a group of globally engaged professionals who come from various disciplines to include Department of Defense, Secret Service, Department of Homeland Security, and the Central Intelligence Agency. It provides a range of security services, but has a particular emphasis on cybersecurity, open source investigation and penetration testing of networks. We employ a wide variety of cyber and cyber forensic analysts. We have patents pending in a variety of applications from novel network security applications to SCADA (Supervisory Control and Data Acquisition) protection and safe browsing solutions for the dark and deep web. For this report, I have relied on these experts and resources.
3. In November 2018, ASOG analyzed audit logs for the central tabulation server of the ES&S Election Management System (EMS) for the Dallas, Texas, General Election of 2018. Our team was surprised at the enormous number of error messages that should not have been there. They numbered in the thousands, and the operator ignored and overrode all of them. This led to various legal challenges in that election, and we provided evidence and analysis in some of them.
4. As a result, ASOG initiated an 18-month study into the major EMS providers in the United States, among which are Dominion that provides EMS services in Maricopa County and ES&S that provides EMS services in Pima County and elsewhere in Arizona. We did thorough background research of the literature and there is confirmed evidence from both Democrat and Republican stakeholders in the vulnerability of Dominion and ES&S. The State of Texas rejected Dominion's certification for use there due to vulnerabilities and major vote tampering has been verified in Dallas County in the 2020 General Election where ES&S operates the EMS services. Next, we began doing passive penetration testing into the vulnerabilities described in the literature and confirmed for ourselves that in many cases, past vulnerabilities already identified were still left open to exploit in the November 2020 election. We also noticed a striking similarity between the approach to software and EMS systems of ES&S and Dominion. This was logical since they share a common ancestry in the Diebold voting system.
5. Over the past three decades, almost all of the states have shifted from a relatively low-technology format to a high-technology format that relies heavily on a handful of private services companies. These private companies supply the hardware and

software, often handle voter registrations, hold the voter records, partially manage the elections, program counting the votes and report the outcomes. Arizona is one of those states.

6. These systems contain a large number of known vulnerabilities to hacking and tampering, both when voters express their voting intention by marking an electronic ballot using ballot marking devices (BMDs) , and at the back end where the votes are stored, tabulated, and reported by election officials. These vulnerabilities are well known, and experts in the field have written extensively about them.

7. Dominion (“Dominion”) and Election Systems and Software (“ES&S”) are privately held companies that provide election technologies and services to government jurisdictions. Numerous counties across the state of Arizona use the ES&S Election Management System and Maricopa County uses the Dominion Election Management System. Both systems have options to be an electronic, paperless voting system with no permanent record of the voter’s choices, or a paper ballot based system or hybrid of those two.

8. Both ES&S and Dominion Election Management System’s central accumulator fail to include a very badly needed protected real-time audit log that maintains the date and time stamps of all significant election events. Key components of the systems utilize unprotected logs. Essentially this allows the internal operator or an external attacker the opportunity to arbitrarily add, modify, or remove log entries, causing the machine to log erroneous election events. The system makes the creation and maintenance of various logs voluntary, so that the user has a choice to “not retain” or “conceal” their actions. Further, when logs are left unprotected and can be altered, they no longer serve the functional purpose of provided a transparent audit log to the public or election officials.

9. My colleagues and I at ASOG have studied the information that is publicly available concerning the November 3, 2020, election results. Based on the significant anomalies and red flags that we have observed, we believe to a reasonable degree of professional certainty that election results have been manipulated within the ES&S and Dominion systems in Arizona. As one example, Dr. Andrew Appel, Princeton Professor of Computer Science and Election Security Expert has observed, with reference to Dominion Voting machines, “I figured out how to make a slightly different computer program that just before the polls were closed it switches some votes around from one candidate to another. I wrote that computer program into a memory chip and now to hack a voting machine you just need 7 minutes alone with it and a screwdriver.” We list below other red flags that our team has uncovered.

10. One red flag where Dominion is used has been seen in Antrim County, Michigan. There we have seen reports of 6,000 votes that were electronically switched from Donald Trump to Joe Biden and were only discoverable through a hand counted manual recount. While the first reports have suggested that it was due to a “glitch”

after an update, it was recanted and later attributed to “clerical error.” This change is important because if it were not due to clerical error, but due to a “glitch” emanating from an update, the system would be required to be “re-certified” according to Dominion officials. This was not done. We are skeptical of these assurances as we know firsthand this has many other plausible explanations and a full investigation of this event needs to be conducted as there are a reported 47 other counties using essentially the same system in Michigan. It is our belief (based on the information we have acquired to this point) that the problem most likely did occur due to a glitch where an update file didn’t properly synchronize the ballot barcode generation and reading portions of the system. If that is indeed the case, there is no reason to assume this would be an isolated error only in Michigan. This “glitch” would either cause the vote to be misread and directed to another candidate on the ballot or cause the entire ballot upload batch to read as zero in the tabulation processor. This in turn hands over the electronic system to an operator at the voting site with full control to allocate votes between candidates for the entire batch of ballots. We have also observed that provisional ballots were accepted properly but in-person ballots were being rejected (zeroed out and/or changed - flipped). Because of the highly vulnerable nature of these systems to error and exploits, it is my professional opinion based on a reasonable degree of certainty that in Maricopa Co. these systems may have experienced the same problem and switched votes from one Presidential candidate to the other.

11. In Dallas County where ES&S is used, the voter records during early voting were captured each day for those voters who cast ballots either in person or by mail-in and catalogued using the hash totals to provide an absolute unique identifier. As required by [state law](#), the Dallas County Elections Department [published](#) the Daily Vote Roster for all voters who cast ballots during Absentee and In-Person Early Voting. The Roster contained the VoterID, name, address, type of vote, and various dates associated with every Early-Voting vote cast. Dallas County claims its source of roster data was the In-Person Electronic Poll Books, and the Absentee Ballot scanners. Dallas County has claimed that entry into the Vote Roster can only be done by a registered Dallas County voter who either appeared In-Person or by Absentee Ballot. The computer that generated the roster was apparently hacked between October 7 and October 30. During that period tens of thousands of vote records were purged, added, or edited from the ES&S generated Vote Roster.

Specifically, over this period, 53,485 voter records had their hash identifier changed, meaning the vote was tampered with. In most cases, this tampering took the form of purging the vote, and then re-constituting it in some form or fashion, but with a change in the hash total meaning the vote was somehow changed. This translates into approximately 107,000 hacked votes in Dallas County alone for ES&S. Ten blocks of voters on Westminster Street in Highland Park had their votes purged and then some of them were selectively re-instated at a later date with changes from the vote intended by the voter as originally recorded. People who double voted were catalogued as well as dead people who voted, people with no VUID voted (800 of them), unregistered university students voted, and people living abroad who claim a

Dallas Residence for voting purposes, but who in a spot check are unknown to the residences they list in the ES&S system. A short list of them includes:

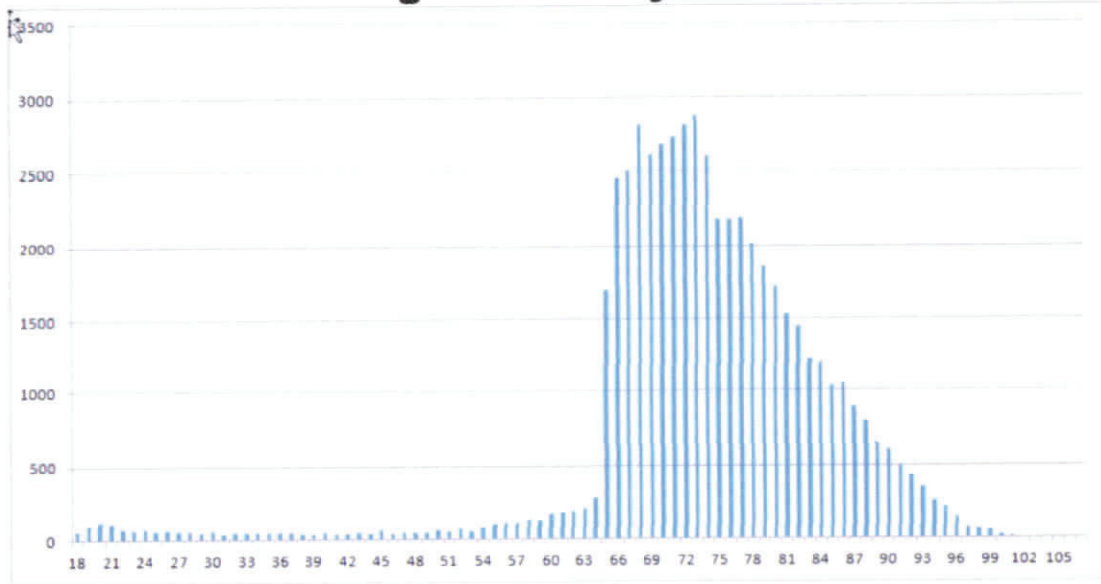
<u>Country</u>	<u>Voters Who Voted</u>
Mexico	118
Guatemala	9
Nicaragua	4
Kenya	18
Canada	154
Ireland	34
China	62
Australia	105
	<hr/> 504

In plain English, at the instant before a voter casts a ballot there is a one-to-one relationship between the voter and their ballot as well as a one-to-one association between the voter and their votes.

At the instant that ballot is cast, the one-to-one relationship between the voter and ballot still exist, but the relationship between the voter and their votes is gone. No one can know how they voted. The key security check on voting integrity is the absolute match between the number of voters in the Vote Roster and the number of ballots counted. If these numbers do not match, either physical ballots were added or removed from the Ballot Counter or "voters" were added or removed from the Vote Roster. In either case, the election has been compromised and the election is nothing more than a lottery. Tens of thousands of Vote Roster entries were undeniably purged and other tens of thousand of entries apparently created out of thin air, using the ES&S EMS system.

12. Equally troubling in Dallas County and the ES&S System is the apparent ease of targeting within the system of certain groups for purging. Over 92% of PURGED In-Person and Absentee voters were over 65. This makes clear the system is easily manipulated by inside or outside actors and this is the system used in much of Arizona, especially in Pima Co.

Who Purged the Baby Boomers?



Purged Voters by Age Source: Dallas County Election Department Vote Rosters Oct 7-Oct 30

13. Where ES&S is concerned, a statistical red flag can be observed in Pima County where public data reveals 66 percent of precincts (164 of 248) contain voter turn-out above 80%, according to county records. Further if these public data votes were normalized to 80% turnout (still 2%+/- above any previous turnout), the excess votes are at least 32,374 over the maximum that could be expected. A sample of this is shown in the table below.

2020 Precinct	2020 Voter Turnout
Pima - Precinct 145	95%
Pima - Precinct 205	94%
Pima - Precinct 216	93%
Pima - Precinct 186	93%
Pima - Precinct 200	93%
Pima - Precinct 195	93%
Pima - Precinct 74	93%
Pima - Precinct 127	93%
Pima - Precinct 172	93%
Pima - Precinct 77	92%
Pima - Precinct 169	92%
Pima - Precinct 207	92%
Pima - Precinct 228	92%
Pima - Precinct 187	92%
Pima - Precinct 213	92%
Pima - Precinct 84	92%
Pima - Precinct 194	92%
Pima - Precinct 193	92%
Pima - Precinct 125	92%

Pima - Precinct 220	92%
Pima - Precinct 173	92%
Pima - Precinct 210	92%
Pima - Precinct 141	91%
Pima - Precinct 212	91%
Pima - Precinct 12	91%
Pima - Precinct 131	91%
Pima - Precinct 106	91%
Pima - Precinct 240	91%
Pima - Precinct 61	91%
Pima - Precinct 199	91%
Pima - Precinct 171	91%
Pima - Precinct 56	91%
Pima - Precinct 46	91%
Pima - Precinct 184	91%
Pima - Precinct 241	91%

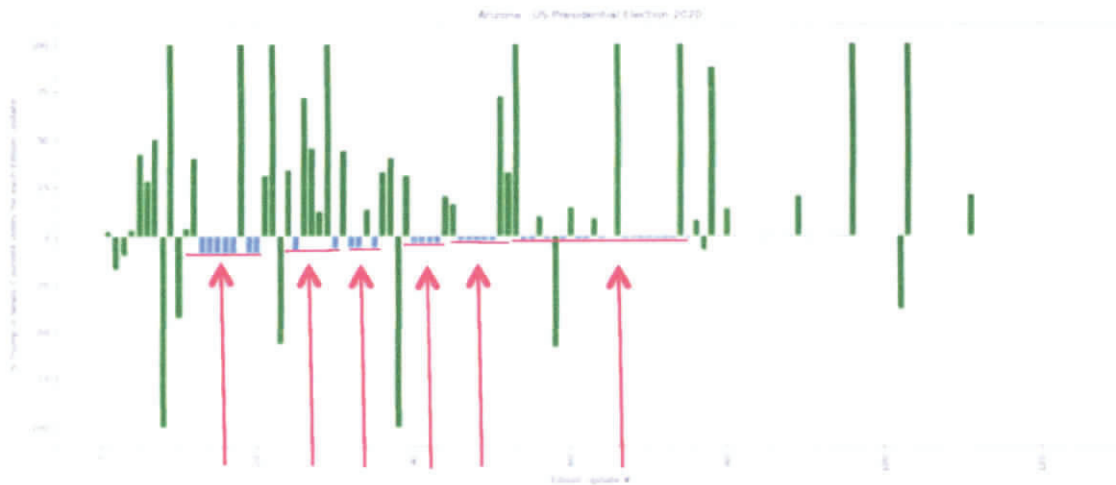
14. A similar outcome can be seen in many precincts in Maricopa County where Dominion is the EMS service provider. Here, public data reveals 54 percent of precincts (300 of 558) contain voter turn-out above 80%, according to county records. Further if these public data votes were normalized to 80% turnout (still 2%+/- above any previous turnout), the excess votes are at least 68,350 over the maximum that could be expected. A sample of this is shown in the table below.

2020 Precinct	2020 Voter Turnout
Maricopa - OVAL	94%
Maricopa - GRAND	94%
Maricopa - RIMROCK	93%
Maricopa - BLACK GOLD	93%
Maricopa - LA SOLANA	93%
Maricopa - PALISADES	93%
Maricopa - SOLCITO	92%
Maricopa - BILTMORE	92%
Maricopa - GRAYHAWK	92%
Maricopa - TERRAVITA	92%
Maricopa - WILDER	92%
Maricopa - SAGUARO	92%
Maricopa - VISTANCIA	92%
Maricopa - AVIANO	92%
Maricopa - FESTIVAL	91%
Maricopa - DEL JOYA	91%
Maricopa - PEAK VIEW	91%
Maricopa - CAREFREE	91%
Maricopa - ALEXANDER	91%
Maricopa - CLIFFVIEW	91%
Maricopa - NORTON	91%
Maricopa - CALAVEROS	91%

Maricopa - CANYON	91%
Maricopa - SKY HAWK	91%
Maricopa - WESTBROOK	91%
Maricopa - EASTMARK	91%
Maricopa - BLUE SKY	91%
Maricopa - RIO VERDE	91%
Maricopa - WOLF RUN	91%
Maricopa - ALPACA	91%

Together, these 2 red flag anomalies account for 100,724 votes that must be regarded with deep suspicion, especially in light of the known and published, demonstrable vulnerabilities of both election systems as shown in other areas.

15. The following data strongly suggests that the additive algorithm (a feature enhancement referred to as “ranked choice voting algorithm” or “RCV”) was activated in the code as shown in the Democracy Suite EMS Results Tally and Reporting User Guide, Chapter 11, Settings 11.2.2. It reads in part, **“RCV METHOD: This will select the specific method of tabulating RCV votes to elect a winner.”** For instance, blank ballots can be entered into the system and treated as “write-ins.” Then the operator can enter an allocation of the write-ins among candidates as he or she wishes. The result then awards the winner based on “points” that the algorithm computes, not actual voter votes. The fact that we observed the percentage of the votes submitted in each batch that went towards a candidate remain unchanged for a series of time and for a number of *consecutive* batches is extremely concerning. In the following graph, the Blue votes indicate the percentage of the batch that went for Biden in Arizona according to the Edison data reported to the NYT. The red lines and arrows indicate the impossible consistencies. The statistical impossibility of the consistent percentage reported to Biden approaches zero. This makes clear an algorithm in the election system is allocating votes based on a percentage.

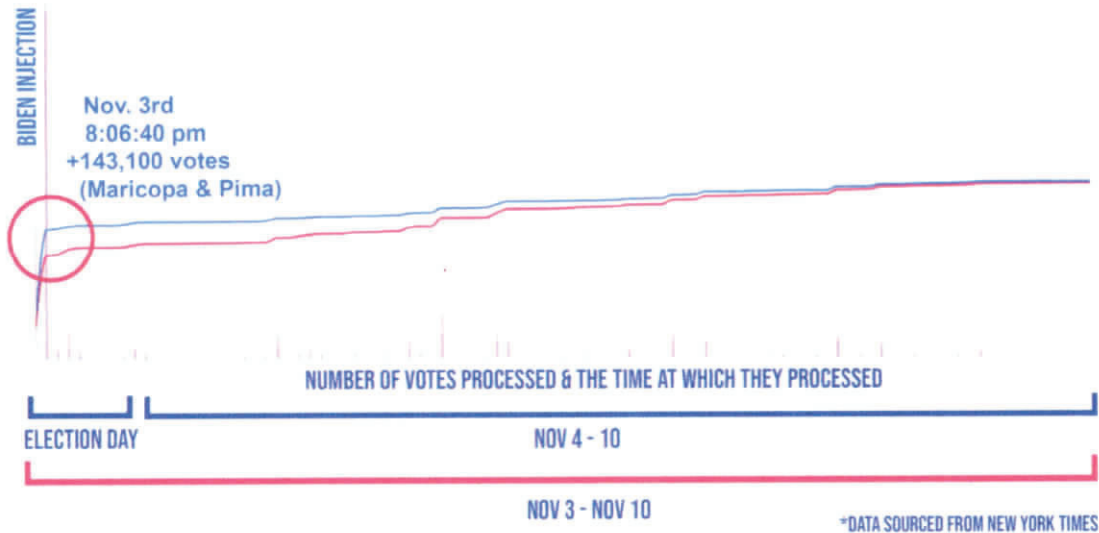


Impossible consistency in percentage of votes counted

16. Yet another statistical red flag in Arizona starts with an improbable, and possibly impossible spike in processed votes. A time series and location specific

analysis would determine whether the equipment on hand at any location would have even been capable of processing this many ballots in the time represented. In Michigan, we have already observed this phenomenon, even though it was physically impossible.

ARIZONA "FIXING" THE VOTE

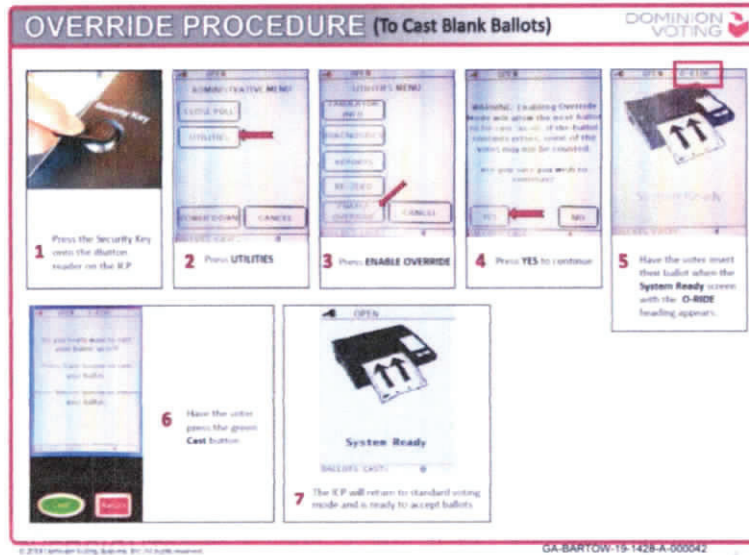


SUMMARY

- Mathematical evidence of the seeding "injection" of votes at the beginning
- A spike means that a large number of votes were injected into the totals
- A normal vote pattern would look like a natural progression – smooth without extreme jumps

This spike, cast almost exclusively for Biden, could easily be explained by the Dominion EMS control system by pre-loading batches of blank ballots in files such as Write-Ins or other adjudication-type files then casting them almost all for Biden using the Override Procedure (to cast Write-In, Blank, or Error ballots) that is available to the operator of the system. A few batches of blank ballots electronically pre-loaded into the adjudication files could easily produce a processed ballot stream this extreme so that actual paper ballots would not be needed until later to create "corroboration" for the electronic count. In this case, the first step would be to forensically test samples of paper ballots to determine if the ballots were real or fraudulently manufactured.

Dominion also has a "Blank Ballot Override" function. Essentially a save for later bucket that can be manually populated later.



14. Based on the foregoing, it is my opinion these statistical anomalies and impossibilities compels the conclusion to a reasonable degree of professional certainty that the vote count in Arizona, in particular Maricopa and Pima counties for candidates for President contain at least 100,724 illegal votes that must be disregarded.

I declare, under the penalty of perjury, that the foregoing is correct.


Russell James Ramsland, Jr.

12/1/2020
Date

EXHIBIT 18



TLP:WHITE

Product ID: AA20-304A

October 30, 2020

Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data

SUMMARY

This advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the [ATT&CK for Enterprise](#) framework for all referenced threat actor techniques.

This joint cybersecurity advisory was coauthored by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI). CISA and the FBI are aware of an Iranian advanced persistent threat (APT) actor targeting U.S. state websites—to include election websites. CISA and the FBI assess this actor is responsible for the mass dissemination of voter intimidation emails to U.S. citizens and the dissemination of U.S. election-related disinformation in mid-October 2020.¹ (Reference FBI FLASH message ME-000138-TT, disseminated October 29, 2020). Further evaluation by CISA and the FBI has identified the targeting of U.S. state election websites was an intentional effort to influence and interfere with the 2020 U.S. presidential election.

TECHNICAL DETAILS

Analysis by CISA and the FBI indicates this actor scanned state websites, to include state election websites, between September 20 and September 28, 2020, with the Acunetix vulnerability scanner (*Active Scanning: Vulnerability Scanning [T1595.002]*). Acunetix is a widely used and legitimate web scanner, which has been used by threat actors for nefarious purposes. Organizations that do not regularly use Acunetix should monitor their logs for any activity from the program that originates from IP addresses provided in this advisory and consider it malicious reconnaissance behavior.

Additionally, CISA and the FBI observed this actor attempting to exploit websites to obtain copies of voter registration data between September 29 and October 17, 2020 (*Exploit Public-Facing*

¹ See FBI FLASH, ME-000138-TT, disseminated 10/29/20, <https://www.ic3.gov/Media/News/2020/201030.pdf>. This disinformation (hereinafter, “the propaganda video”) was in the form of a video purporting to misattribute the activity to a U.S. domestic actor and implies that individuals could cast fraudulent ballots, even from overseas. <https://www.odni.gov/index.php/newsroom/press-releases/item/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security>.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI’s 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.dhs.gov.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see <https://us-cert.cisa.gov/tlp>.

TLP: WHITE

Application [T1190]). This includes attempted exploitation of known vulnerabilities, directory traversal, Structured Query Language (SQL) injection, web shell uploads, and leveraging unique flaws in websites.

CISA and the FBI can confirm that the actor successfully obtained voter registration data in at least one state. The access of voter registration data appeared to involve the abuse of website misconfigurations and a scripted process using the cURL tool to iterate through voter records. A review of the records that were copied and obtained reveals the information was used in the propaganda video.

CISA and FBI analysis of identified activity against state websites, including state election websites, referenced in this product cannot all be fully attributed to this Iranian APT actor. FBI analysis of the Iranian APT actor's activity has identified targeting of U.S. elections' infrastructure (*Compromise Infrastructure* [T1584]) within a similar timeframe, use of IP addresses and IP ranges – including numerous virtual private network (VPN) service exit nodes – which correlate to this Iran APT actor (*Gather Victim Host Information* [T1592]), and other investigative information.

Reconnaissance

The FBI has information indicating this Iran-based actor attempted to access PDF documents from state voter sites using advanced open-source queries (*Search Open Websites and Domains* [T1539]). The actor demonstrated interest in PDFs hosted on URLs with the words “vote” or “voter” and “registration.” The FBI identified queries of URLs for election-related sites.

The FBI also has information indicating the actor researched the following information in a suspected attempt to further their efforts to survey and exploit state election websites.

- YOURLS exploit
- Bypassing ModSecurity Web Application Firewall
- Detecting Web Application Firewalls
- SQLmap tool

Acunetix Scanning

CISA's analysis identified the scanning of multiple entities by the Acunetix Web Vulnerability scanning platform between September 20 and September 28, 2020 (*Active Scanning: Vulnerability Scanning* [T1595.002]).

The actor used the scanner to attempt SQL injection into various fields in `/registration/registration/details` with status codes 404 or 500:

```
/registration/registration/details?addresscity=-1 or 3*2<(0+5+513-513) --  
&addressstreet1=xxxxx&btbeginregistration=begin voter  
registration&btnnextelectionworkerinfo=next&btnnextpersonalinfo=next&btnnextresde  
tails=next&btnnextvoterinformation=next&btsubmit=submit&chkageverno=on&chkagever  
yes=on&chkcitizenno=on&chkcitizenyes=on&chkdisabledvoter=on&chkelectionworker=on&  
chkresprivate=1&chkstatecancel=on&dlnumber=1&dob=xxxx/x/x&email=sample@email.tst&
```

```
firstname=xxxxx&gender=radio&hdnaddresscity=&hdngender=&last4ssn=xxxxx&lastname=x  
xxxxinjeuee&mailaddresscountry=sample@xxx.xxx&mailaddressline1=sample@email.tst&  
mailaddressline2=sample@xxx.xxx&mailaddressline3=sample@xxx.xxx&mailaddressstate=  
aa&mailaddresszip=sample@xxxx.xxx&mailaddresszipex=sample@xxx.xxx&middlename=xxxx  
x&overseas=1&partycode=a&phoneno1=xxx-xxx-xxxx&phoneno2=xxx-xxx-  
xxxx&radio=consent&statecancelcity=xxxxxxx&statecancelcountry=usa&statecancelstat  
e=XXaa&statecancelzip=xxxxx&statecancelzipext=xxxxx&suffixname=esq&txtmailaddress  
city=sample@xxx.xxx
```

Requests

The actor used the following requests associated with this scanning activity.

```
2020-09-26 13:12:56 x.x.x.x GET /x/x v[$acunetix]=1 443 - x.x.x.x  
Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+(KHTML,+like+Gecko)+Chrome/41.  
0.2228.0+Safari/537.21 - 200 0 0 0
```

```
2020-09-26 13:13:19 X.X.x.x GET /x/x voterid[$acunetix]=1 443 - x.x.x.x  
Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+(KHTML,+like+Gecko)+Chrome/41.  
0.2228.0+Safari/537.21 - 200 0 0 1375
```

```
2020-09-26 13:13:18 .X.x.x GET /x/x voterid=;print(md5(acunetix_wvs_security_test));  
443 - X.X.x.x
```

User Agents Observed

CISA and FBI have observed the following user agents associated with this scanning activity.

```
Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+(KHTML,+like+Gecko)+Chrome  
/41.0.2228.0+Safari/537.21 - 500 0 0 0
```

```
Mozilla/5.0+(X11;+U;+Linux+x86_64;+en-  
US;+rv:1.9b4)+Gecko/2008031318+Firefox/3.0b4
```

```
Mozilla/5.0+(X11;+U;+Linux+i686;+en-  
US;+rv:1.8.1.17)+Gecko/20080922+Ubuntu/7.10+(gutsy)+Firefox/2.0.0.17
```

Exfiltration

Obtaining Voter Registration Data

Following the review of web server access logs, CISA analysts, in coordination with the FBI, found instances of the cURL and FDM User Agents sending GET requests to a web resource associated with voter registration data. The activity occurred between September 29 and October 17, 2020. Suspected scripted activity submitted several hundred thousand queries iterating through voter

TLP:WHITE

identification values, and retrieving results with varying levels of success [*Gather Victim Identity Information* (T1589)]. A sample of the records identified by the FBI reveals they match information in the aforementioned propaganda video.

Requests

The actor used the following requests.

```
2020-10-17 13:07:51 x.x.x.x GET /x/x voterid=XXXX1 443 - x.x.x.x curl/7.55.1 - 200 0 0 1406
```

```
2020-10-17 13:07:55 x.x.x.x GET /x/x voterid=XXXX2 443 - x.x.x.x curl/7.55.1 - 200 0 0 1390
```

```
2020-10-17 13:07:58 x.x.x.x GET /x/x voterid=XXXX3 443 - x.x.x.x curl/7.55.1 - 200 0 0 1625
```

```
2020-10-17 13:08:00 x.x.x.x GET /x/x voterid=XXXX4 443 - x.x.x.x curl/7.55.1 - 200 0 0 1390
```

Note: incrementing voterid values in cs_uri_query field

User Agents

CISA and FBI have observed the following user agents.

```
FDM+3.x
```

```
curl/7.55.1
```

```
Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 - 500 0 0 0
```

```
Mozilla/5.0+(X11;+U;+Linux+x86_64;+en-US;+rv:1.9b4)+Gecko/2008031318+Firefox/3.0b4
```

See figure 1 below for a timeline of the actor's malicious activity.

TECHNICAL FINDINGS

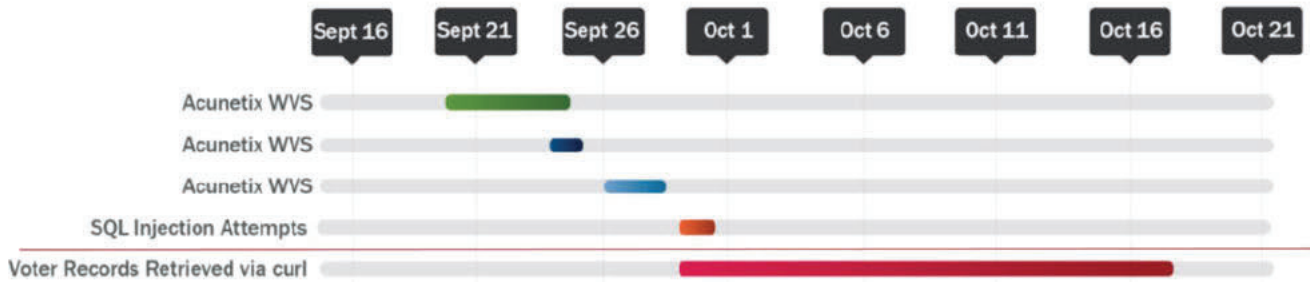


Figure 1: Overview of malicious activity

MITIGATIONS

Detection

Acunetix Scanning

Organizations can identify Acunetix scanning activity by using the following keywords while performing log analysis.

- `$acunetix`
- `acunetix_wvs_security_test`

Indicators of Compromise

For a downloadable copy of IOCs, see [AA20-304A.stix](#).

Disclaimer: Many of the IP addresses included below likely correspond to publicly available VPN services, which can be used by individuals all over the world. Although this creates the potential for false positives, any activity listed should warrant further investigation. The actor likely uses various IP addresses and VPN services.

The following IPs have been associated with this activity.

- 102.129.239[.]185 (Acunetix Scanning)
- 143.244.38[.]60 (Acunetix Scanning and cURL requests)
- 45.139.49[.]228 (Acunetix Scanning)
- 156.146.54[.]90 (Acunetix Scanning)
- 109.202.111[.]236 (cURL requests)
- 185.77.248[.]17 (cURL requests)
- 217.138.211[.]249 (cURL requests)
- 217.146.82[.]207 (cURL requests)
- 37.235.103[.]85 (cURL requests)
- 37.235.98[.]64 (cURL requests)
- 70.32.5[.]96 (cURL requests)

- 70.32.6[.]20 (cURL requests)
- 70.32.6[.]8 (cURL requests)
- 70.32.6[.]97 (cURL requests)
- 70.32.6[.]98 (cURL requests)
- 77.243.191[.]21 (cURL requests and FDM+3.x (Free Download Manager v3) enumeration/iteration)
- 92.223.89[.]73 (cURL requests)

CISA and the FBI are aware the following IOCs have been used by this Iran-based actor. These IP addresses facilitated the mass dissemination of voter intimidation email messages on October 20, 2020.

- 195.181.170[.]244 (Observed September 30 and October 20, 2020)
- 102.129.239[.]185 (Observed September 30, 2020)
- 104.206.13[.]27 (Observed September 30, 2020)
- 154.16.93[.]125 (Observed September 30, 2020)
- 185.191.207[.]169 (Observed September 30, 2020)
- 185.191.207[.]52 (Observed September 30, 2020)
- 194.127.172[.]98 (Observed September 30, 2020)
- 194.35.233[.]83 (Observed September 30, 2020)
- 198.147.23[.]147 (Observed September 30, 2020)
- 198.16.66[.]139 (Observed September 30, 2020)
- 212.102.45[.]3 (Observed September 30, 2020)
- 212.102.45[.]58 (Observed September 30, 2020)
- 31.168.98[.]73 (Observed September 30, 2020)
- 37.120.204[.]156 (Observed September 30, 2020)
- 5.160.253[.]50 (Observed September 30, 2020)
- 5.253.204[.]74 (Observed September 30, 2020)
- 64.44.81[.]68 (Observed September 30, 2020)
- 84.17.45[.]218 (Observed September 30, 2020)
- 89.187.182[.]106 (Observed September 30, 2020)
- 89.187.182[.]111 (Observed September 30, 2020)
- 89.34.98[.]114 (Observed September 30, 2020)
- 89.44.201[.]211 (Observed September 30, 2020)

Recommendations

The following list provides recommended self-protection mitigation strategies against cyber techniques used by advanced persistent threat actors:

- Validate input as a method of sanitizing untrusted input submitted by web application users. Validating input can significantly reduce the probability of successful exploitation by providing

protection against security flaws in web applications. The types of attacks possibly prevented include SQL injection, Cross Site Scripting (XSS), and command injection.

- Audit your network for systems using Remote Desktop Protocol (RDP) and other internet-facing services. Disable unnecessary services and install available patches for the services in use. Users may need to work with their technology vendors to confirm that patches will not affect system processes.
- Verify all cloud-based virtual machine instances with a public IP, and avoid using open RDP ports, unless there is a valid need. Place any system with an open RDP port behind a firewall and require users to use a VPN to access it through the firewall.
- Enable strong password requirements and account lockout policies to defend against brute-force attacks.
- Apply multi-factor authentication, when possible.
- Maintain a good information back-up strategy by routinely backing up all critical data and system configuration information on a separate device. Store the backups offline, verify their integrity, and verify the restoration process.
- Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- Ensure third parties that require RDP access follow internal remote access policies.
- Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.
- Regulate and limit external to internal RDP connections. When external access to internal resources is required, use secure methods, such as a VPNs. However, recognize the security of VPNs matches the security of the connected devices.
- Use security features provided by social media platforms; use [strong passwords](#), change passwords frequently, and use a different password for each social media account.
- See CISA's Tip on [Best Practices for Securing Election Systems](#) for more information.

General Mitigations

Keep applications and systems updated and patched

Apply all available software updates and patches and automate this process to the greatest extent possible (e.g., by using an update service provided directly from the vendor). Automating updates and patches is critical because of the speed of threat actors to create new exploits following the release of a patch. These "N-day" exploits can be as damaging as zero-day exploits. Ensure the authenticity and integrity of vendor updates by using signed updates delivered over protected links. Without the rapid and thorough application of patches, threat actors can operate inside a defender's patch cycle.²

² NSA "NSA'S Top Ten Cybersecurity Mitigation Strategies" <https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nas-top10-cybersecurity-mitigation-strategies.pdf>

Additionally, use tools (e.g., the OWASP Dependency-Check Project tool³) to identify the publicly known vulnerabilities in third-party libraries depended upon by the application.

Scan web applications for SQL injection and other common web vulnerabilities

Implement a plan to scan public-facing web servers for common web vulnerabilities (e.g., SQL injection, cross-site scripting) by using a commercial web application vulnerability scanner in combination with a source code scanner.⁴ Fixing or patching vulnerabilities after they are identified is especially crucial for networks hosting older web applications. As sites get older, more vulnerabilities are discovered and exposed.

Deploy a web application firewall

Deploy a web application firewall (WAF) to prevent invalid input attacks and other attacks destined for the web application. WAFs are intrusion/detection/prevention devices that inspect each web request made to and from the web application to determine if the request is malicious. Some WAFs install on the host system and others are dedicated devices that sit in front of the web application. WAFs also weaken the effectiveness of automated web vulnerability scanning tools.

Deploy techniques to protect against web shells

Patch web application vulnerabilities or fix configuration weaknesses that allow web shell attacks, and follow guidance on detecting and preventing web shell malware.⁵ Malicious cyber actors often deploy web shells—software that can enable remote administration—on a victim's web server. Malicious cyber actors can use web shells to execute arbitrary system commands commonly sent over HTTP or HTTPS. Attackers often create web shells by adding or modifying a file in an existing web application. Web shells provide attackers with persistent access to a compromised network using communications channels disguised to blend in with legitimate traffic. Web shell malware is a long-standing, pervasive threat that continues to evade many security tools.

Use multi-factor authentication for administrator accounts

Prioritize protection for accounts with elevated privileges, remote access, or used on high-value assets.⁶ Use physical token-based authentication systems to supplement knowledge-based factors such as passwords and personal identification numbers (PINs).⁷ Organizations should migrate away from single-factor authentication, such as password-based systems, which are subject to poor user

³ <https://owasp.org/www-project-dependency-check/>

⁴ NSA "Defending Against the Exploitation of SQL Vulnerabilities to Compromise a Network" <https://apps.nsa.gov/iaarchive/library/ia-guidance/tech-briefs/defending-against-the-exploitation-of-sql-vulnerabilities-to-cfm>

⁵ NSA & ASD "CyberSecurity Information: Detect and Prevent Web Shell Malware" <https://media.defense.gov/2020/Jun/09/2002313081/-1/-1/0/CSI-DETECT-AND-PREVENT-WEB-SHELL-MALWARE-20200422.PDF>

⁶ <https://us-cert.cisa.gov/cdm/event/Identifying-and-Protecting-High-Value-Assets-Closer-Look-Governance-Needs-HVAs>

⁷ NSA "NSA'S Top Ten Cybersecurity Mitigation Strategies" <https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csi-nas-top-10-cybersecurity-mitigation-strategies.pdf>

choices and more susceptible to credential theft, forgery, and password reuse across multiple systems.

Remediate critical web application security risks

First, identify and remediate critical web application security risks. Next, move on to other less critical vulnerabilities. Follow available guidance on securing web applications.^{8,9,10}

How do I respond to unauthorized access to election-related systems?

Implement your security incident response and business continuity plan

It may take time for your organization's IT professionals to isolate and remove threats to your systems and restore normal operations. In the meantime, take steps to maintain your organization's essential functions according to your business continuity plan. Organizations should maintain and regularly test backup plans, disaster recovery plans, and business continuity procedures.

Contact CISA or law enforcement immediately

To report an intrusion and to request incident response resources or technical assistance, contact CISA (Central@cisa.gov or 888-282-0870) or the FBI through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov or 855-292-3937).

RESOURCES

- CISA Tip: [Best Practices for Securing Election Systems](#)
- CISA Tip: [Securing Voter Registration Data](#)
- CISA Tip: [Website Security](#)
- CISA Tip: [Avoiding Social Engineering and Phishing Attacks](#)
- CISA Tip: [Securing Network Infrastructure Devices](#)
- Joint Advisory: [Technical Approaches to Uncovering and Remediating Malicious Activity](#)
- CISA Insights: [Actions to Counter Email-Based Attacks on Election-related Entities](#)
- FBI and CISA Public Service Announcement (PSA): [Spoofed Internet Domains and Email Accounts Pose Cyber and Disinformation Risks to Voters](#)
- FBI and CISA PSA: [Foreign Actors Likely to Use Online Journals to Spread Disinformation Regarding 2020 Elections](#)
- FBI and CISA PSA: [Distributed Denial of Service Attacks Could Hinder Access to Voting Information, Would Not Prevent Voting](#)
- FBI and CISA PSA: [False Claims of Hacked Voter Information Likely Intended to Cast Doubt on Legitimacy of U.S. Elections](#) FBI and CISA PSA: [Cyber Threats to Voting Processes Could Slow But Not Prevent Voting](#)

⁸ NSA "Building Web Applications – Security for Developers" <https://apps.nsa.gov/iaarchive/library/ia-guidance/security-tips/building-web-applications-security-recommendations-for.cfm>

⁹ <https://owasp.org/www-project-top-ten/>

¹⁰

https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

CYBERSECURITY ADVISORY

TLP:WHITE

FBI | CISA

- FBI and CISA PSA: [Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results](#)

TLP: WHITE

EXHIBIT 19

Declaration of Matthew Bromberg Ph.D

December 1, 2020

Pursuant to 28 U.S.C Section 1746, I, Matthew Bromberg, make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. Matthew Bromberg has a Ph.D in Electrical Engineering from the University of California at Davis and a Masters degree in Mathematics from the University of California at Berkeley. I have been employed, for over 28 years, in the signal processing and wireless signal processing domain, with an emphasis on statistical signal processing. I have published numerous journal and conference articles. Additionally, I have held Top Secret and SAP clearances and I am an inventor of nearly 30 patents, one of which has over 1000 citations in the field of MIMO communications (Multiple Input Multiple Output).
3. I reside at 4303 West Eaglerock Pl., Wenatchee WA, 98801.
4. Given the data sources referenced in this document, I assert that in Georgia, Pennsylvania and the city of Milwaukee, a simple statistical model of vote fraud is a better fit to the sudden jump in Biden vote percentages among absentee ballots received later in the counting process of the 2020 presidential election. It is also a better fit when constrained to a single large Metropolitan area such as Milwaukee..
5. Given the same data sources, I also assert that Milwaukee precincts exhibit statistical anomalies that are not normally present in fair elections.. The fraud model hypothesis in Milwaukee has a posterior probability of 100% to machine precision. This model predicts 105,639 fraudulent Biden ballots in Milwaukee.
6. I assert that the data suggests aberrant statistical anomalies in the vote counts in Michigan, when observed as a function of time.
7. I assert that the data implies statistical anomalies supportive of vote switching in Maricopa county Arizona.

Signature:

Supporting evidence for the assertions in (4) and 5 is provided in the following pages.

1 Impact of Fraud on the Election

In the analysis that follows, it is possible to obtain rough estimates on how vote fraud could possibly have effected the election. In Georgia, there is evidence that votes were actually switched from Trump to Biden. As many as 51,110 Biden votes were fraudulent and as many as 51,110 votes could be added to Trump. An audit to determine vote switching will be more difficult, since it is likely the Trump ballots have been destroyed in Georgia, based on reports of ballots being shredded there. If instead we presume that Bidens fraudulent votes were simply added to the totals, then we estimate that 104,107 ballots should be removed from Biden's totals.

In Pennsylvania, from just one batch of absentee ballots, approximately 72668 of them are estimated to be fraudulent Biden votes. Our analysis of Milwaukee shows that 105,639 Biden ballots could be fraudulent. Moreover there is evidence of vote switching here, which might give as many as 42365 additional ballots to Trump, and remove the same from Biden.

Michigan yields an estimate of 237,140 fraudulent Biden votes added to the total, using conservative estimates of the Biden percentage among the new ballots.

2 Statistical Model

The simplest statistical model for computing the probabilities for an election outcome is a binomial distribution, which assigns a probability p for a given person within the population to select a candidate. If we assume that each person chooses their candidate independently, then we obtain the Binomial distribution in the form,

$$P(k|N) \equiv {}_N C_k p^k (1-p)^{N-k}, \quad (1)$$

where $P(k|N)$ is the probability that you observe k votes for a candidate in a population of N voters, and where ${}_N C_k$ is the number of ways to choose k people out of a group of N people.

For larger N , the binomial distribution can be approximated by a Gaussian distribution, which is used in the election fraud analysis in [1]. The chief reason for this is the difficulty of computing $P(k|N)$ for large N and k . However this problem can be overcome by computing the probabilities in the log domain and using the log beta function to compute ${}_N C_k$.

For this analysis it is more useful to compute the probabilities as a function of f the observed fraction of the candidate's votes. In this formulation we have $k = Nf$, and $N - k = N(1 - f)$, and therefore we define the fractional probability as,

$$B_N(f) \equiv {}_N C_{Nf} p^{Nf} (1-p)^{N(1-f)}. \quad (2)$$

2.1 Fraud Model

To model voting fraud we assume a fixed fraction α of votes are given to the cheater. The pool of available voters who actually voted is now $N(1 - \alpha)$. The fraction who actually voted for the cheater is given by $f - \alpha$. The probability that the fraction f voters reported for the cheater, with the fraction α stolen, can therefore be written as,

$$C_{N,\alpha}(f) \equiv B_{N(1-\alpha)}(f - \alpha). \quad (3)$$

This is similar to the fraud model used in the election fraud analysis given in [1]. We use the Binomial distribution directly, rather than the Gaussian distribution, since it should be more accurate for small N, k or f .

2.2 Posterior Probability of Fraud Model

A hypothesis test can now be set up between the standard voting statistics of (2) vs the statistics of the fraud model (3). If we use Bayesian inference we can compute an estimate of the posterior probability of the fraud model. This can be written as,

$$P(F|f) = \frac{C_{N,\alpha}(f)p_F}{C_{N,\alpha}(f)p_F + B_N(f)(1-p_F)},$$

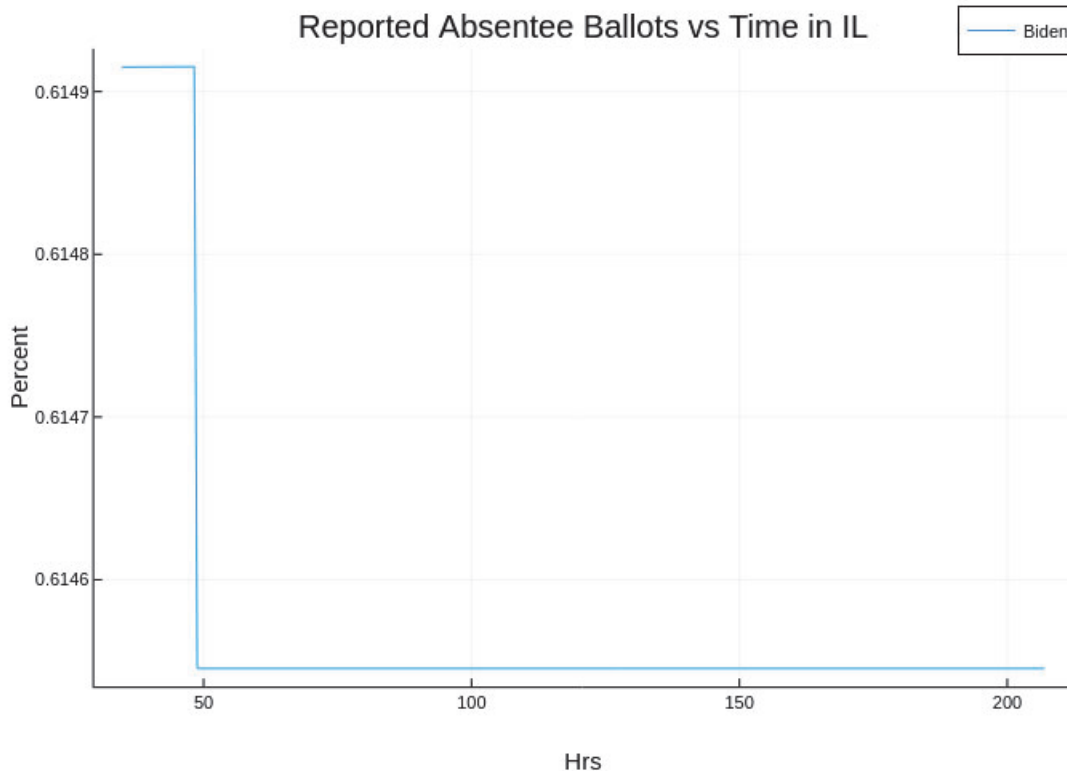


Figure 1: Reported Biden Fraction In Illinois vs Time

where p_F is the prior probability of fraud. In our investigation we assume fraud is unlikely and set $p_F = 0.01$.

3 Analysis of Absentee Ballots in the 2020 Election

For this analysis we extracted data from the `all_states_timeseries.csv` file, which can be found at the internet url: <https://wiki.audittheelection.com/index.php/Datasets>. We look at the absentee ballot results near the beginning of the time series and then compare it to the end or the middle of the period, after a sufficient enough ballots were added.

For the models in Section 2 we assign the probability p of a Biden vote using the final data. This assumption is actually more favorable to the cheater. As mentioned earlier we set the prior probability of fraud to $p_F = 0.01$, and the cheating fraction, α , is set to $\alpha = f - p$, where f is the observed Biden fraction in the newly added ballots. This isolates the statistics of the added ballots from the final observed statistics.

We focus on the absentee ballots, because they are dominated by large democratic cities and there is no obvious reason why those statistics should change appreciably over time. Furthermore it should be noted that the start time for this data, mid day Nov. 4., was well after some of the larger absentee ballot dumps occurred.

3.1 Control Case Illinois

We choose Illinois as a control case, since it has a significant number of absentee ballots that were counted later and provides a fairly clean baseline. The reported Biden fraction vs time is given in Figure 1.

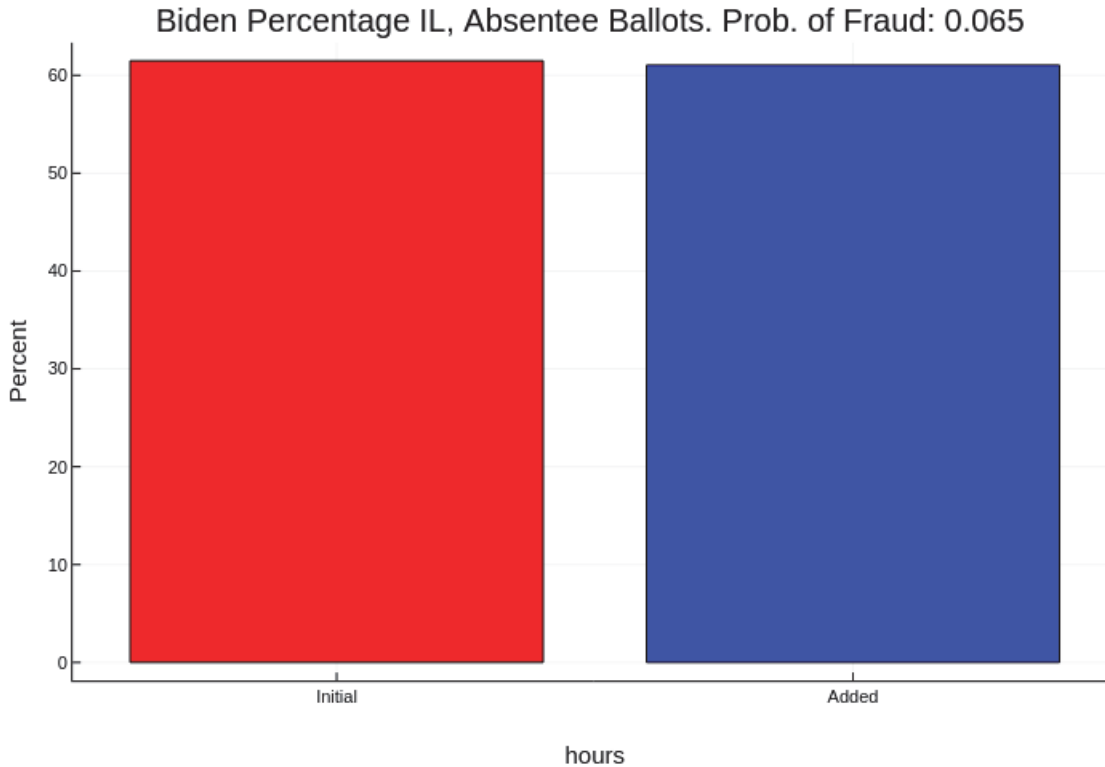


Figure 2: Before and Added Biden Fraction

As we can see there is not much change in the Biden statistics from the initial 601,714 absentee ballots when compared with the 54,117 ballots that were added. This is further shown by the bar chart in Figure 2.

Using our formula for the posterior probability of fraud in (3) we obtain the probability that the fraud model is correct of 6.5%. This lends good support to the idea that the Illinois absentee ballots were counted fairly.

3.2 Analysis of Georgia Absentee Ballots

The Georgia absentee ballot count started at 3,701,005 and 303,988 ballots were added. The Biden fraction among absentee ballots as a function of time is shown in Figure (3). This plot shows a statistical abnormality in that the Biden fraction appears to always be increasing. This is statistically unlikely and is not typically seen in fair elections. Normally you would see a mixture of votes of Biden and his opponents, and would see random deviation around the asymptote.

We investigate this phenomenon more fully in Figure (4). The added ballots have a Biden percentage of around 70%, while the initial statistics were at 50%. This is a very large jump for such a large sample size and seems very unlikely. Indeed the probability that the fraud model is correct is 100%, up to the precision of double floating point arithmetic.

Assuming that the prior absentee ballot distribution is the correct one, we can form a simple prediction for how many of Biden's ballots were fraudulent. Let $N_1 = 303,988$, the number of ballots added, and let $B = 189,497$ be the number of Biden votes in this new batch. If the fraction of Biden votes should actually be $f = 0.509$. Let x be the proposed number of fraudulent Biden votes, then we

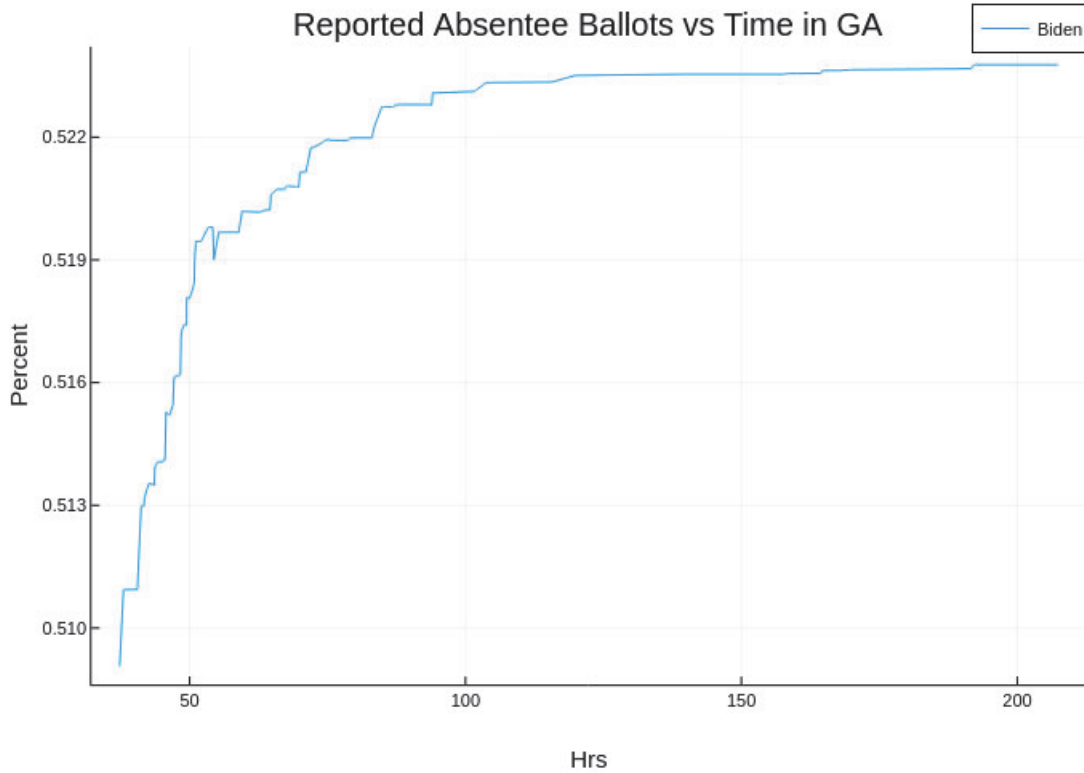


Figure 3: Georgia Absentee Ballots vs Time: (Biden Fraction)

have,

$$\begin{aligned}\frac{B-x}{N_1-x} &= f \\ x &= \frac{B-N_1f}{1-f}.\end{aligned}\quad (4)$$

In the case that votes were actually switched from Trump to Biden, then the formula becomes,

$$\begin{aligned}\frac{B-x}{N_1} &= f \\ x &= B - N_1f\end{aligned}$$

This would suggest that 104,107 ballots were fraudulently manufactured for Biden. If we presume that actually those ballots were switched from Trump to Biden then as many as 19% of the new absentee ballots for Biden were fraudulent, which totals around 51,110 ballots that should be removed from Biden's totals and added to Trump. We shall see in Section 6, that there is substantial evidence that some Trump votes were actually switched to Biden votes.

3.3 Analysis of Pennsylvania Absentee Ballots

The Pennsylvania absentee ballot count started at 785,473 and 319,741 ballots were added at 39 hours after the start of the data record. The Biden fraction among absentee ballots as a function of time is shown in Figure (5). This plot shows some oddities in that the Biden fraction fluctuates with large deviations.

In Figure (6) we see the initial Biden percentage compared with the Biden percentage of the added ballots over the first 39 hours. The added ballots have a Biden percentage of around 83%, while the

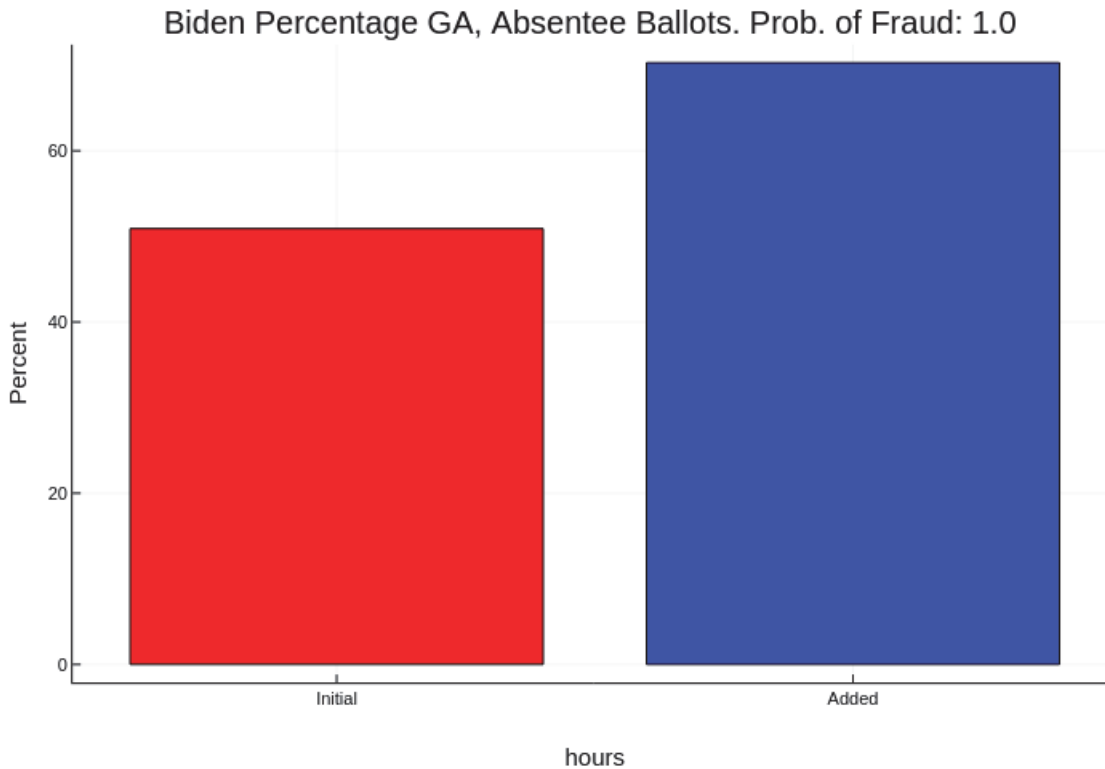


Figure 4: Before and After Biden Fraction in Georgia

initial statistics were at 78%. This is a very large jump for such a large sample size and seems very unlikely. Indeed the probability that the fraud model is correct is 100%, up to the precision of double floating point arithmetic.

If we just examine the initial large batch of votes among the absentee ballots, we see an unexplained jump of 5% for Biden. Although it is likely that most of the fraud, if any, occurred earlier in the vote count, just this batch of ballots suggests that approximately 72668 Biden ballots are fraudulent. If we presume that the votes were stolen from Trump's votes, then 15987 Biden ballots are fraudulent and should be added to Trump's total.

4 Analysis of Milwaukee County in Wisconsin

We now switch our analysis to a data set that contains precinct data for Milwaukee county. The data was obtained from the twitter account of @shylockh, who derived his sources from the New York Times and in some cases from the unofficial precinct reports from the Wisconsin elections commission website. We examine vote percentages for ballots added between Wednesday morning, 11/04/2020 and Thursday night 11/05/2020.

This data set gives the total vote count by party affiliation. Because the data set is confined to Milwaukee, we can assume that the statistics should not be time varying. The voting pool here is highly partisan in favor of democrats and we don't expect any significant difference in the voting percentage, especially since a large number of absentee ballots were already counted by Wednesday morning.

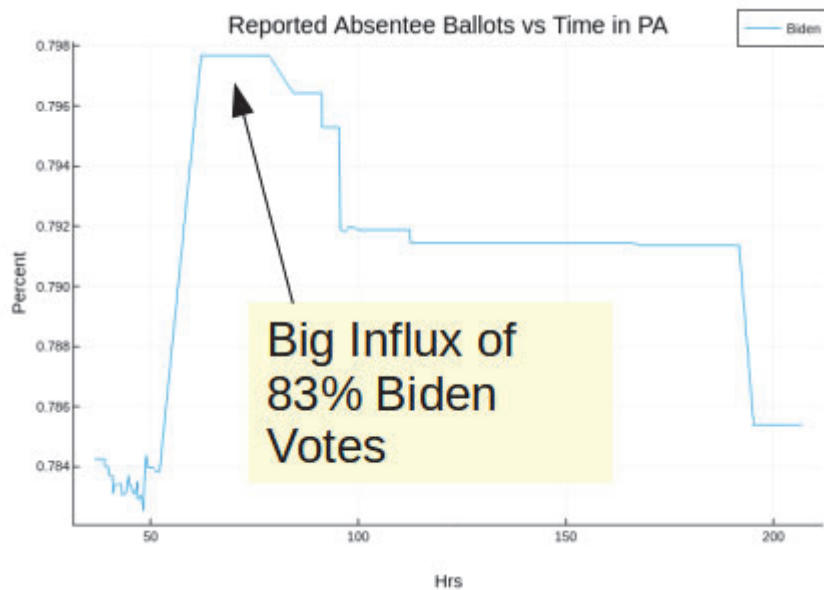


Figure 5: Pennsylvania Absentee Ballots vs Time: (Biden Fraction)

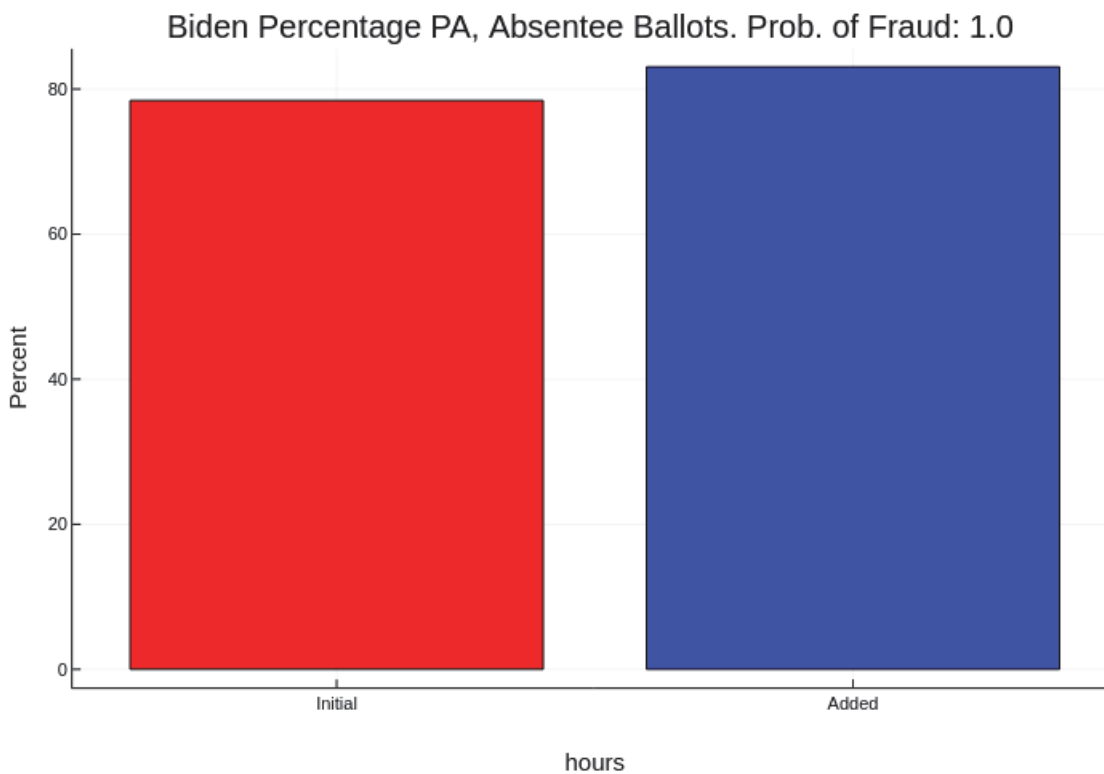


Figure 6: Before and After Biden Fraction in Pennsylvania

4.1 Analysis of Milwaukee County Democrat results

The percentage of democrat voters increases by 15% among the ballots added on Wednesday and Thursday. On Wednesday morning Milwaukee had received 165,776 ballots. By Thursday evening 458,935 ballots were received, adding 293,159 ballots.

In Figure 7 we see the large deviation in democrat percentage between the Wednesday morning and those added by Thursday evening. This too causes the posterior probability of the fraud model to be 100% to machine precision.

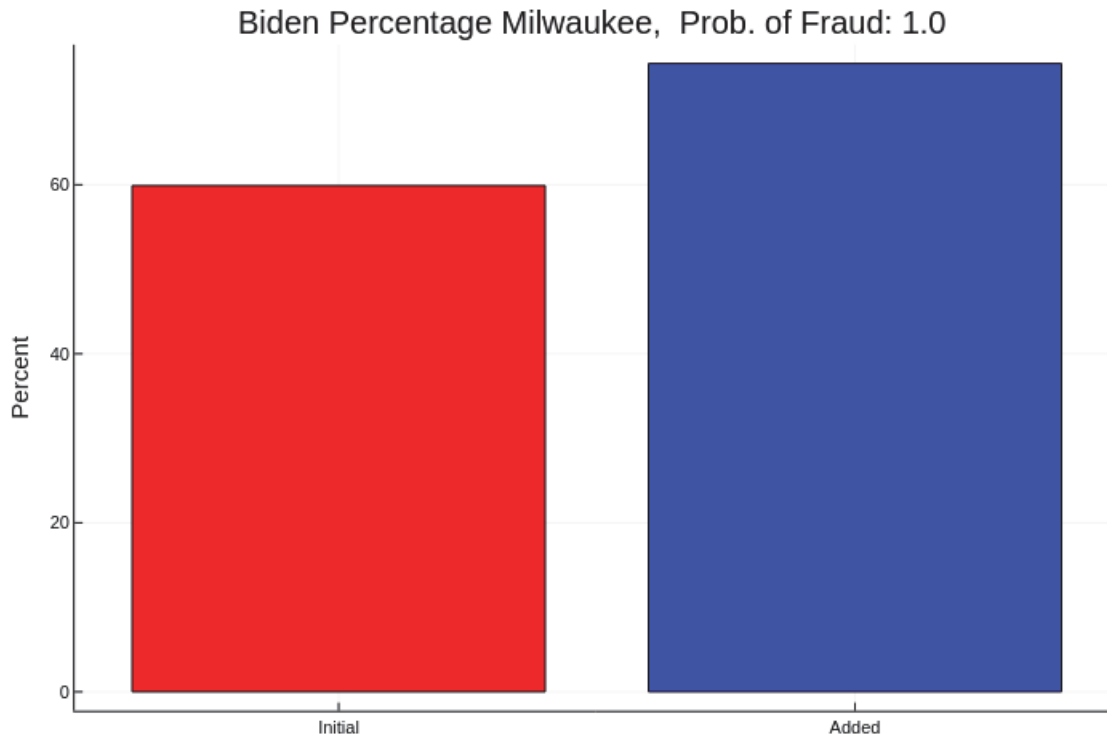


Figure 7: Before and After Democrat Fraction in Milwaukee

Assuming that there was fraud, we estimate that 105,639 fraudulent Biden ballots were added between Wednesday and Thursday of 11/05/2020 in Milwaukee alone. However as we shall see below, many of these votes may well have been switched from Trump to Biden, which would also give Trump an additional 42365 votes and remove 42365 votes from Biden.

4.2 Candidate Percentages Sorted by Ward Size

Another useful tool for evaluating fraud is to look at the cumulative vote percentages sorted by an independent input factor. An easy factor to use is ward or precinct size. This concept was used throughout the report on voter irregularities in [2]. In that report there was an anomalous dependency on precinct size in many of the 2016 primary elections. The larger precincts had introduced the use of voting machines. But one could also theorize the opportunity for cheaters to cheat in small precincts, where there may be less oversight.

Normally we would expect the cumulative vote percentage to converge to an asymptote, and bounce around the mean until convergence. An example of this can be found from the 2000 Florida Democratic presidential primary between Gore and Bradley. This is shown in Figure 8, and is taken from [2].

However when one sorts the Milwaukee, Thursday night data, by precinct size, you will see trend-lines that do not converge to an asymptote, as shown in Figure 9. It appears that smaller precincts

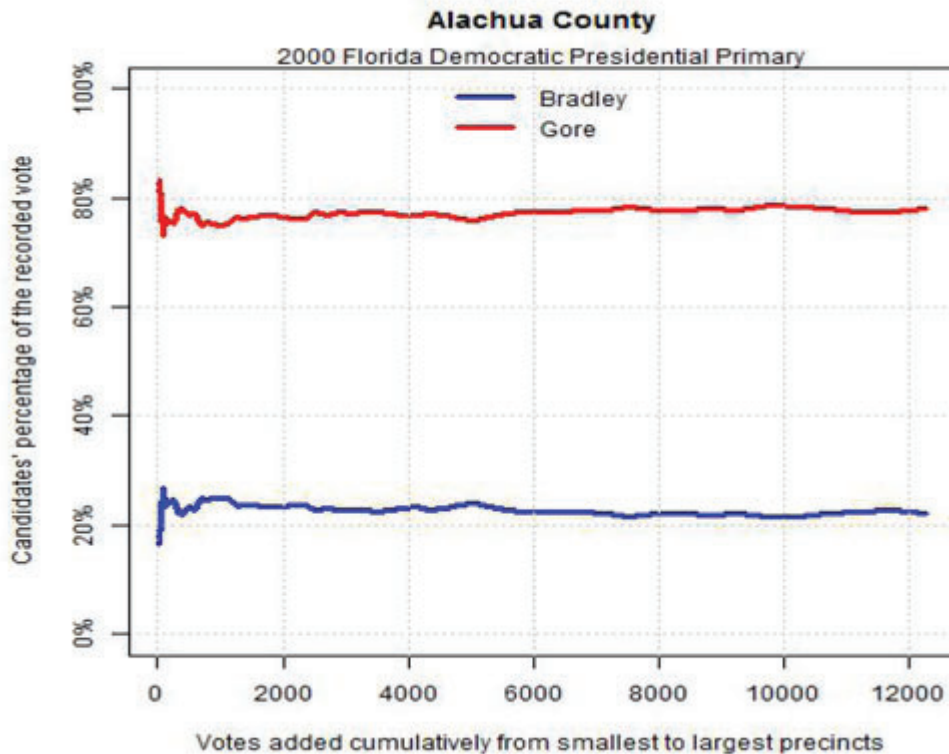


Figure 8: Baseline Cumulative Fractions Sorted by Precinct Size

almost uniformly have higher Democrat percentages. There is no obvious reason for this. It was certainly not seen in the control case in Figure 8. Furthermore the third party percentages quickly converge to their asymptote as would be expected in a fair election. One possible model for this would be vote switching from Trump to Biden, which would show up more strongly in the smaller precincts.

5 Analysis of Third Party Vote Count

Third party voters offer another way to examine a possible fraud mechanism. Votes could either be switched from third party candidates to the cheater, or fraudulent ballots that are added to benefit the cheater, may not include third party choices. For the control example, we look at absentee ballots in the state of Massachusetts. In Massachusetts the initial absentee ballot count was 117,618, and the number of added absentee ballots is 10,281.

The reported 3rd party percentage of absentee ballots vs time in Massachusetts is shown in Figure 10 and the comparison of the initial and added 3rd party ballots in MA is shown in Figure 11. There is only a small change in party preference, relative to the size of the added ballots. Therefore the probability of the fraud model is only 22%.

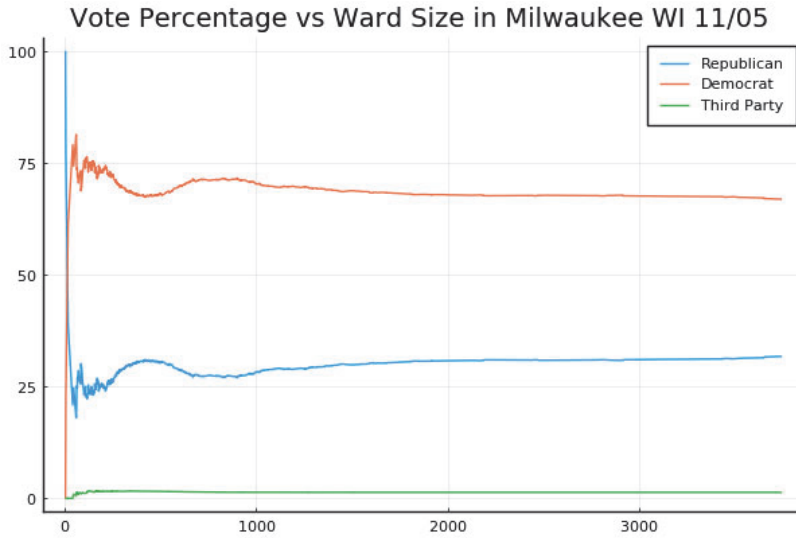


Figure 9: Milwaukee Democrat Ballots Percentage vs Ward Size

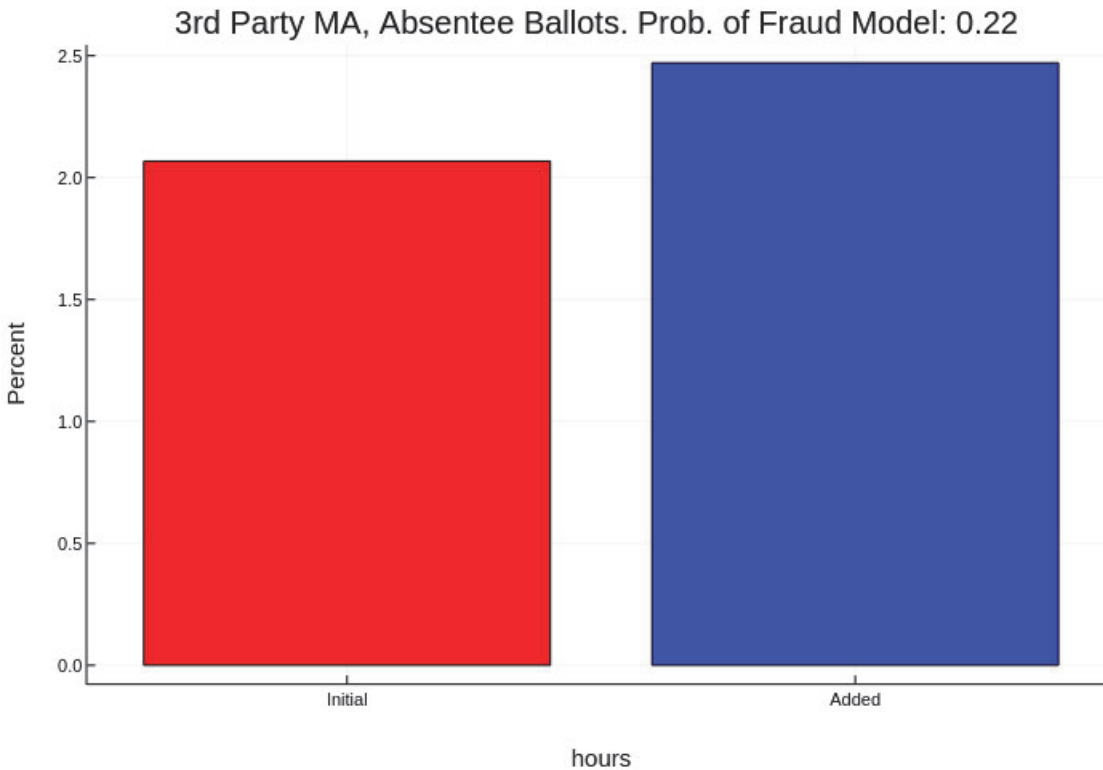


Figure 11: MA 3rd Party Percentage Initial and Added

When we look at the total 3rd party percentages in Milwaukee, between Wednesday morning and Thursday night, we see a significant drop from 1.9 percent to 1.4% for the newly added ballots. But this is among 293,159 added ballots. This is illustrated in Figure 12. Again in this case the fraud model has a posterior probability of 100% to machine precision.

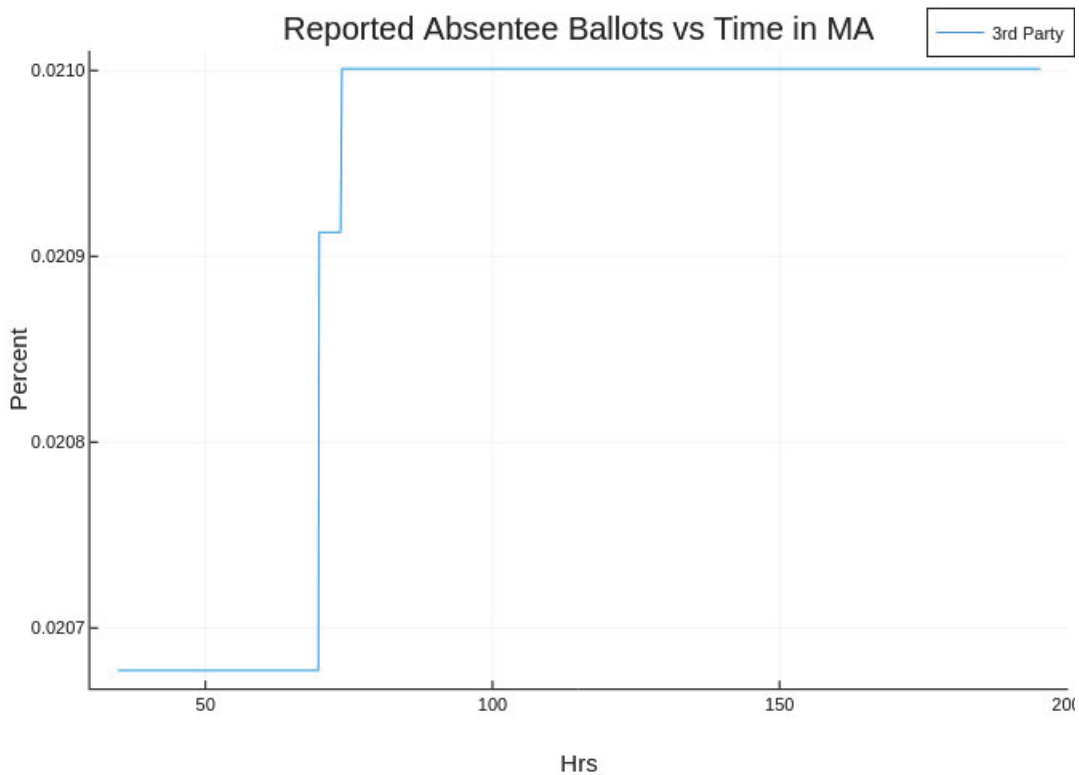


Figure 10: MA 3rd Party Absentee Votes vs Time

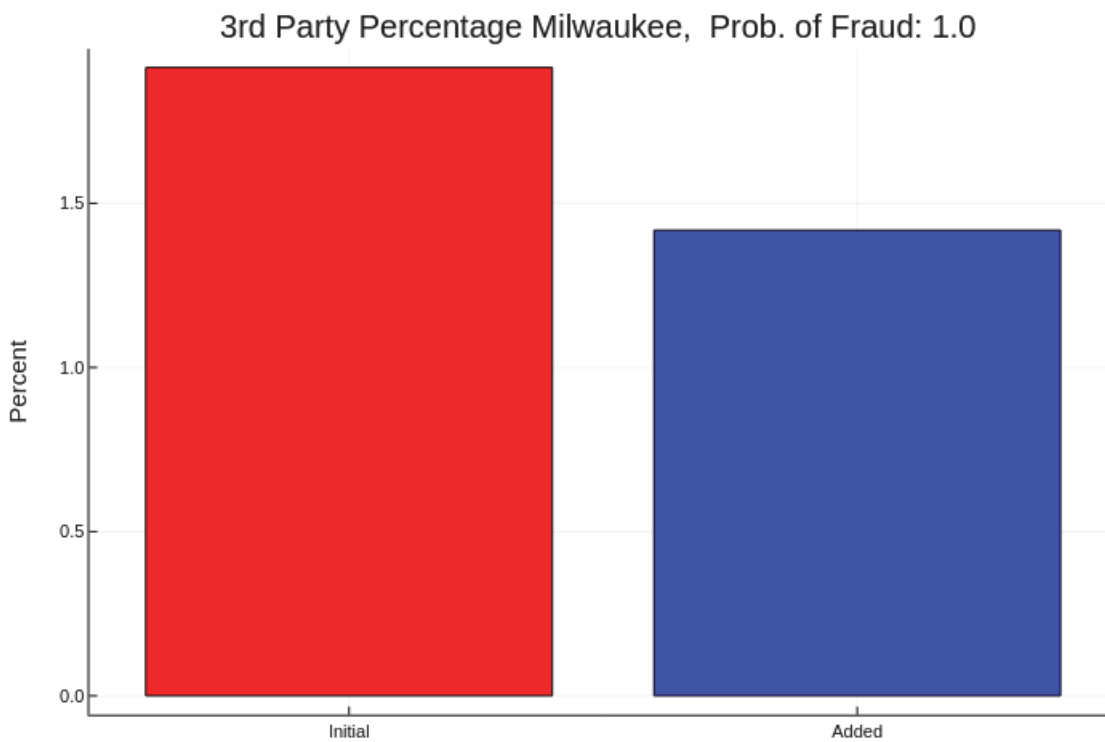


Figure 12: Milwaukee 3rd Party Percentages between Wednesday and Added

6 Analysis of Fulton and DeKalb Counties in Georgia

We perform a precinct level analysis of Fulton and DeKalb counties in Georgia based on an aggregate data set likely culled from the New York Times. The Fulton data was collected on 11/08/2020 and the DeKalb data was collected on 11/09/2020. As in Milwaukee we look at the cumulative vote percentages as a function of precinct size. A plot of this for DeKalb county is shown in Figure 13.

Although there are somewhat concerning trendlines in the beginning, after the size 600 precinct mark, thereafter the overall picture is what one would expect of an election where the voter preferences are not dependent on precinct size. Both DeKalb and Fulton counties are in predominantly urban Atlanta, neighbor one another, and have similar voting preferences across precincts. DeKalb county is still suspect, however, due to the irregularities observed prior to the Ward 600 mark.

Absentee Vote Percentage vs Precinct Size in DeKalb GA 11/0

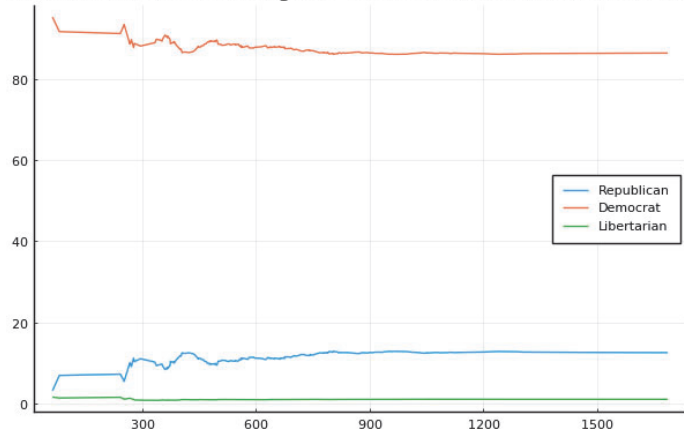


Figure 13: Dekalb County Absentee Ballots: Percentages vs Precinct Size

A different story emerges when we plot the absentee vote percentages for Fulton county as a function of precinct size, as can be seen in Figure 14. Here the trendlines for the Democrat and Republican percentages are quite pronounced, amounting to a difference of 8 percent from the halfway mark.

We divide the Fulton county data into a group of smaller precincts and larger precincts. One group has precincts less than 308 and another larger than 308. The total absentee ballots for the small group is 24,575, and the large group is 120,029. The small group has a Democrat percentage of 85% and the large group has a percentage of 77%, for a change of 8%. The fraud model is preferred in this scenario again with probability of 100% to machine precision.

One might presume that small precincts generally favor Democrats over large precincts, biasing the results. However take a closer look at the Libertarian party results in Fulton county in Figure 15. The percentages are exactly what we would expect if there were no bias in precinct size. The percentages bounce around a mean, not trending in any direction.

So if there were a bias favoring the democrats in small precincts, we would expect that to effect both the Republican and Libertarian totals. However it appears to only effect Republican totals, as if the Republican ballots were switched over to Democrat in a higher percentage in the smaller precincts. Indeed if a fixed number of ballots are switched in each district, it would have a larger effect in the smaller districts and then show up as trend lines in these percentage plots. At a minimum the data suggests a statistical anomaly that is not normally present in a fair election.

7 Michigan Analysis

We now due a time series analysis for Michigan. The data was culled from Edison Research. We first show, Trump, Biden and 3rd party voting percentages vs hours after the start of the election in Figure 16. The third party votes shows the proper convergence to an asymptote that we would expect from

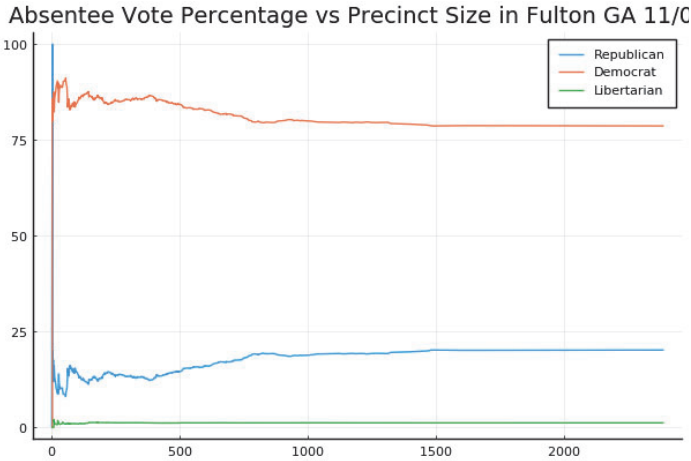


Figure 14: Fulton County Absentee Ballots: Percentages vs Precinct Size

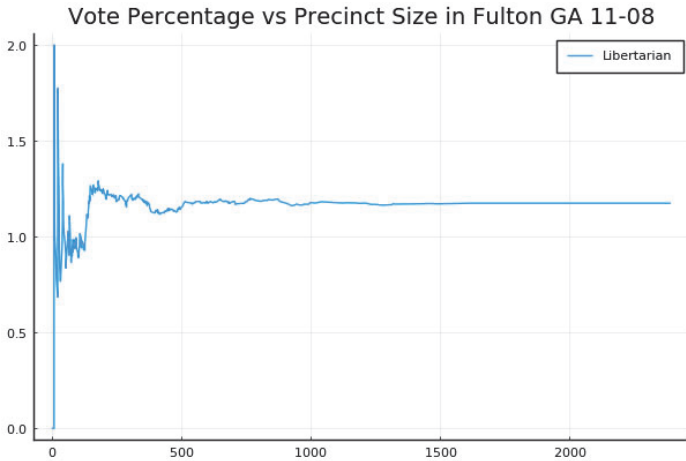


Figure 15: Fulton County Absentee Ballots: Libertarian Percentage vs Precinct Size

the law of large numbers. However the Trump and Biden percentages are vastly different You can see large discrete jumps in the percentages as very large Biden ballot dumps occur over time. You also see that the Biden percentages are mostly always increasing after hour 27, which is statistically unlikely in a fair election.

Note also that almost a million of the ballots are received by hour 27, and we use this as our starting point. At that point we have a total of 970,119 votes cast. At the end of 167 hours we have 5,531,222 votes cast. At our initial point the Biden percentage is 38%, but the new ballots have a Biden percentage totaling 53% as seen in Figure 17. The fraud model has posterior likelihood of 100% to machine precision.

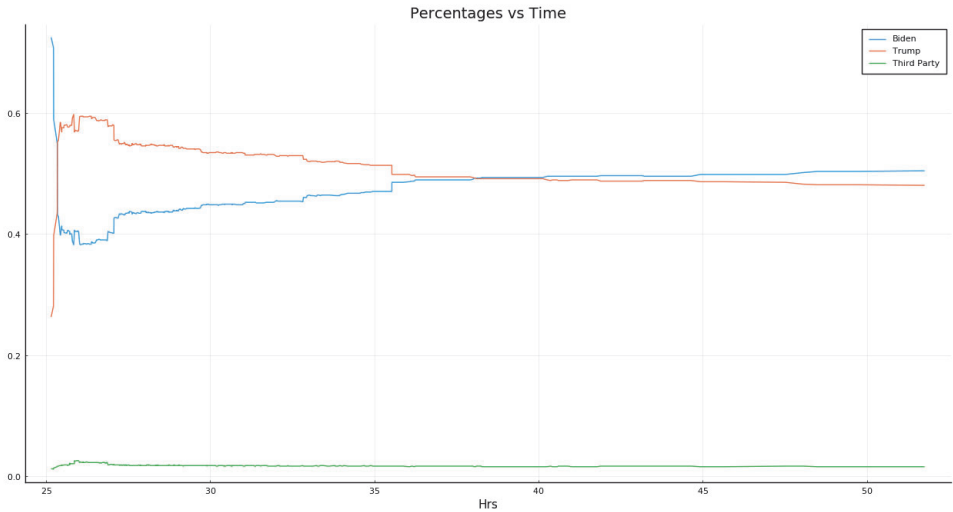


Figure 16: Michigan Vote Percentage vs Time

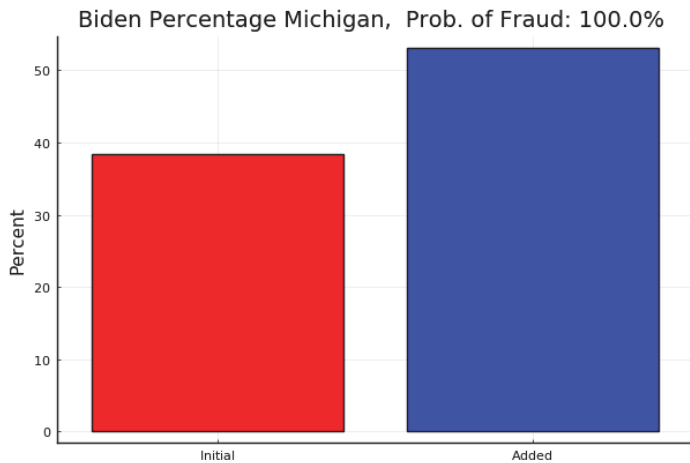


Figure 17: Biden Percentage Before and Added

For Michigan we compute the estimated amount of fraudulent Biden ballots conservatively, assuming that the 50.5 percent seen at the end of the count should have been the correct percentage among the newly added ballots. From this and (4) we obtain an estimate of 237,140 fraudulent votes added for Biden.

8 Maricopa Precinct Analysis

We apply a similar analysis to Maricopa county in Arizona. The data was obtained from the Maricopa county recorder website at https://recorder.maricopa.gov/media/ArizonaExportByPrecinct_110320.txt. Precincts are sorted by size and the cumulative vote percentages are tallied. It should rapidly approach an asymptote, but again in Figure 18 we see an anomaly. The Biden percentage is higher in the smaller precincts, primarily at the expense of Trump, again suggesting vote switching, since the 3rd party percentages immediately approach its asymptote.

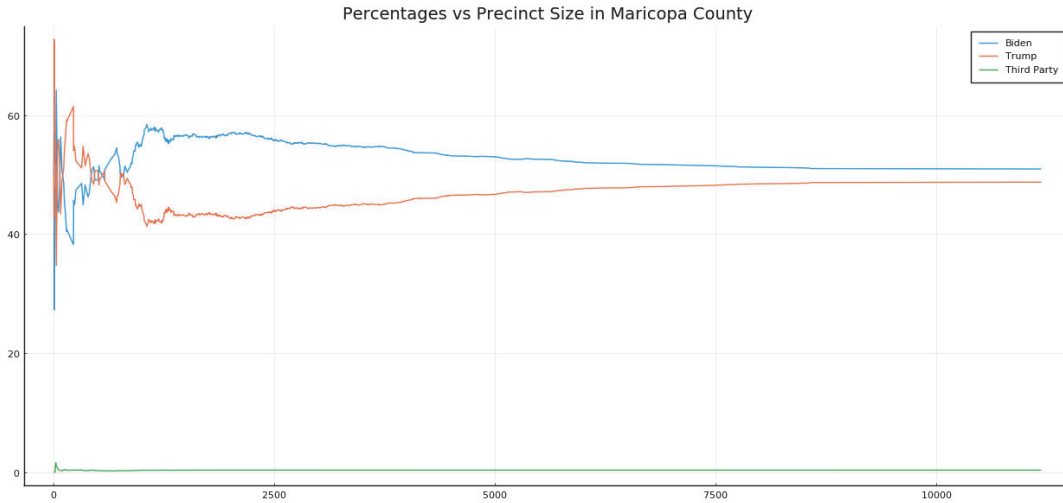


Figure 18: Maricopa County Arizona Percentage vs Precinct Size

In Figure 19 we focus on the third party percentages, which we see are indeed independent of precinct size and converge quickly to its asymptote. This is about what we would expect if the third party candidates were counted fairly. It is in sharp contrast to the precinct size dependency and slow convergence of the Trump and Biden percentages.

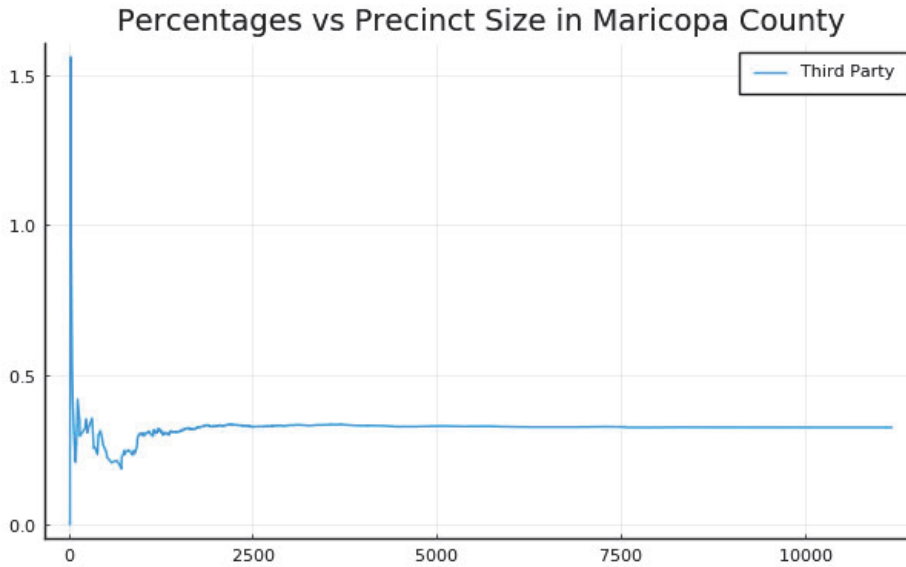


Figure 19: Third Party Percentages vs Size in Maricopa County

References

- [1] Peter Klimek, Yuri Yegorov, Rudolf Hanel, and Stefan Thurner. Statistical detection of systematic election irregularities. 2, 2.1
- [2] lulu Fries'dat and Anselmo Sampietro. An electoral system in crisis. <http://www.electoralssystemincrisis.org/>. 4.2

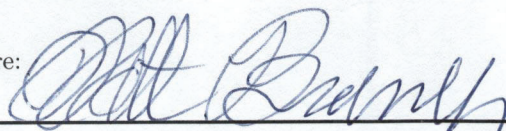
Declaration of Matthew Bromberg Ph.D

December 1, 2020

Pursuant to 28 U.S.C Section 1746, I, Matthew Bromberg, make the following declaration.

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.
2. Matthew Bromberg has a Ph.D in Electrical Engineering from the University of California at Davis and a Masters degree in Mathematics from the University of California at Berkeley. I have been employed, for over 28 years, in the signal processing and wireless signal processing domain, with an emphasis on statistical signal processing. I have published numerous journal and conference articles. Additionally, I have held Top Secret and SAP clearances and I am an inventor of nearly 30 patents, one of which has over 1000 citations in the field of MIMO communications (Multiple Input Multiple Output).
3. I reside at 4303 West Eaglerock Pl., Wenatchee WA, 98801.
4. Given the data sources referenced in this document, I assert that in Georgia, Pennsylvania and the city of Milwaukee, a simple statistical model of vote fraud is a better fit to the sudden jump in Biden vote percentages among absentee ballots received later in the counting process of the 2020 presidential election. It is also a better fit when constrained to a single large Metropolitan area such as Milwaukee..
5. Given the same data sources, I also assert that Milwaukee precincts exhibit statistical anomalies that are not normally present in fair elections.. The fraud model hypothesis in Milwaukee has a posterior probability of 100% to machine precision. This model predicts 105,639 fraudulent Biden ballots in Milwaukee.
6. I assert that the data suggests aberrant statistical anomalies in the vote counts in Michigan, when observed as a function of time.
7. I assert that the data implies statistical anomalies supportive of vote switching in Maricopa county Arizona.

Signature: _____



Supporting evidence for the assertions in (4) and 5 is provided in the following pages.

EXHIBIT 20

DECLARATION

I make this Declaration of my own personal knowledge, and I am competent to testify to the matters contained herein.

1. I served as an official legal observer of the 2020 general election. I observed at the following location: 510 S. Third Ave Phoenix AZ 85003 on Sunday(s) 10-25-2020, 11-01-2020 and Thursday 11-05-2020.
2. While serving as an observer, I personally witnessed the following:
3. On Sunday October 25, 2020, I arrived to serve from 7:15 am to 4:30 pm and was provided a complete tour of the facility from opening of mail-in ballots, *elevated* signature verification and the adjudication process. I was not shown the normal signature verification process, if there was one.
4. There was no ballot counting/tabulation on Sunday, October 25, 2020.
5. I was told that approximately 12% of all mail in / early ballots were in need of adjudication, for reasons including but limited to mis-marking *bubbles* and *write-in* candidates, in order to establish *voter intent*.
6. After watching the adjudication process, I was satisfied the “one Republican and one Democrat” process was being accomplished in a very diligent, straightforward and honest manner.
7. I was concerned and did voice my complaint that the two Maricopa County *referees*, who are called upon to settle any unresolved disputes between the adjudicators, were registered “Independent Party” members. I was told that this *set up* was laid out per Arizona Statute.
8. I asked one referee about her bias and how she voted for President and a very wide grin appeared on the upper cheeks and eyes on that referee’s

masked face and after 10 seconds or so, she said: "I cannot say" (I regret not having this county employee's name, but can easily identify her from a photo or in person).

9. During my October 25, 2020 tour of duty, I was able to ask questions and received feedback from every county employee I engaged at the tabulation center.
10. I engaged *BRUCE* who was the Dominion "Master of Ceremonies" employee who was in sole charge of operating the Dominion server and software, as a Maricopa County contractor. To my knowledge, *BRUCE* was the sole Dominion representative working in the Maricopa County Recorder Ballot Tabulation Center, while I was observing during 10-25-20 (11-01-20 & 11-05-20). To this moment, I deeply regret not having obtained his last name and have been working to obtain it. *BRUCE* is approximately 5'10 180lbs "Ginger" Red/Blond hair. I can easily identify him from a photo or in person
11. I spoke, one on one, with *BRUCE* twice on Sunday October 25, 2020 about the safety and security of the digital data, that he alone was collecting and storing into the Dominion system. When I told him that I grew up watching the 1966 original Mission Impossible and that I had just watched a Tom Cruise "Mission Impossible" movie, where "Tom" was able to access the ultra-secure space portrayed in the movie via HVAC ductwork, *BRUCE* (with a very amused look on his face the entire time) kept physically pointing to the the heavy duty glass/plexiglass server space and carefully pointed out how every

wire, cable and power supply cord were hung in a “basket” path suspended from the ceiling, to and from the server and to all counting/tabulation equipment. He assured me that nothing in that room was connected to the internet.

12. When I continued to pitch my position that “a savvy 14 year old could somehow hack into the data and change the outcome of the results,” *BRUCE* replied; “there must be *trust* in the process” and ended our final exchange on 10-25-20, with a smile, saying that he was a registered Republican.
13. As no ballot counting/tabulation of ballots was to occur that day, at or about 2:30 pm Sunday October 25, 2020 I ended my assigned shift and I departed the Maricopa County Recorder Ballot Tabulation Center.
14. On 11-01-2020, I served from 7:15 am to 4:30 pm at the Maricopa County Recorder Ballot Tabulation Center.
15. While waiting for ballot tabulation activity to commence, Mr. Greg Wodynski, a fellow Republican observer assigned that day, arrived. I was relieved to learn that Greg Wodynski had far more than a general working knowledge of computer programming and had experience in that field for decades.
16. Given my inability to satisfy myself about the security of the data during my 10-25-20 experience, I was hopeful that Greg Wodynski would be able to ask questions that would illuminate in a manner in which I could trust the Dominion data collection and storage system and process.

17. When there was a problem with the operation of one of the older, smaller tabulation devices *BRUCE* was called into action and Greg Wodynski and I sprung to our feet to observe the problem and to watch how it would be resolved.
18. Given my limited knowledge of software and programming, I was truly an observer, seeking to understand what was being done with or to the data.
19. I observed *BRUCE* and his laptop interfacing the broken/stalled tabulation device and handling folders full of data.
20. Greg Wodynski was following closely and understood precisely what it was that *BRUCE* was doing with the data on his laptop, given their exchanges.
21. I came to understand “when a file becomes too full of data, a *subset* folder had to be created.” I am unsure if that *subset* folder was a copy of the original file, a brand new separate file thereby deleting the original file or how that data was handled exactly and did not understand fully, how the broken/stalled tabulation device was returned to service. Greg Wodynski will know, exactly what took place.
22. When Greg Wodynski and I asked how the data was stored as a backup, in case the building burned down, Maricopa County Vendor Dominion employee *BRUCE* admitted that he took a complete copy of the voter files, being stored in the Dominion system out of the building with him every night as a form of a “back up” copy (When the Dominion “Master of Ceremonies” takes the entire voter files into his sole possession while

unobserved off county property with him every night, it does not matter that the system, the County bought into, is purposefully not attached to the internet).

23. On Thursday 11-05-2020 I was assigned to stand a post at 2:30 pm at the Maricopa County Recorder Ballot Tabulation Center. On that day and time the only activity in the tabulation room was the processing of Overseas ballots. These Overseas ballots were being electronically generated by a two person team, consisting of differing political party members. The aforementioned "Independent" county referee was teamed up with a republican.
24. There were about 20 teams of two who were inputting votes made by Overseas voters from stacks of printed *.pdf* sheets of paper having hand written serial numbers, in red ink.
25. I voiced my concern to the lead county worker, about the fact that the "Independent" county worker may not be as dutiful as a Republican or Democrat would be to the process of creating electronic ballots that were to be counted by Dominion machines and software. I do not have the name of the "lead county worker, but can identify her from a picture or in person.
26. About 20 minutes later I asked the lead county worker "where the hand written serial numbered printed *.pdf* documents were generated?"
27. At that moment, my phone rang and the lead county worker told me to "take that call outside." I instantly muted the ringer, while continuing to press her for answers about "where the secured portal was, who was

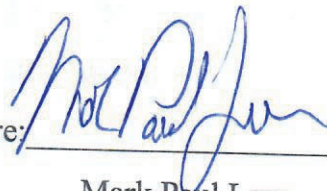
responsible for hand writing serial numbers on each *.pdf* and most importantly, who was observing that process?”

28. I was told “the secure portal was *offsite* and that there was no oversight.”
29. At that point the lead county worker turned and walked away with her assistants, who seem to be serving as witnesses.
30. About 10 minutes later, while observing another set of folks who were “adjudicating” damaged *.pdf* ballots, unsupervised, I took my phone out and saw two text messages from AZ State Director of Election Day Operations Gina Swoboda at 3:45 “Hi mark. You have been removed by maricopa elections. Please leave. Thank you.” & “I am sending another observer” It was Ms. Swoboda’s call I muted as she left me a voicemail stating what she texted when she didn’t reach me by voice. I departed the Maricopa County Recorder Ballot Tabulation Center at approximately 4:00 pm Thursday 11-05-2020.

I declare under penalty of perjury under the laws of the State of Arizona that I have read the above Declaration, am familiar with its contents, and know the same to be true and correct of my own personal knowledge.

November 24, 2020.

Signature: _____



Mark Paul Low

EXHIBIT 21

DECLARATION

I make this Declaration of my own personal knowledge, and I am competent to testify to the matters contained herein.

1. I served as an official legal observer of the 2020 general election. I observed at the following location(s): _Oct 17, 2020 and Oct 21, 2020 at the Maricopa County Tabulation and Election Center in Phoenix, AZ. I also observed at the Happy Trails Voting location, Surprise, AZ on October 28, 2020 _____.

2. While serving as an observer, I personally witnessed the following: At the MCTEC site I observed in 2 different locations: signature verification and ballot processing. In the signature verification room on October 17 I was told to remain at a card table which was at least 10' – 12' from where all of the computer monitors/screens were turned away from me and I was unable to see any of the signatures during the process. On Oct 21 there were more screeners in the room and I was able to turn my chair to observe 2 screens approximately 6 – 8' from me. In this area of the room there were 3-5 screeners looking at “Low Confidence” signatures for the entire afternoon until there was a power outage for approximately 15 – 20 minutes. The “Low Confidence” signatures were indicated at the bottom of the screen with a bright yellow banner. I asked the woman who we were allowed to speak with (Celia) what happened to these signatures and were these votes counted. She informed me that they were counted and that the “Low Confidence” indicator was a new program that they were testing. Following

the brief power outage a quiet discussion among the 3-5 screeners that I could see were looking at Low Confidence signatures was that at least one of them that I could see was now looking at High Confidence signatures. Since I was able to see the Low Confidence signatures earlier I was disturbed that; 1. there were so many screeners looking at the Low Confidence for an entire afternoon 2. that the signatures were not even close to the signatures that they were “comparing” the ballot signature to and 3. I was told by Celia that these signatures were counted I communicated this with Gina Swoboda, who was my contact for observing. In the ballot processing room there were 75 -90 processing tables with, I was told, one Republican and one Democrat on each side of the table. I was told to remain in a yellow taped area which was at least 15' from any of the tables. I couldn't see anything that they were doing other than removing ballots and comparing the number on the ballot to the number on the envelope and then separating the ballot from the envelope. It appeared that they were only to record information with a red pen and the process seemed appropriate. The room was the size of a gymnasium and I really couldn't observe anything specific, although I tried to observe when individuals had questions and when they were filling out there 'reports.' When the press arrived on October 21 in the morning I found it interesting that the women who had been in a supervisory capacity when I observed on Oct 17 were now at a table “closer” to me and processing ballots for about an hour and a half while several press people with photographers filed in and out.

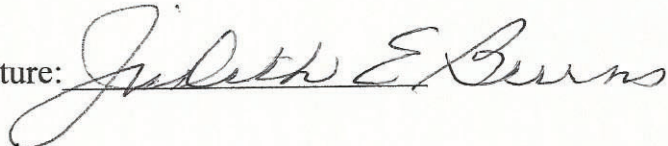
3. October 28 I observed voting at the Happy Trails site in Surprise, AZ. Immediately after voting started it became evident that the glue on the envelope in which people placed their ballots was not going to stick and the envelopes would not remain closed. People did not want to lick the envelopes or take their masks off to do so. The poll workers used masking tape on these ballots. I called the contact person on my ID and reported this to them. There were many, if not most, of the ballots throughout the day that had masking tape used to close the envelope. I was very concerned that these ballots would not be counted. One of the supervisors at the site went to the election depot to get something to assist in sealing the envelopes. He came back with a small container which they put water in and sealing envelopes continued to be a problem throughout the day. The supervisor didn't seem at all concerned about doing this. I was told to not ask questions or talk to anybody at that point.

4.

5.

I declare under penalty of perjury under the laws of the State of Arizona that I have read the above Declaration, am familiar with its contents, and know the same to be true and correct of my own personal knowledge.

Dated November 16, 2020.

Signature: 

Printed Name: Judith E. Burns

EXHIBIT 22

DECLARATION

Monday November 23rd 2020

I make this Declaration of my own personal knowledge, and I am competent to testify to the matters contained herein .

1. I served as an official legally approved GOP observer of the 2020 general election. I observed at the following location: MCTEC (Maricopa County Tabulation Election Center) 510 S. Third Ave Phoenix AZ 85003.
2. On Saturday 10-24-2020 & Sunday 11-01-2020 I observed for approximately 8-9 hour daytime 8-5 shift in the tabulation intake room. My signature is on visitor logs kept by staff.
3. In this tabulation and adjudication work area was the Dominion computer system computer hardware on what I observed to be racked Dell branded computer hardware, 5-6 Canon scanners on work are tables and two larger free standing (presumably Dominion) bulk ballot scanners.
4. I interacted with several supervisors including Celia (a lead person at MTEC who granted me access), Rene a supervisor in tabulation area, and Mary C. Connor another lead person – in and outside the tabulation room.
5. I spoke to Bruce who identified himself as Dominion employee on contract to Maricopa County for this election and observed another Dominion employee named John. Bruce and John appeared to have shared **Dominion system administration roles and demonstrated and acknowledged systems administration access to the voting computer systems.** Other recorder's office employees and supervisors worked with Bruce and John closely.
6. All the mentioned scanners were optically reading the mail-in ballots, converting the paper ballots into electronic images and discerning voter tabulation data into electronic format (data "votes tabulated" and scanned ballots in an image format – think jpeg format for example) and all stored in the computer systems files on hard drives.
7. On Thursday Nov 5th. I spent time in a signature verification room. I interacted with several supervisors including Celia (a lead authority person at MTEC) and Mary C. Connor a supervisor who escorted me to the signature working area room.

8. On Sunday Nov 1st in the adjudication and tabulation scanning room area, and in witness with another GOP Observer named Mark, I spoke to Bruce from Dominion and asked questions on the computer system contained in that room and connected to the ballot scanners. All mail in ballots were in theory feeding the data into this Dominion computer system.
9. Staff supervisors and Dominion employees stated that about 12% of mail in ballots were being rejected in the ballot readers and needed human intervention in the adjudication process. This amounted to tens of thousands of ballots that required intervention on the two shifts and days I observed adjudication and ballot tabulation.
10. On Sunday 11-01-2020 I asked Bruce how the tabulation data and scanned images were being stored and backed up. It is common IT practice to do regular data (disk drive) backup in the event of some system failure. Bruce stated that he would perform a manual daily system backup to an external hard drive attached to and in the secured computer bay "glass cage" within the larger adjudication/tabulation room. The hard drive was in a rubberized orange case and was easily visible, he pointed and identified it. I asked what software program he was using to perform automated backup ups. He stated he was not using an automated backup, and inferred he was doing a simple manual data copy to that "orange disk". Bruce stated that he took a second copy of the daily backup the orange external backup up target hard drive. Bruce reached for a new boxed hard drive on a nearby desk where he administered the systems at then pointed to a shelf with a box filled with spare and new empty hard drives.
11. **Bruce stated he made a daily second disk backup to a new spare hard drives daily. I asked him where the second daily disk drive backup data copy was being stored. Bruce stated the daily external disk copies were being physically moved off site to another location outside the MTEC building. I asked Bruce to what facility and by whom the disks were being relocated and he provided a vague answer that the were being carried to another building somewhere uptown. I then inquired if there was chain of custody of this daily data hard drive copy being moved outside the MTEC building and outside**

the tabulation room. He stated there was NO CHAIN OF CUSTODY on data backup up hard drives leaving the MTEC facility on a daily basis for an undisclosed location.

12. Sunday 11-01-2020 I observed Bruce discussing (and then explaining to me when I inquired) on specifics of a process where he was manually manipulating stored scanner tabulation data files. The purpose of this manual manipulation was due to what he described as a processing issue at the numerous adjudication computer workstations.
13. Bruce described having to take the scanned mail in ballot tabulation data files from a ever-growing large data file in the Dominion system storage devices and creating smaller subsets (data directories) containing scanned ballot files; presumably so that adjudication work stations staff could more effectively access and perform adjudication operations. This manual file operation performed by Dominion employee Bruce entailed taking ballot files from one large file directory and placing into many smaller file directories. Then performing a human driven and manual file quantity count - post the worker driving adjudication processing. This post count was to determine that the total number of files adjudicated in smaller batches equaled the total files (ballots) needing adjudication in the original source files. **This manual administrator operation at the file and directory level on the tabulation system storage was of concern to me. It was a human intervention process and therefore creating a potential for intention or non-intentional errors or lost ballot files.**

I declare under penalty of perjury that I have read the above Declaration, am familiar with its contents, and know the same to be true and correct of my own personal knowledge.

Dated November 23, 2020

Signature: 

Printed Name: Gregory Wodynski

EXHIBIT 23

DECLARATION

DECEMBER 1, 2020

My name is Linda Brickman. Thank you for allowing me to come forward and speak with all of you.

Effective November 12, 2020, as the 1st Vice-Chair of the Maricopa County Republican Committee (MCRC), by operation of law upon the resignation of the Chairman, I took over the performance of all the Chairman's duties.

I was notified by Rey Valenzuela, Director of Elections, that the Logic & Accuracy (L&A) Certification of the Dominion voting systems would take place on November 23rd. With limited notice, I was later notified the date was moved to November 18, 2020 at 10:00 AM.

There will be around eleven (11) issues that I need to share with you. Starting with a little background first please.

I arrived at the Maricopa County Tabulations and Election Center (MCTEC) prior to 10:00 AM, for what was supposed to be a morning turn around inspection of the Dominion Software and equipment; however, it took some eight (8) hours before the two formal L&A Certifications were completed, with mixed results.

We began in the BCC or Tabulation room, where the Dominion Software/machines were set up ready for actual testing.

There were about eight or 9 regular (vs high speed) machines set to tabulate all the numbers from test ballots (pictures already sent to you) selected by staff from the Secretary of State's (SOS) Elections office as part of the SOS L&A Certification, and one main frame

computer behind glass-like walls plugged into the wall, and a computer technicians work station with a desktop computer to transfer results from the individual tabulators and into the server. This main frame machine that I observed was to calculate all the test ballots and add up the “0’s” to give a grand total of all 8 or 9 machine total ballots counted, equaling “0.”

Problems occurred almost from the start with the SOS certification. For example, a number of the ballots could not be read by the tabulator machines; at least one or more of the tabulators broke down and portions had to be replaced; incorrect information had been inputted into each tabulator earlier that morning; the “wrong files” were loaded up into the main frame by the computer technician; and neither SOS staff nor the computer technician were able to quickly resolve the problems. Instead, we were alerted it might take an hour or more to work things out, so we adjourned until 2:00 PM, after lunch.

At approximately 2:00 PM I asked if the problem was resolved, and what had happened. Instead, I was informed that the machines were not calculating correctly, and all the machines were shut down during the break and reset; and they were going to start a brand, new test.

About an hour plus later, the ballots were run into the tabulators and printouts of the results in the form of a “cashier’s tape” were reviewed by me and others. Then, the memory sticks from each tabulator were removed and handed to the computer technician for loading into the server along with other relevant files we were told.

Printouts were generated by the Dominion server, and County Chairs from the 3 County Political Parties, as well as other observers, began comparing the individual voting totals tabulated for accuracy. Once completed, the County Chairs were asked to fill out

and sign the “Certification” for the SOS L&A. And per Rey Valenzuela, Director of Elections, other observers could sign if they insisted, but only in an “Observer Capacity” and not in an official party capacity.

Then came time to sign the Certification.

Based on the issues described above with the SOS L&A test, and my familiarity with reports from other State Secretary of States (for example, Texas), the December 2019 Democratic US Senators written investigation into Dominion including irregularities in earlier elections, as well as reports from forensic experts including local Arizona ones, I denied certification, writing on the form: “CERTIFICATION DENIED – LINDA BRICKMAN – MC [Maricopa County] CHAIRMAN.”

We then began the 2nd L&A test, but this one was conducted by Maricopa County Elections Staff and on separate Dominion voting tabulator machines. This was a similar process with results going to the server and reports printed out. But whatever problems or irregularities surfaced during the first SOS test, they did not manifest this time.

And for the same reasons noted above, I denied certification, writing on the Maricopa County form: “CERTIFICATION DENIED – LINDA BRICKMAN – MC [Maricopa County] CHAIRMAN.”

I also have copies of each of those ballots counted, with copies available upon request. Again, my reasons as noted above were my first-hand observations of the flaws and irregularities in the SOS L&A tabulating and calculating of the Dominion software, the unexplained turning off the computer system and doing a reset versus a correction, and the over 5 hours for the SOS test and results review, plus my lack of faith in the 2nd L&A

test – we could see the machines, but could not see or observe the software behind the machine to confirm what had gone on.

As a veteran County Elections Worker who actually worked the election both during the August Primary, and the General from 10/19/20 to 11/11/20 working in the Signature Verifications room, Duplication room, Adjudication room, ABC Room, and Hand Count Audit, let me share just about 6 irregularities I PERSONALLY OBSERVED:

- (1) Signature verification standards were constantly being lowered by Supervisors in order to more quickly process that higher amount of early and mail-in ballots (from approx. 15 points of similarities, to a minimum of 3, lowered to 1, and ultimately to none – “Just pass each signature verification through”) “There are too many rejection of ballots each day, so push them through.”.**
- (2) Challenged signatures on envelopes where the signature was a completely different person than the name of the listed voter, was let through and approved by supervisors.**
- (3) Challenged runs or batches of envelopes for signature verification observed by me to be the exact same handwriting on the affidavit envelopes on numerous envelopes. When I asked if the County Attorney would be alerted for possible ballot fraud, I was told no, but supervisors would take care of it (I can supply one of the batches with book numbers that I texted in case I needed it).**
- (4) In the Duplication room, I observed with my Democratic partner the preparation of a new ballot since the original may have been soiled, damaged, or ripped, and wouldn’t go through the tabulator. I read her a Trump/Republican ballot and as soon as she entered it into the system the ballot defaulted on the screen to a**

Biden/Democratic ballot. We reported this to supervisors, and others in the room commented that they had witnessed the same manipulation. We were never told what, if any, corrective action was taken.

(5) Election Office Observers – when it became apparent that more and more early and mail-in ballots would need to be processed, I mentioned that the current rule of the number of observers per party was not adequate (1 per party, unless all parties agreed to more). And since the Governor refused to call the Legislature into session for any reason, and little incentive for the Democrats to agree to a higher adequate number, there was no way 1 observer per Party, forced to the back of a room, or behind a see-through wall, had a legitimate opportunity to see what elections workers were seeing in real time and doing, especially where up to 20 or more workers processing tasks, sometimes in 10 seconds or less! And I personally observed most observers acting “clueless”, and do not believe any of them even realized the challenges I made and referenced above.

(6) And lastly, one of the most egregious incidents in both the Duplication and Adjudication rooms which I worked, I observed the problem of Trump votes with voters checking the bubble for a vote for Trump, but ALSO, writing in the name “Donald Trump” and checking the bubble next to his hand written name again, as a duplicated vote, counting as an “OVERVOTE,” which means – no vote was counted at all, despite the policy having been changed to allow these overvotes. Supervisors contradicted their own policies where the intent was clear. Ray Valenzuela, Director of Elections, told me openly at the morning of the Dominion Certification (November 18, 2020), that this was incorrect, the Supervisors were terribly mistaken

and as an Adjudicator, I was instructed incorrectly, and these many votes SHOULD HAVE BEEN COUNTED AND NOT TURNED AWAY AS AN OVERVOTE.

The next day, I was called outside the room where I was working and reprimanded for causing trouble over the weekend and was told to stop saying that there were wrong doings going on in other rooms, so I was suppressed from speaking the truth for fear of retaliation or pressure of being let go. So, the supervisor kept me working ALONE in my corner of the room, not to circulate with others.

Chairman Finchem, Legislators, and Mayor, I am here today not as an expert in the Dominion software, but as a voter in Maricopa County, who wants to hear the truth and speak the truth and not feel suppressed to speak before you now.

There should be integrity in our voting electorate. Voting is not a right; voting is not a privilege; voting is not an option. Voting is an obligation of every legal American Citizen.

Thank you.

God Bless America – and God Bless Donald Trump!

Linda Brickman

Maricopa County Republican Committee Chairman (MCRC)

Signed: *Linda S Brickman*

Dated: December 1, 2020