DATE FILED: December 17, 2021 11:53 AM
FILING ID: BC329FCB8936E
CASE NUMBER: 2020CV34319

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

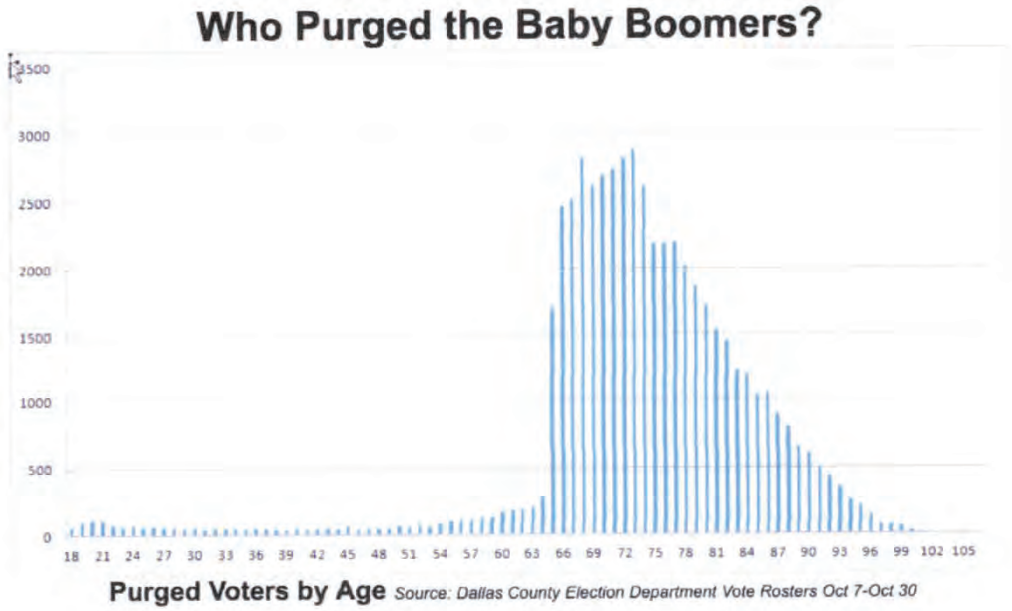
Dallas Residence for voting purposes, but who in a spot check are unknown to the residences they list in the ES&S system. A short list of them includes:

Country	Voters Who Voted
Mexico	118
Guatemala	9
Nicaragua	4
Kenya	18
Canada	154
Ireland	34
China	62
Australia	105
	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.



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%

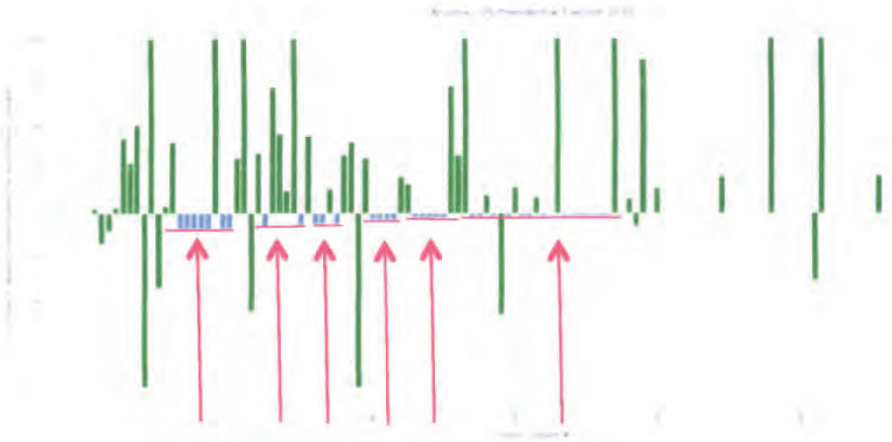
14. A similar outcome can be seen in many precincts in Maricopa County where Dominion is the EMS service provider. Here, public data reveals 54 percent of precincts (300 of 558) contain voter turn-out above 80%, according to county records. Further if these public data votes were normalized to 80% turnout (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.

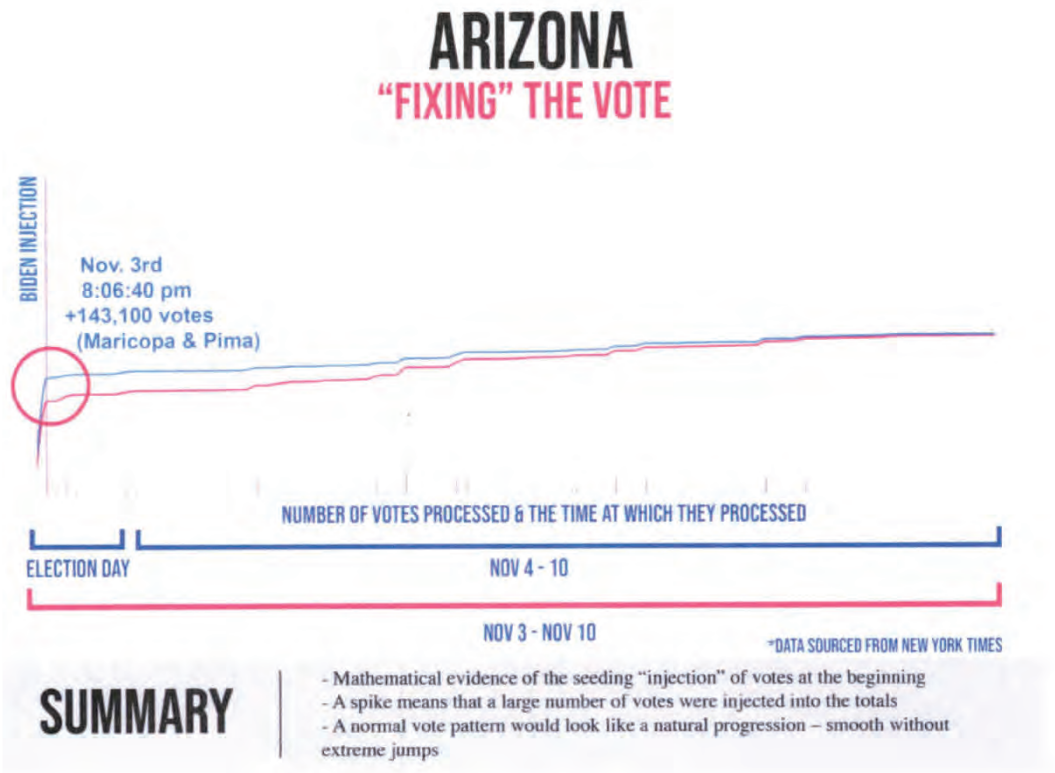
15. The following data strongly suggests that the additive algorithm (a feature enhancement referred to as "ranked choice voting algorithm" or "RCV") was activated in the code as shown in the Democracy Suite EMS Results Tally and Reporting User Guide, Chapter 11, Settings 11.2.2. It reads in part, "**RCV 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

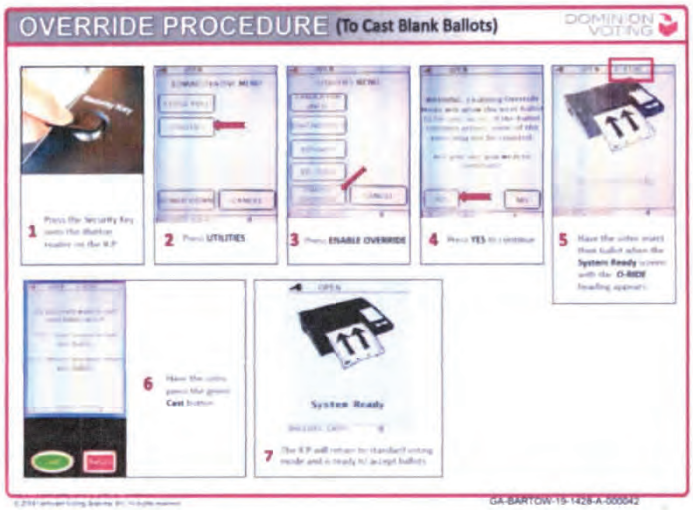
16. Yet another statistical red flag in Arizona starts with an improbable, and possibly impossible spike in processed votes. A time series and location specific

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.



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.

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&btnbeginregistration=begin voter
registration&btnnextelectionworkerinfo=next&btnnextpersonalinfo=next&btnnextresde
tails=next&btnnextvoterinformation=next&btnsubmit=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
xxxxinjjeuee&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

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

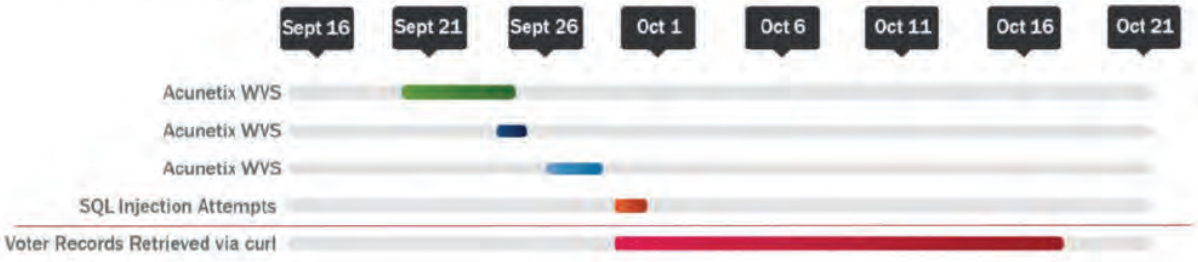


Figure 1: Overview of malicious activity

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-nsas-top10-cybersecurity-mitigation-strategies.pdf

Additionally, use tools (e.g., the OWASP Dependency-Check Project tool[3]) 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-nsas-top10-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

- FBI and CISA PSA: Foreign Actors and Cybercriminals Likely to Spread Disinformation Regarding 2020 Election Results

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 statististical 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,

$$P(k|N) \equiv {}_N C_k p^k (1-p)^{N-k}, \tag{1}$$

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,

$$B_N(f) \equiv {}_N C_{Nf} p^{Nf} (1-p)^{N(1-f)}. \tag{2}$$

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,

$$C_{N,\alpha}(f) \equiv B_{N(1-\alpha)}(f-\alpha). \tag{3}$$

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,

$$P(F|f) = \frac{C_{N,\alpha}(f) p_F}{C_{N,\alpha}(f) p_F + B_N(f)(1-p_F)},$$

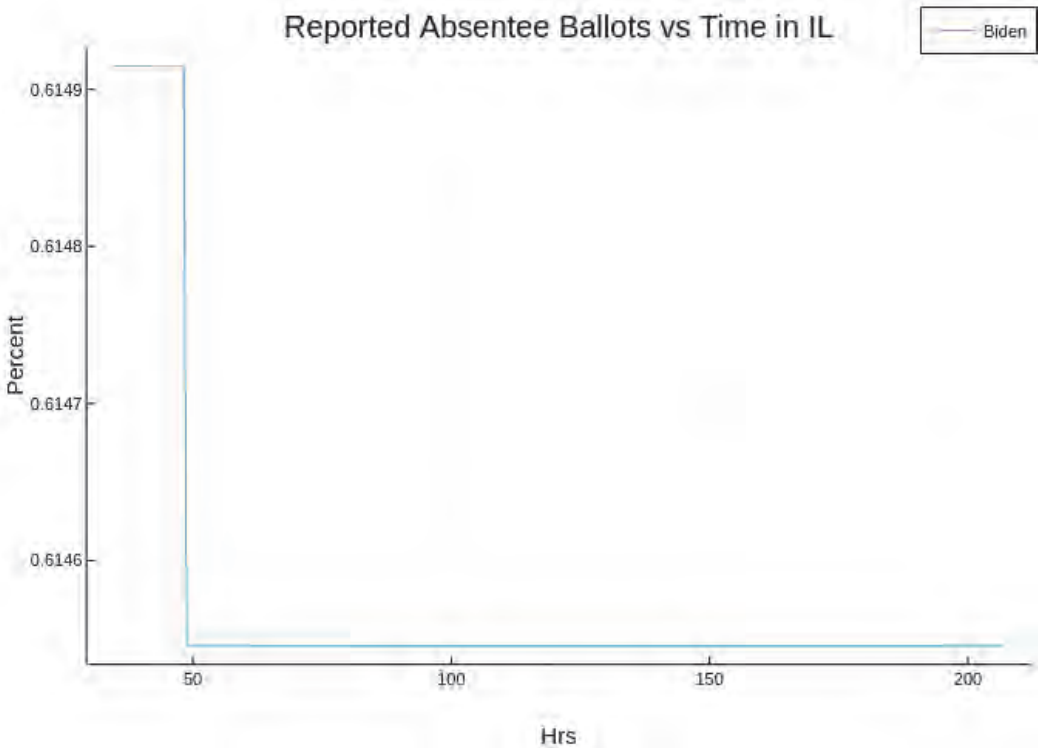


Figure 1: Reported Biden Fraction In Illinois vs Time

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 occured.

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.

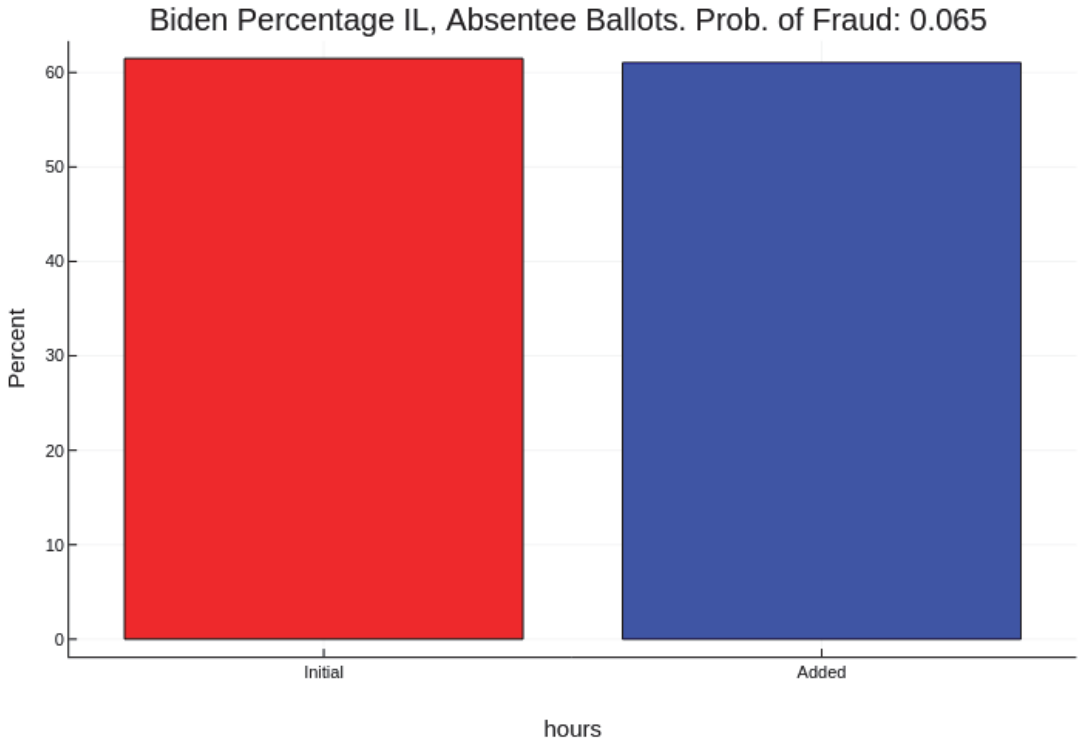


Figure 2: Before and Added Biden Fraction

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 statitics 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

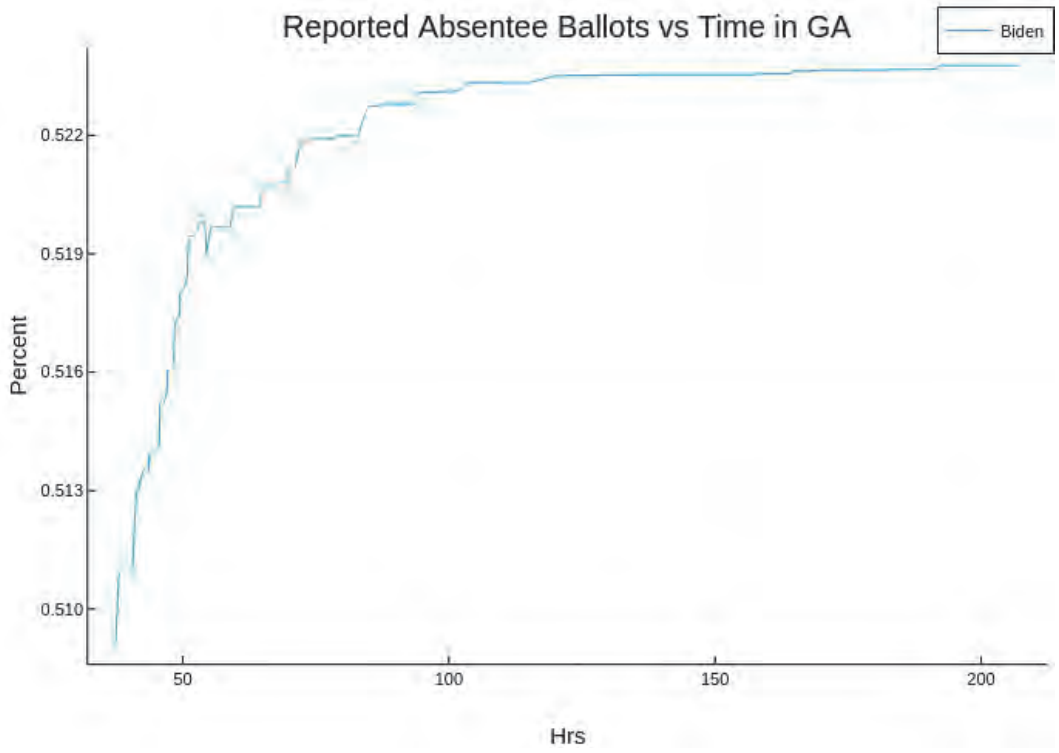


Figure 3: Georgia Absentee Ballots vs Time: (Biden Fraction)

have,

$$\frac{B-x}{N_1-x} = f$$
$$x = \frac{B-N_1 f}{1-f}. \tag{4}$$

In the case that votes were actually switched from Trump to Biden, then the formula becomes,

$$\frac{B-x}{N_1} = f$$
$$x = B - N_1 f$$

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

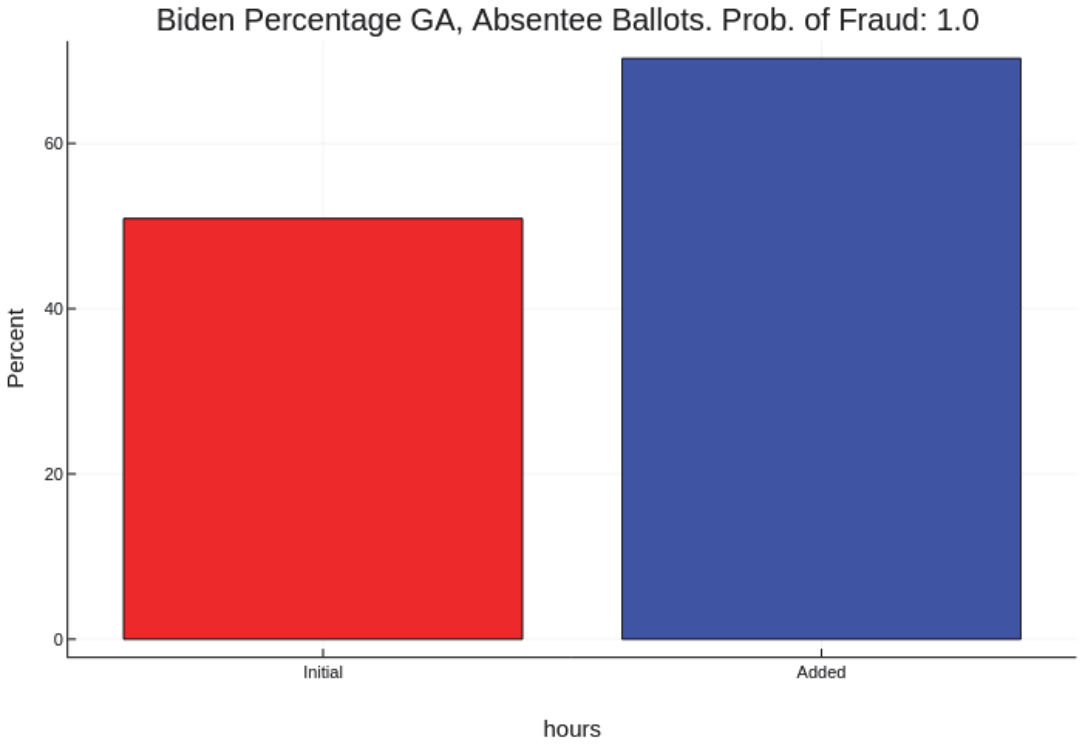


Figure 4: Before and After Biden Fraction in Georgia

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 Trumps 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 acount of @shylockh, who derived his sources from the New York Times and in some cases from the unofficial precinct reports from the Wisconsin elections commision 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.

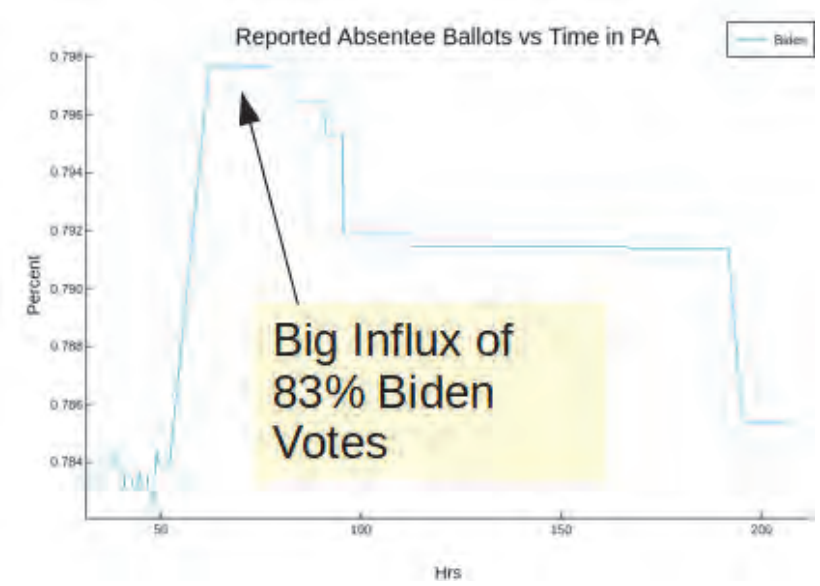


Figure 5: Pennsylvania Absentee Ballots vs Time: (Biden Fraction)

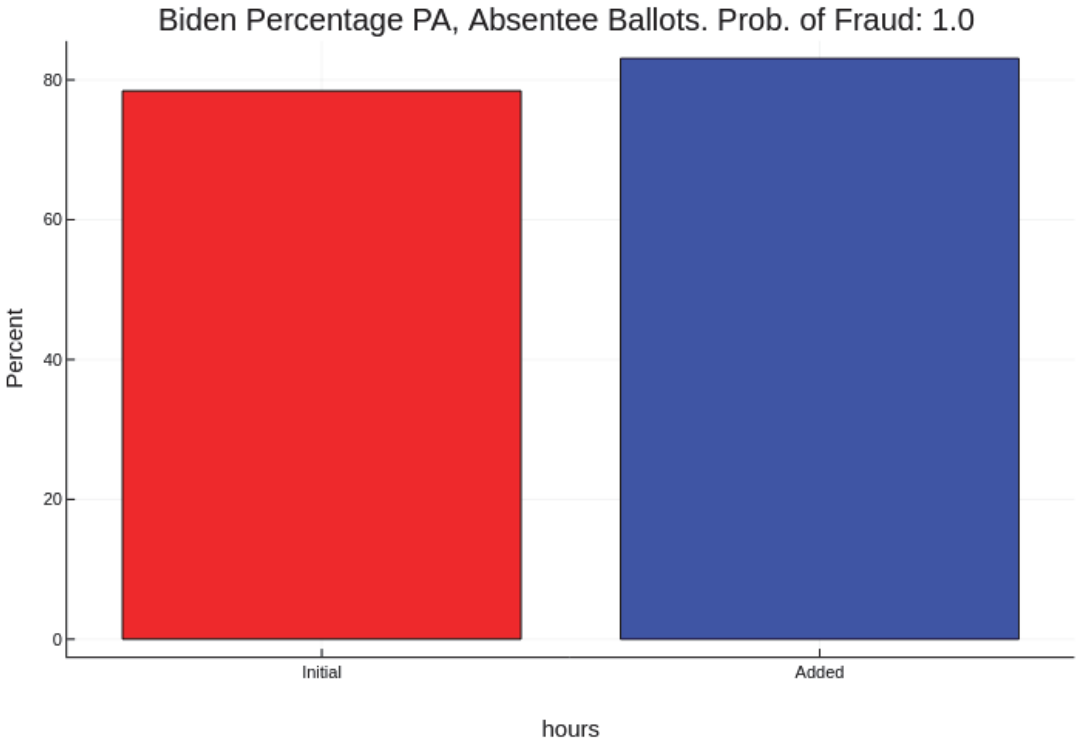


Figure 6: Before and After Biden Fraction in Pennsylvania

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.

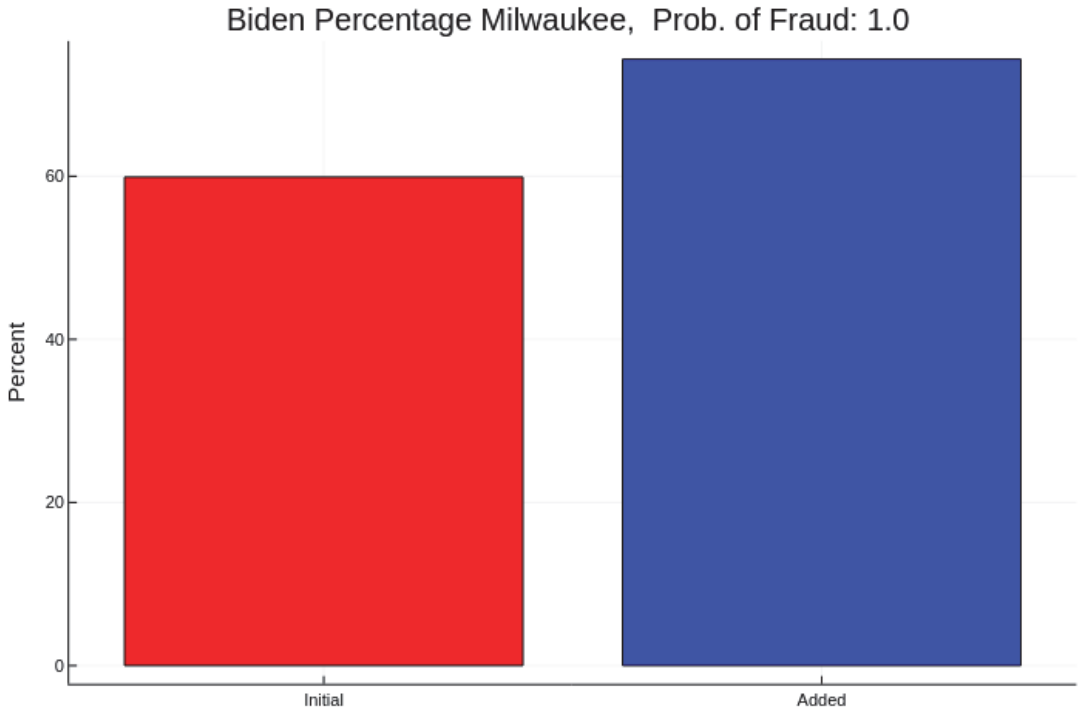


Figure 7: Before and After Democrat Fraction in Milwaukee

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

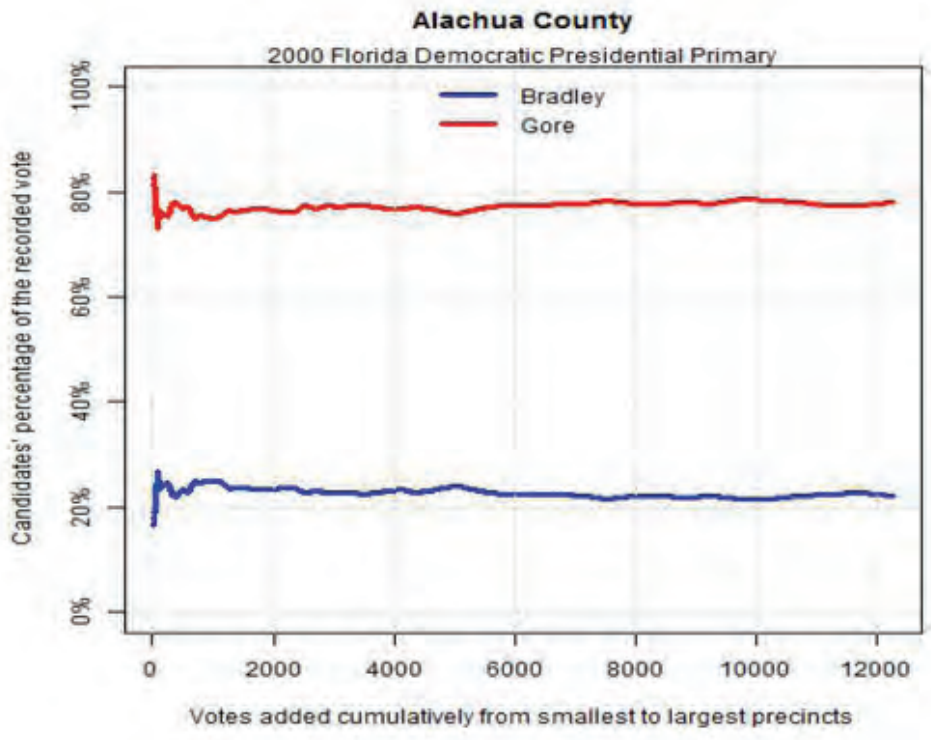


Figure 8: Baseline Cumulative Fractions Sorted by Precinct Size

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 inital 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%.

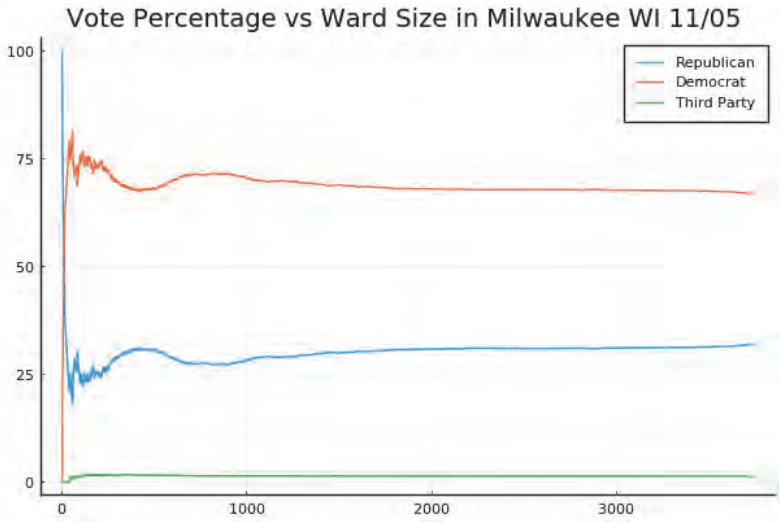


Figure 9: Milwaukee Democrat Ballots Percentage vs Ward Size

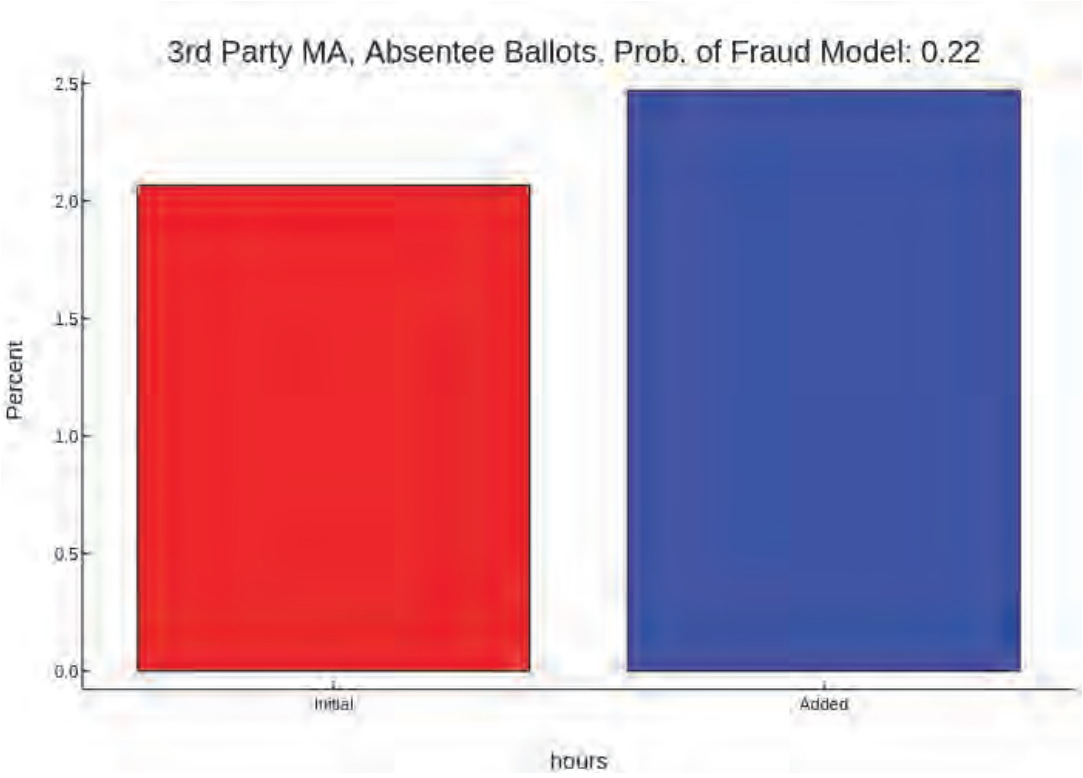


Figure 11: MA 3rd Party Percentage Initial and Added

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.

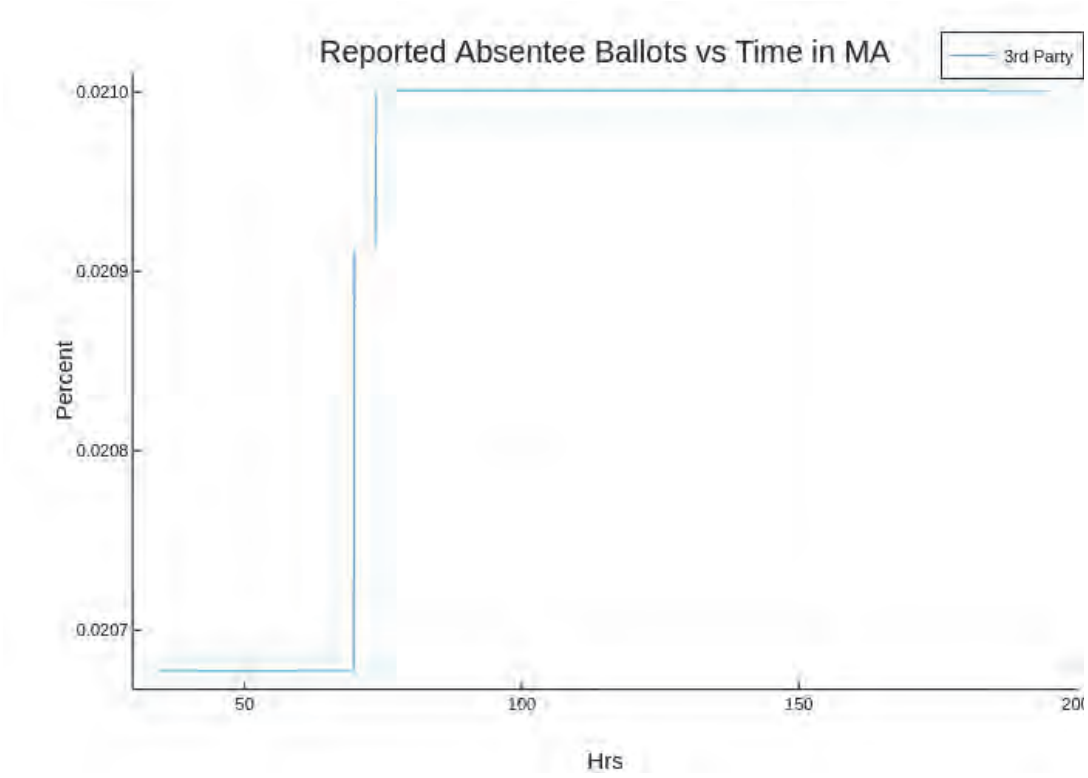


Figure 10: MA 3rd Party Absentee Votes vs Time

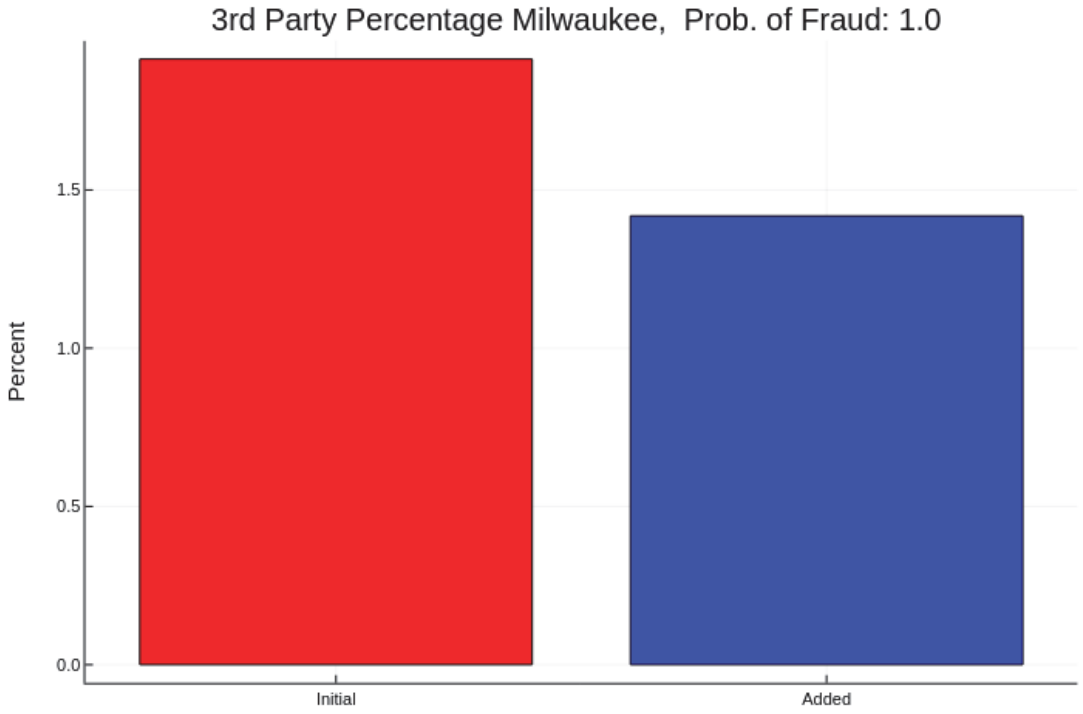


Figure 12: Milwaukee 3rd Party Percentages between Wednesday and Added

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 irregularites observed prior to the Ward 600 mark.

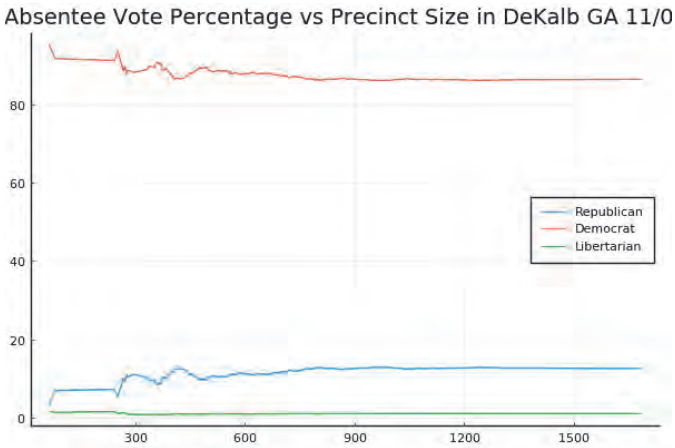


Figure 13: Dekalb County Absentee Ballots: Percentages vs Precinct Size

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

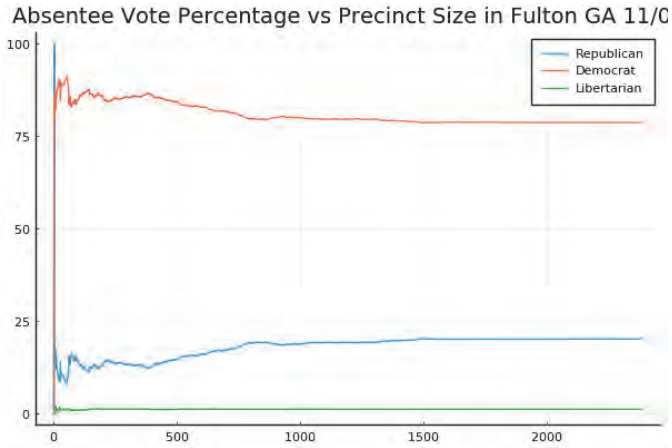


Figure 14: Fulton County Absentee Ballots: Percentages vs Precinct Size

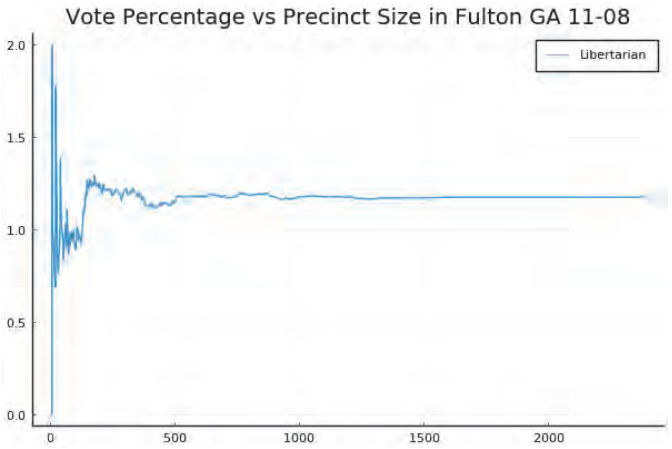


Figure 15: Fulton County Absentee Ballots: Libertarian Percentage vs Precinct Size

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.

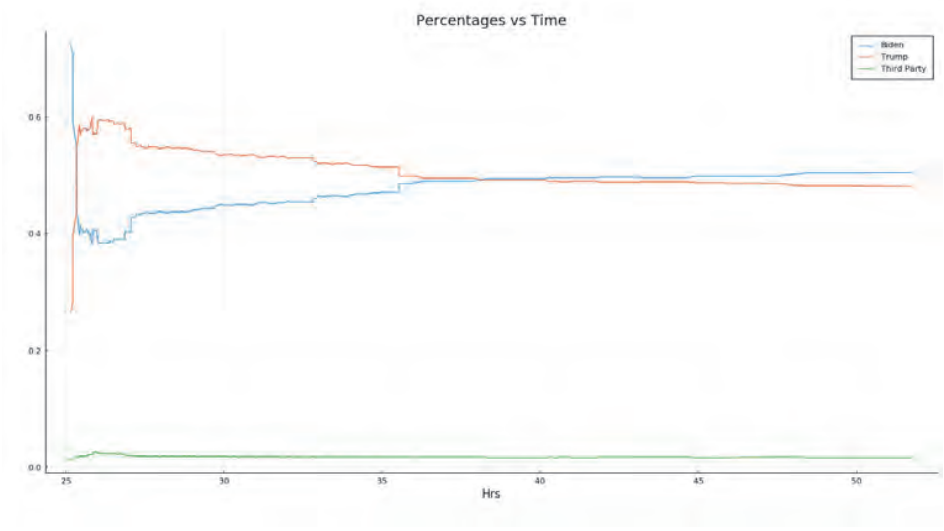


Figure 16: Michigan Vote Percentage vs Time

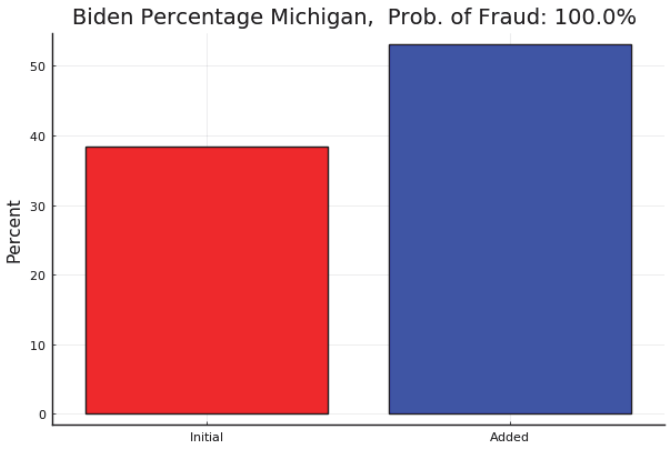


Figure 17: Biden Percentage Before and Added

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 similiar 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 it's asymptote.

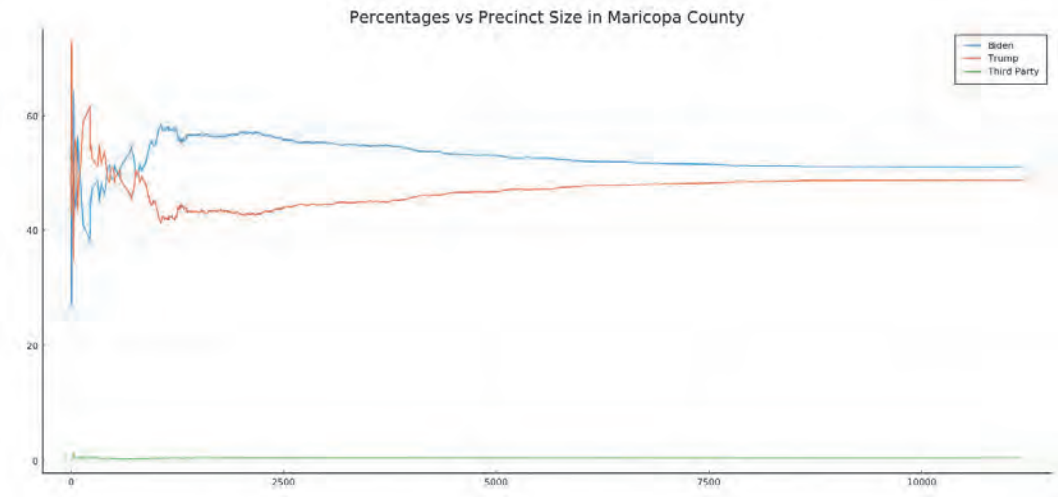


Figure 18: Maricopa County Arizona Percentage vs Precinct Size

In Figure 19 we focus on the third party percentages, which we see are indeed independent of precinct size and converge quickly to it's 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.

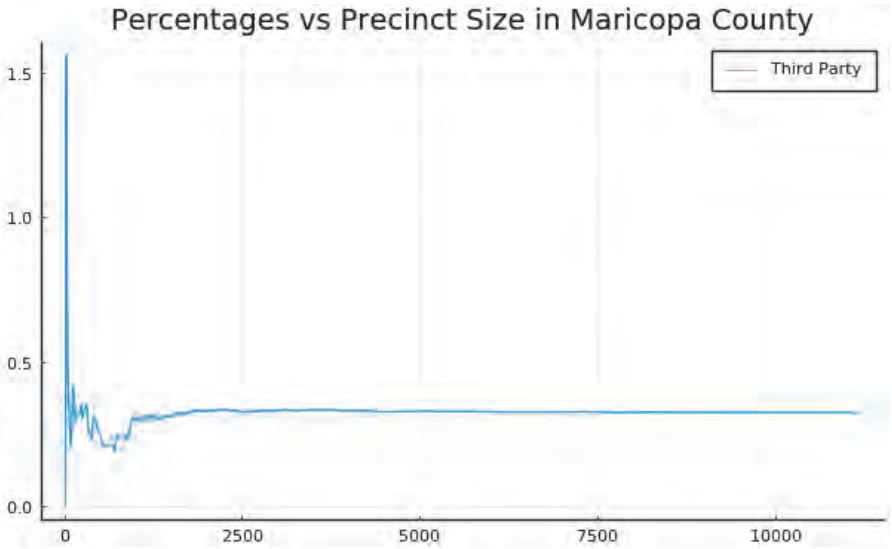


Figure 19: Third Party Percentages vs Size in Maricopa County

References

[1] Peter Klimek, Yuri Yegorov, Rudolf Hanel, and Stefan Thurner. Statistical detection of systematic election irregularities. 2, 2.1

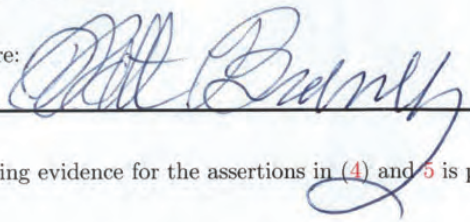
[2] lulu Fries'dat and Anselmo Sampietro. An electoral system in crisis. http://www.electoralsystemincrisis.org/. 4.2

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 statististical 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 remained 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 seemed 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: Judith E. Burns

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: Gregory Wodynski

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**