Subject:	RE: Public Information Request (TX-SOS-23-1141) - SOS PIR 23-1126
Date:	Monday, December 18, 2023 at 10:13:26 AM Eastern Standard Time
From:	GeneralCounsel
To:	AO Records
CC:	GeneralCounsel
Attachments:	12.18.23 Documents.zip

EXTERNAL SENDER

Good morning,

As a follow up to our December 8 email, please see the attached zipped folder containing the documents responsive to your Request.

The responsive documents contain email addresses of the general public. An email address of a member of the public is confidential under section 552.137 of the Texas Government Code. The attorney general authorized all governmental bodies to withhold an email address of a member of the public without first requesting an attorney general opinion in Open Records Decision No. 684 (2009). Thus, this information has been redacted.

Kind regards,

Jennifer Williams
Legal Assistant to the General Counsel
Office of the Texas Secretary of State

From: GeneralCounsel <GeneralCounsel@sos.texas.gov>
Sent: Friday, December 8, 2023 4:42 PM
To: 'AO Records' <records@americanoversight.org>
Cc: GeneralCounsel <GeneralCounsel@sos.texas.gov>
Subject: FW: Public Information Request (TX-SOS-23-1141) - SOS PIR 23-1126

Good afternoon,

Thank you for contacting the Office of the Texas Secretary of State (the "Office"). This email responds to your request for information under the Public Information Act, Chapter 552 of the Texas Government Code (the "PIA"), which was received by the Office on November 21, 2023 (the "Request"). The Office was closed November 22-24, 2023 in observance of Thanksgiving. Therefore, the 10th business day from the date that the Office received the Request is today, December 8, 2023.

We are processing your request in accordance with the terms of the PIA. We require additional time to review our records and produce responsive documents. We will provide you responsive documents—to the extent such information is not excepted from disclosure under state or federal law—by 5:00 p.m. on December 18, 2023. *See* Tex. Gov't Code § 552.221(d).

Kind regards,

Jennifer Williams
Legal Assistant to the General Counsel
Office of the Texas Secretary of State

From: AO Records <records@americanoversight.org>
Sent: Tuesday, November 21, 2023 11:16 AM
To: GeneralCounsel <GeneralCounsel@sos.texas.gov>
Subject: Public Information Request (TX-SOS-23-1141)

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear Public Information Officer:

Please find attached a request for records under the Texas Public Information Act.

Sincerely,
Dylan Winters
Paralegal | American Oversight
records@americanoversight.org |
www.americanoversight.org | @weareoversight

PIR: TX-SOS-23-1141

From: Walter Daugherity [redacted]
Sent: Sunday, June 11, 2023 6:18 PM
To: Elections Internet
Subject: Application of ES&S for certification of 6.2.0.0 and 6.3.0.0 voting machine software
Attachments: ES&S Certification.pdf

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear Secretary Nelson,

I am a Texas citizen and taxpayer residing in Brazos County, and I do not consent to certification of ES&S voting machine software versions 6.2.0.0 and 6.3.0.0 without further specific examination by additional experts, as detailed in the attached letter I am hereby officially submitting for your consideration.

Sincerely,

--
```
Dr. Walter C. Daugherity            Senior Lecturer Emeritus
>1/128 Chickasaw & Cherokee         Dept. of Computer Science & Eng.
Life Member, American MENSA         Texas A & M University
ACM Member since 1963               College Station, TX 77843-3112
Faculty Senate Parliamentarian Emeritus
E-mail: daugher@cs.tamu.edu
http://faculty.cs.tamu.edu/daugher
              ---Not an official document of Texas A&M---
```

June 6, 2023

Mrs. Jane Nelson
Texas Secretary of State
Via email to elections@sos.texas.gov

Re: Application of ES&S for certification of 6.2.0.0 and 6.3.0.0 voting machine software

Dear Secretary Nelson,

I am a Texas citizen and taxpayer residing in Brazos County, and I do not consent to certification of ES&S voting machine software versions 6.2.0.0 and 6.3.0.0 without further specific examination by additional experts, as detailed below.

As a Senior Lecturer Emeritus in the Department of Computer Science and Engineering at Texas A&M University, and a computer consultant to major national and international firms and government agencies (including classified work), I have given expert testimony many times regarding ongoing vulnerabilities in voting machines, including vulnerabilities in their hardware, software, and network capabilities. For example, on January 24, 2023, I addressed the Texas Senate Committee on Administration on this subject.

To comply with Texas statutes regarding Voting System Standards, you must not approve ES&S voting machine software versions 6.2.0.0 and 6.3.0.0 without further specific examination by additional experts to determine whether or not they comply with Election Code 122.001(a)(4), which mandates that

> "A voting system may not be used in an election unless the system…is safe from fraudulent or unauthorized manipulation."

There are two areas which require further specific examination by additional qualified experts:

(1) Source code for ES&S voting machine software versions 6.2.0.0 and 6.3.0.0, and
(2) Hardware and software security vulnerabilities, including susceptibility to remote access.

Regarding (1), I attach my expert declaration in the Alabama Secretary of State case. This explains how election results from ES&S software showed very strong evidence of a specific type of manipulation, namely, a Proportional-Integral-Derivative (PID) controller. Consequently, it is imperative that you engage an additional examiner to do a detailed review of the source code for ES&S voting machine software versions 6.2.0.0 and 6.3.0.0, to determine whether or not the source code contains a PID controller. I am qualified to do such an examination, as evidenced by my Curriculum Vitae in the attached Alabama Secretary of State case.

Regarding (2), the ES&S system contains a permanently open back door called iDRAC. Consequently, it is imperative that you engage an additional examiner, with at least CISSP certification, to do a detailed cybersecurity review, including iDRAC and penetration testing.

If either (a) the source code examiner determines that a PID controller is present, or (b) the cybersecurity examiner determines that the system is vulnerable to remote access, or both, then the system is not “safe from fraudulent or unauthorized manipulation,” and is therefore forbidden to be used under Election Code 122.001(a)(4).

Thank you for your prompt attention to these vital matters. All Texans are relying on you!

Sincerely,

/s/ *Walter C. Daugherity*

Walter C. Daugherity

Attachment: Expert declaration in the Alabama Secretary of State case

ATTACHMENT

DECLARATION OF EXPERT WALTER C. DAUGHERITY

WALTER C. DAUGHERITY declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct.

Introduction

1. I am a Senior Lecturer Emeritus in the Department of Computer Science and Engineering at Texas A&M University and also a computer consultant to major national and international firms, as well as to government agencies, including classified work.

2. Prior to my retirement in 2019, I taught computer science and engineering at both the undergraduate and graduate levels for 37 years, the last 32 years being at Texas A&M University. Courses I developed and taught include courses in artificial intelligence, expert systems, programming and software design, quantum computing, and cyberethics.

3. I have published 26 research articles related to expert systems, fuzzy logic, noise-based logic, and quantum computing from over $2.8 million in funded research projects, plus conference papers and other publications.

4. As a computer expert I have consulted for major national and international firms, including IBM Federal Systems Division, *New York Times*, *Washington Post*, *Los Angeles Times*, Southwestern Bell Telephone, Fulbright & Jaworski (Houston), and Phonogram B.V.

(Amsterdam), and also for government agencies such as Cheyenne and Arapaho Tribes of Oklahoma, Texas Department of Agriculture, U. S. Customs Service, and classified work.

5. Further details about my qualifications are included in my Curriculum Vitae attached as Exhibit A.

6. I analyzed the public record Cast Vote Records ("CVR") for numerous counties in the United States which use voting machine software from ES&S, including Pima County in Arizona. The CVR collects in spreadsheet format the selections contained on each ballot, in the order recorded through the tabulator machines, without any information that would identify the voter (i.e., no name, address, Social Security number, driver's license number, voter registration number, etc.).

7. I am informed that election officials in Alabama have either refused all Alabama Open Records Act (also known as Freedom of Information Act, or "FOIA") requests for their county's public record CVR's, or they have claimed that such information is not available. However, all counties in Alabama utilize voting machine software from ES&S, and to the best of my knowledge that software is functionally equivalent to the software used on ES&S voting systems elsewhere in the United States.

8. My detailed analysis below of the CVR data from Pima County, Arizona, which also uses ES&S tabulators, shows, in my expert opinion, that ballots can be, and in fact have been artificially processed through the tabulators tracking a Proportional-Integral-Derivative (PID) type control function in a closed-loop feedback system. A PID controller (or variations) is a software coded algorithm programmed to maintain a measured process variable (that is, an outcome, such as a ratio) at a pre-specified desired setpoint.

9. PID controllers are used everywhere, from cruise control in automobiles to Category III autoland for an aircraft making a landing when the runway is completely fogged in, to industrial automation of all kinds, such as robots, refineries and other chemical plants, manufacturing quality control, and self-driving cars.

10. An analysis of the actual cumulative ratios of the vote tallies for early mail-in and in-person votes prior to Election Day ("early votes") for the seventeen races in Pima County shows a significant and systematic decline in the cumulative ratio as counting progresses. For example, the graph in ¶ 22 below shows the first block of ballots being 75% for a candidate, the next block of ballots being 74% for the candidate, the next block of ballots being 73%, and so on, systematically declining all the way to Election Day.

11. This near straight-line decrease in the cumulative ratio falls within a narrow band for the races analyzed in Pima County. Such a uniform and predictable pattern is so statistically implausible that it would not occur without artificial manipulation.

12. As detailed below, my analysis shows to a reasonable degree of scientific and mathematical certainty that vote counting by ES&S electronic voting machines used in Pima County was manipulated and tightly controlled to reach predetermined outcomes. This manipulation could have been performed manually or by computer, but for reasons described below it is unlikely to have been performed manually.

The ES&S Electronic Voting Machines Were Used To Manipulate Early Vote Counting In Pima County, Arizona

13. In the November 2020 General Election there were numerous contests on the ballot in Pima County, Arizona, from the office of the Presidency down to local county races, and judicial retention questions, propositions, etc.

14. After the election I received the CVR public record report for Pima County, Arizona, from Benny White, one of the candidates for office in Pima County.

15. My analysis of the CVR demonstrates a PID function at work in all 17 races in Pima County I analyzed.

16. There were three main methods of voting: mail-in (absentee), early in-person, and Election Day voting. A very small percentage of ballots was cast by other means, such as remote ballot transmission as provided by the Uniformed and Overseas Citizens Absentee Voting Act ("UOCAVA") for members of the military, their families, and others.

17. In the case of mail-in (absentee) ballots, the general process in Pima County, Arizona, is similar to that prescribed at https://www.sos.alabama.gov/alabama-votes/voter/absentee-voting: Alabama voters write their county's Absentee Election Manager (usually the Circuit Clerk) to request an Absentee Ballot Application, receive the form, return the form with the required documentation, receive an absentee ballot by mail, and return the absentee ballot by mail with the required affidavit and notarization or witness attestation. To be valid, a mailed absentee ballot must be delivered to the county's Absentee Election Manager by noon on Election Day.

18. Since each of these steps takes an unpredictable amount of time, there is no expected pattern to the order in which mail-in ballots arrive to be counted and entered in the CVR.

19. For the November 3, 2020, election 526,319 ballot records are listed in the Pima County "2020 General Election Post Election CVR (Cast Vote Record) Aggregate" file, with CVR sequence numbers 1 through 526,332. (Thirteen of those numbers do not appear,

confirming that the total number of Cast Vote Records is 526,319, which equals 526,332 minus 13. The materials that I reviewed did not explain why these 13 entries were stricken.)

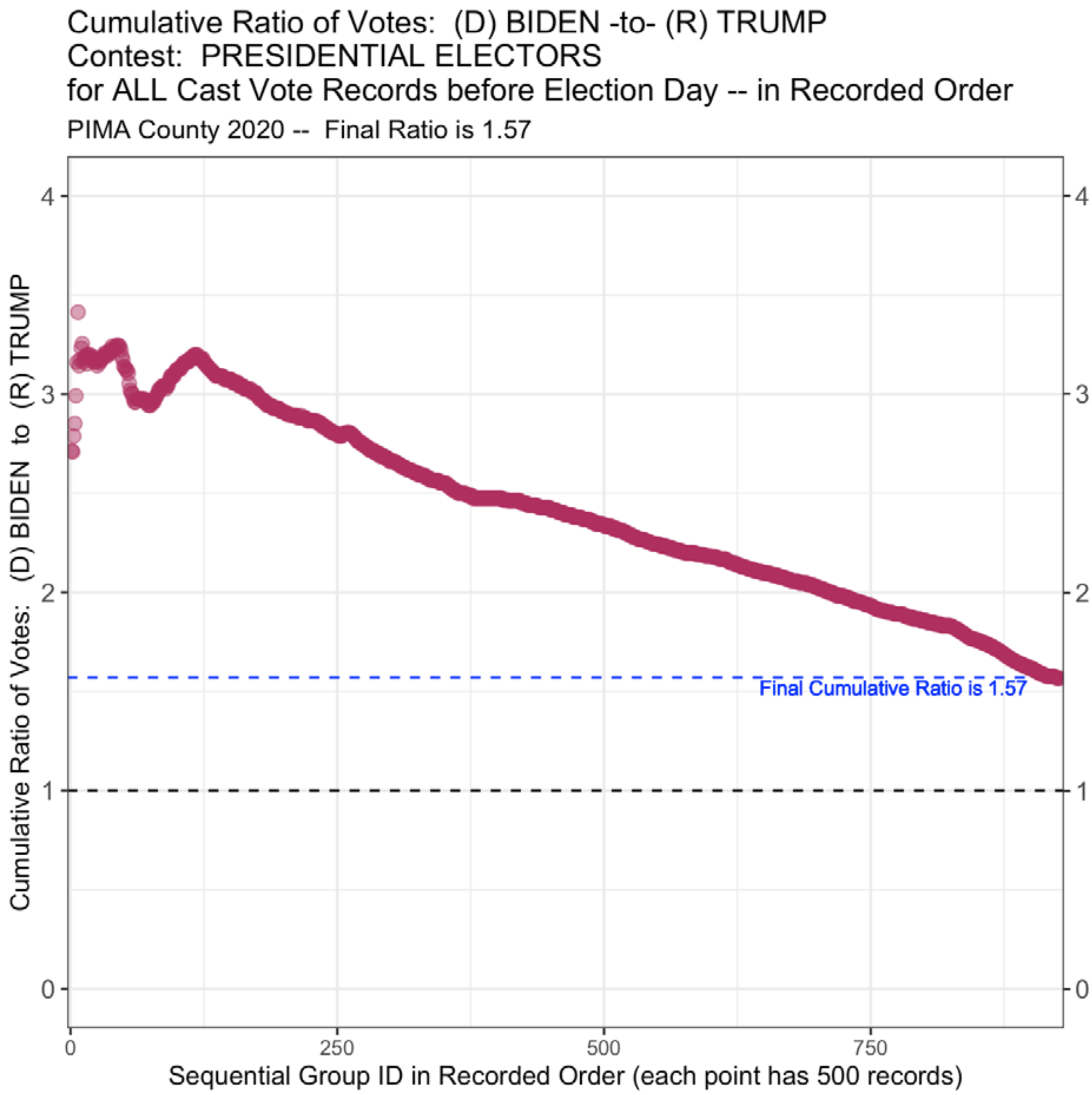
20. Since the early votes were not sorted and batched by precincts[1] before Election Day as Election Day votes were, by looking to see where in the CVR file consecutive ballots are all from the same precinct we can determine the point at which Election Day counting began. The first batch of ballots with consecutive precinct numbers starts with CVR# 413,241 for precinct 208, so the early votes are CVR# 1 through 413,239 (since CVR# 413,240 is one of the 13 missing numbers).

21. Graphing the CVR public record report data as the cumulative Democrat/Republican ratio in the data's CVR sequence shows that the CVR entries are not independent of each other or of their order in the CVR, which they should be. In other words, knowing one block of votes was 75% for a candidate should not allow one to predict whether the next block would be a higher or lower percentage, much less to predict that it would be 74% (instead of 63% or 85% or some other value).

22. This manipulated systematic decline is illustrated in the graph[2] below of this ratio in the Presidential race:

[1] Technically, the "precinct number" 1 to 249 in the CVR file is a *voting district* which is determined by actual precinct, U. S. House district, state Senate district, Board of Supervisors district, school district, etc.; each voting district requires a unique ballot. However, following common usage, we will also call these voting districts "precincts".

[2] All graphs were prepared at my direction by Cynthia Butler, a professional statistician.



23. This graph and the graphs of this ratio in 16 additional contests all show a similar and very consistent pattern that would not exist in independent data without artificial manipulation. After an initial fluctuation due to the small number of votes counted at first, the cumulative Democrat/Republican ratio over time as additional votes were recorded in the CVR public record report closely followed a downward sloping line. For the Presidential race this decline was from over 300% down to 157% by Election Day.

24. The common opinion that Democrats vote earlier than Republicans would not explain the lack of randomness between the data in the CVR graph. Further, although conventional wisdom suggests that strong supporters may vote early to demonstrate their support, and late deciders and late voters might cause a dropoff from the initial surge, this would only suggest a downward trend line without the precisely staggered step-down function described below.

25. Very small deviations from a downward sloping straight line indicate tight (strong) control, whereas wide deviations indicate weak or no control.

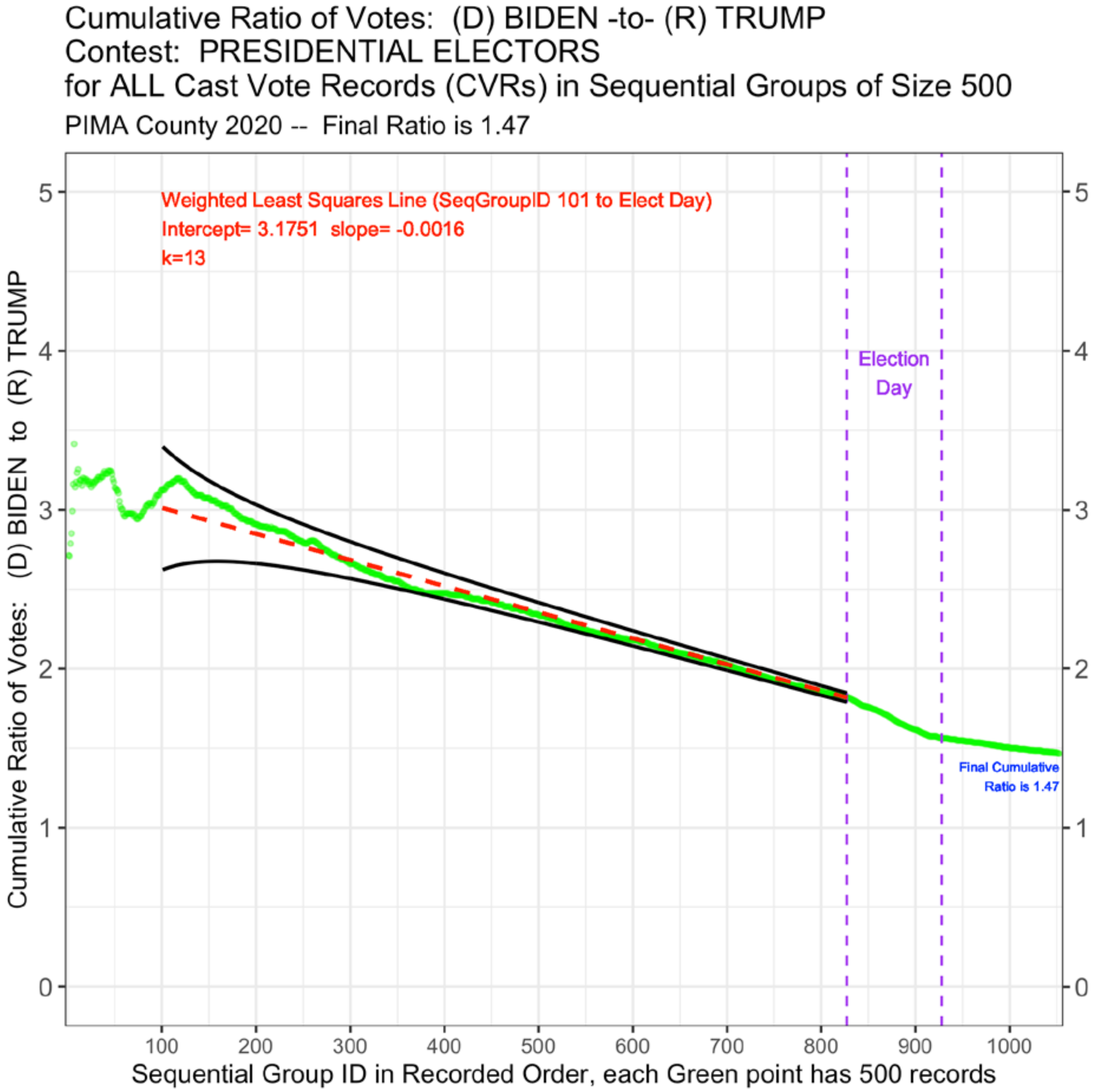
26. Since the effect of each additional vote on the cumulative ratio decreases as the number of votes increases, the deviation from a negative linear slope must be weighted in inverse proportion to the number of votes counted so far.

27. Also, to avoid the initial fluctuations due to the small number of votes at first, the following analysis begins after 50,000 votes, which is approximately 12% of the number of early votes recorded prior to November 3, 2020.

28. For the Presidential race, the least-squares linear regression trend line (the red dashed line in the following graph) has the equation

$$y = -0.0016x + 3.1751$$

where $\boldsymbol{x}$ is the sequential Group ID number.



29. Note how closely the actual CVR data (in green) follows the red trend line. To determine exactly how closely, we add the black boundary "curbs" (which must be weighted as described in ¶ 26) and find the narrowest curbs that contain all the green points. Also, as stated above, to avoid the initial fluctuations due to the small number of votes at first, the following analysis begins after 50,000 votes.

30. As in the graph in ¶ 22, ballots are grouped sequentially in batches of size 500 (Group 1 contains ballots 1-500, Group 2 contains ballots 501-1000, etc., in exactly the same

order as recorded in the CVR records), so the last Group before Election Day is Group 826. (See ¶ 20 for how it was determined that there were approximately 413,239 early votes counted prior to Election Day.)

31. To quantify the degree of control, the pair of narrowing black boundary lines in this graph shows a fixed percentage of deviation above and below a linear slope, weighted by the number of votes counted so far.

32. The boundary line equations are

$$y = (-0.0016x + 3.1751)\left(1 \pm \frac{k}{x}\right)$$

making $\frac{100k}{x}$ the percentage of deviation above and below a negative linear slope weighted by the number of votes counted so far. By testing integral values of ***k***, it was determined that setting ***k*** = 13 is the minimum value such that the black boundaries include *all* the green data points, making the maximum percentage deviation at Election Day only $\frac{100\cdot 13}{826} = 1.57\%$, an extremely close fit.

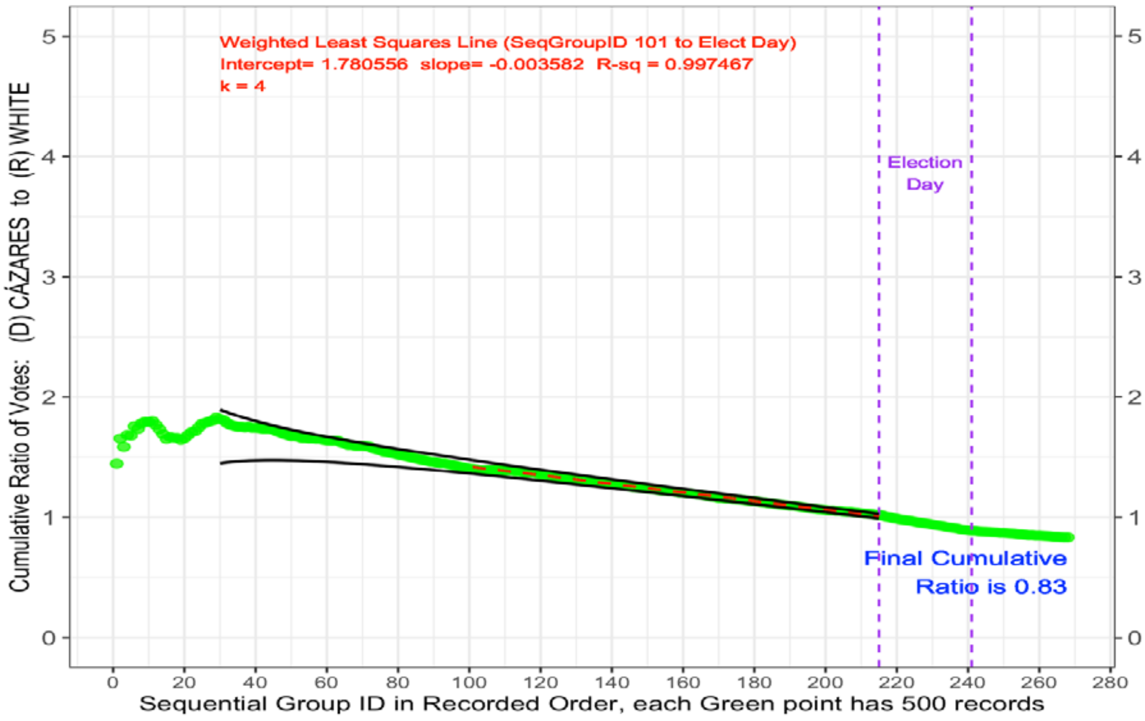
33. In statistical terms, the R^2 value for the red dashed line is 0.993, meaning that 99.3% of the total variation in the cumulative ratio is accounted for by the sequential Group number.

34. This means that after 50,000 votes out of a total of 413,239 early vote ballots have been counted, the cumulative Democrat/Republican ratio then follows a straight sloping line so closely that it must have been controlled.

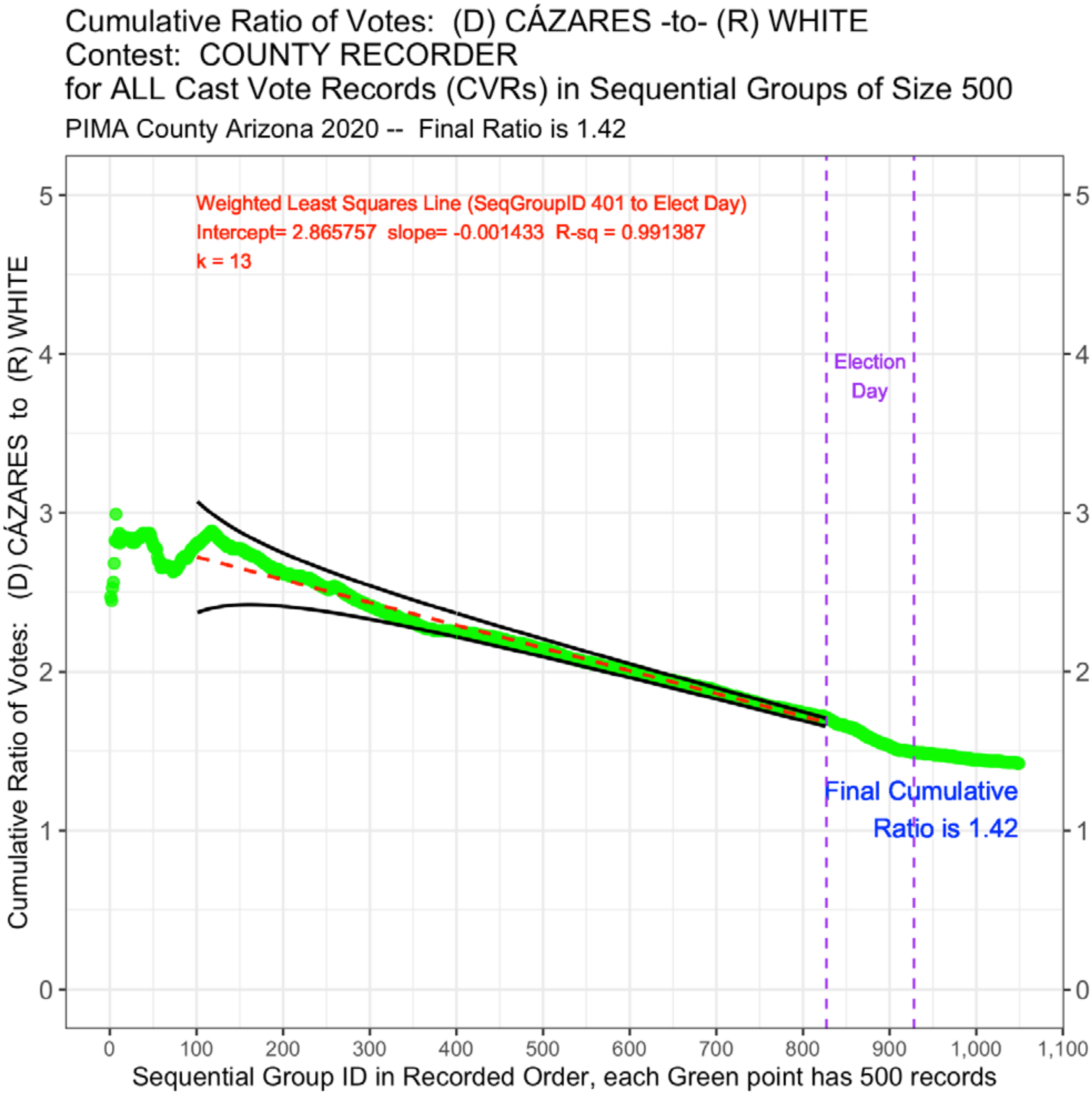
35. Put another way, after about 12% of the early votes are recorded, the next block of ballots is 75% for the Democrat candidate, the next block after that is 74%, the next block 73%, and so on, systematically declining all the way to Election Day.

36. After approximately the first twelve percent of votes are tabulated, the early votes are predictable and dependent in the relationship between one block of votes and the next. Such predictability and dependence would not occur without artificial manipulation. Achieving such predictability requires what should be independent votes to be artificially manipulated to form the downward sloping line for the cumulative vote ratio. In my expert opinion such predictability is so statistically improbable as to be impossible without manipulation or control and thus demonstrates to a reasonable degree of scientific and mathematical certainty that the tabulation of these ballots was artificially controlled.

37. For confirmation, below are two additional graphs, one for Board of Supervisors District 4, and one for County Recorder, which are similarly predictable. The boundary curbs were also added, and the R^2 values for the red dashed lines are 0.997 and 0.991, respectively, confirming that over 99% of the total variation in the cumulative ratio is accounted for by the sequential Group number in both races. In the case of the Board of Supervisors District 4 race, $\boldsymbol{k} = 4$ is the minimum integral value such that the black boundaries include *all* the green data points, again giving a maximum percentage deviation at Election Day of less than 2%.



Cumulative Ratio of Votes: (D) DIAMOND -to- (R) CHRISTY
Contest: BOARD OF SUPERVISORS, DIST. 4
for ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 -- Final Ratio is 0.83



38. Note that neither the current Alabama statutory election audit procedures[3] nor the various forms of risk-limiting audits used by other states would have detected this controlled manipulation, since they do not take into account the sequence that votes are recorded.

[3] Code of Alabama Title 17, the Alabama Voter Confidence Act #2021-446, *et al.*

Proportional-Integral-Derivative (PID) Controller

39. The standard method of producing such control as described above is to use a Proportional-Integral-Derivative (PID) controller in a closed-loop feedback system. As noted above, PID controllers are used everywhere, from cruise control in automobiles to Category III autoland for an aircraft making a landing when the runway is completely fogged in, to industrial automation of all kinds, such as robots, refineries and other chemical plants, manufacturing quality control, and self-driving cars.

40. By using all three factors (Proportional, Integral, and Derivative), a PID controller is the simplest (and therefore the most widely-used) design which controls both steady-state and transient responses, that is, it is able to reach and maintain a predetermined setpoint (outcome) despite unplanned disturbances. For example, in a Category III autoland situation when the airport is completely fogged in, the PID controller aims the aircraft for the start of the runway on a 3° glide slope, but if a sudden gust of wind pushes the nose down, the PID controller will activate the control surfaces to increase attitude and get back on the desired glide slope.

41. As a proof of concept, I programmed a PID controller with a linearly-ramping decreasing setpoint (the red dashed line) to produce the observed cumulative ratio and obtained good convergence after tuning the PID parameters to $K_p = 0.070$, $K_i = 0.300$, and $K_d = 0$. The system was not optimum (it was underdamped) but it was stable (with no unbounded oscillation) and closely tracked the continuing downward setpoint change along the red dashed line. Since the other 16 races had the same inexplicable downward slope, they would also match the same PID controller using their corresponding linearly-ramping decreasing setpoints.

42. The complete collection of graphs for all 17 races is attached as Exhibit B. Note that almost all of the graphs are almost identical to one another in shape, down to the twin peaks at the beginning and the "hiccup" when about 25% of the early votes have been counted.

Consistency with Pima County Whistleblower's Allegations

43. My analysis above is based on the data that I reviewed, and not on any consideration of specific allegations of fraud. It was brought to my attention on May 4, 2022, subsequent to the analysis described above, that a Pima County whistleblower's email addressed to Criminal.Division@usdoj.gov and Arizona legislators with a subject line of "Meeting held by Pima County Democrats (Voter Fraud Planning meeting)" included allegations consistent with, and corroborative of, my conclusions. The whistleblower's full email is attached as Exhibit C. My independent analysis stands separate from this email, but the similarity between the allegations in the email and the result of my analysis is striking.

44. Specifically, the following allegations were made by the whistleblower, reproduced here verbatim (without editing or spelling corrections or any other changes) from the full email in Exhibit C:

a. [Allegation] Please be advised that Pima County Recorder, located at 240 N Stone Ave, Tucson, AZ 85701 in Pima County Arizona and the Democratic Party added "fraud votes" in the initial count to the Vote-By-Mail (VBM) totals released at 8pm on Nov 3rd 2020.

b. [Allegation] There were approximately 35,000 fraud votes added to each democrat candidate's vote totals. Candidates impacted include county, state and federal election candidates. Through the utilization of the automated ballot count machines in Pima County Elections, my understanding is that 35,000 was embedded into each democrat candidate's total votes.

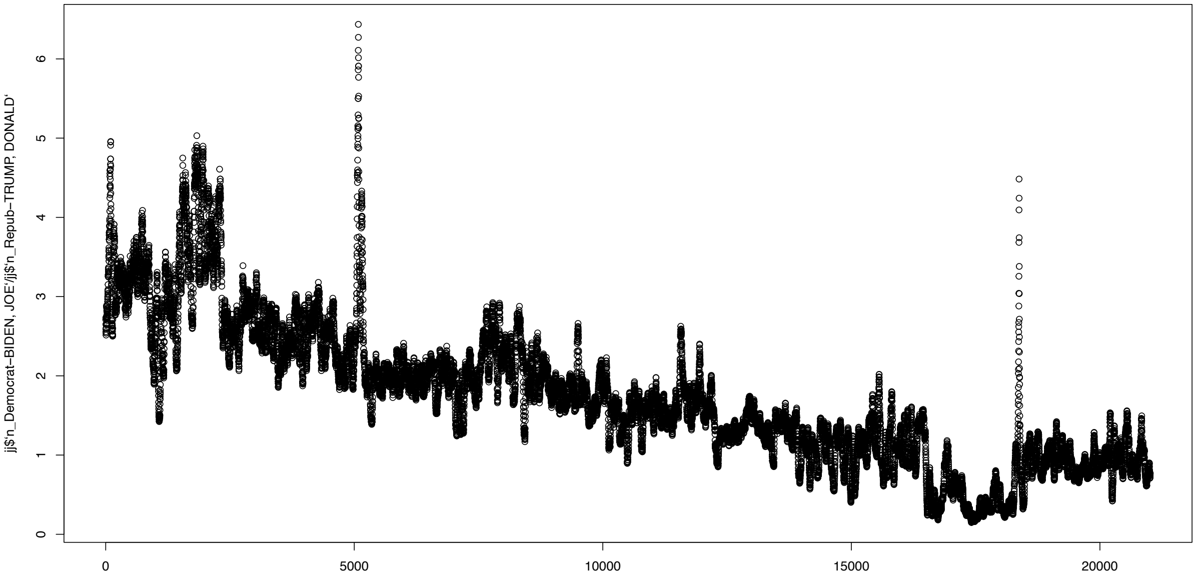
c. [Allegation] When I asked "how in the world will 35,000 be kept hidden or from being discovered", it was stated that "spread distribution will be embedded across the total registered voter range and will not exceed the registered voter count, and the 35,000 was determined allowable for pima county based on our county registered voter count". It was also stated that "total voter turnout versus total registered voters determine how many votes we can embed. The embedding will auto adjust based on voter turn-out." Because the "embed votes are distributed sporadically all embedded votes will not be found, if audited, because the embeds are in groups of approximately 1,000. This is so the county recorder can declare an orversite issue or error as a group of 1,000 is a normal and acceptable error." "Maricopa County's embed totals will be substantially higher than Pima due to embeds being calculated based on the total number of registered voters."

d. [Allegation] When I asked "has this ever been tested? and how do we know it works?" The response was "Yes, this has been testing and has shown significant success in Arizona Judicial Retention Elections since 2014 even undetectable in post audits because no candidate will spend the kind of funds needed to audit and contact voters to verify votes in the full potential of total registered voters which is more then 500,000 registered voter. This year our Secretary of State has removed precinct level detail for election night releases so canidates can't see precinct over-votes".

45. I note that the whistleblower's allegation in ¶ 44(c) that "The embedding [of fraudulent votes] will auto adjust based on voter turn-out" is consistent with the tight control quantified in ¶ ¶ 31-33. It is also consistent with a PID controller's having been used, since "auto adjust" is exactly what a PID controller is designed to do (see ¶ ¶ 39-41).

46. To evaluate the whistleblower's allegation in ¶ 44(c) that "the embeds are in groups of approximately 1,000," the CVR public record report for the Presidential race was scanned for any groups of 1,000 votes with an abnormally high proportion of votes for the Democrat candidate.

47. This scanning process identified multiple groups of 1,000 votes with an abnormally high percentage of votes for the Democrat candidate, as graphed here with an *x* scale of 25:



The tallest spike, near *x* = 5000, is approximately Cast Vote Record numbers 127,024 through 128,023. This block of 1,000 votes is over 6 to 1 Democrat/Republican, while the preceding 1,000-vote block is less than 3 to 1 Democrat/Republican, and the average ratio for 1,000-vote blocks up to Election Day is even less than this preceding block. This is consistent with the whistleblower's allegation.

48. Physical ballots corresponding to CVR numbers 127,024 through 128,023 (approximately) should therefore be examined for authenticity (genuine VoteSecur™ paper from Rolland with the embedded ghost taggant, verified outer envelope signature, unbroken chain of custody, etc.).

49. Note that, if the whistleblower's allegation of 35,000 Democrat "fraud votes" is verified by a physical audit of these ballot numbers, then because the cumulative Democrat/Republican ratio was 1.57 at Election Day, there would also need to be 35,000 / 1.57 = 22,293 Republican "fraud votes" included in order to spread them out and attempt to avoid detection, for a total of 35,000 + 22,293 = 57,293, or about 57 1,000-vote blocks. Thus the physical ballots corresponding to the highest 57 spikes deviating from the downward slope are most likely to be the alleged fraudulent votes.

50. After the other 56 spikes are identified, the corresponding physical ballots should also be examined for authenticity (genuine VoteSecur™ paper from Rolland with the embedded ghost taggant, verified outer envelope signature, unbroken chain of custody, etc.).

51. The same spike analysis should also be done on the other contests in Pima County.

52. Being able to find these spikes, like the one for CVR numbers 127,024 to 128,023 (approximately), confirms the sworn statement of Dr. Eric Coomer, who said, "It would be

illegal, highly illegal [to change votes]. So that's a fact. And it would be impossible to do undetected." [4]

53. The whistleblower also alleged in ¶ 44(c) that the number of "fraud votes" to be embedded was planned to "not exceed the registered voter count" (presumably by precinct) in order to avoid detection.

54. To reiterate, the statements in ¶ 44 are allegations by a whistleblower and the statements in ¶¶ 45-53 are mine.

55. Software to perform this type of manipulation could be installed in a variety of ways, including vendor programming, operating system components, open-source or commercial off-the-shelf libraries, remote access, viruses or other malware, etc.

Conclusions

56. The evidence detailed above overwhelmingly demonstrates to a reasonable degree of scientific and mathematical certainty that the sequence of the CVR data in Pima County shows artificial control within ES&S voting systems used there. Thus, artificial control by ES&S voting systems used in Alabama is also possible.

57. Such control could be implemented by manual means or by a computer algorithm, such as a PID controller or some equivalent mathematical procedure. However, the alternating oscillations above and below the trend line, with decreasing deviations from the trend line, would require a prohibitive amount of calculation to accomplish by hand, not to mention the careful manual sorting of many thousands of batches of ballots to achieve the actual curves observed in the 17 races analyzed. This means that some type of computer algorithm is

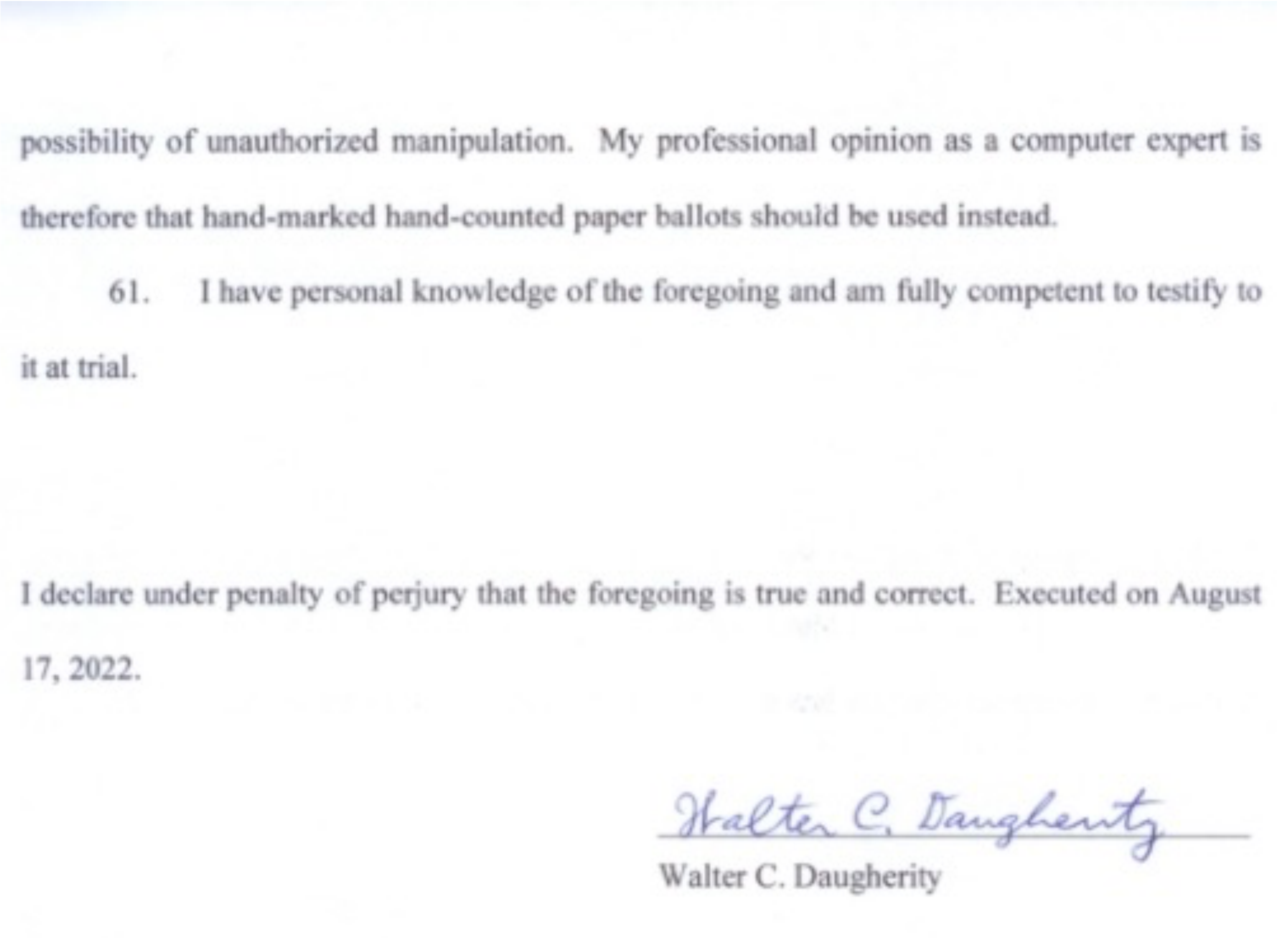
[4] Deposition of Eric Coomer, September 23, 2021, pp. 98-101.

indicated, and a PID controller is the simplest control function that would exhibit following a trend line with alternating oscillations above and below the trend line with decreasing deviations from the trend line.

58. As noted above, I am informed that election officicals in Alabama have refused all Alabama Open Records Act (also known as Freedom of Information Act, or "FOIA") requests for their county's public record CVR or claim that such information is not available. I am prepared to analyze any Alabama CVR which is released to the public to determine whether or not it also exhibits artificial control. Since all counties in Alabama utilize voting machine software from ES&S, and to the best of my knowledge that software is functionally equivalent to the software in ES&S tabulators used in Pima County, CVR's from the ES&S electronic voting machines used in Alabama may likewise reveal artificial control. The analysis above of the results of using ES&S voting machine software in Arizona is thus directly applicable and relevant to Alabama.

59. Such manipulating software could be installed in a variety of ways, including vendor programming, operating system components, open-source or commercial off-the-shelf libraries, remote access, viruses or other malware, etc.

60. Unless and until future proposed electronic voting systems (including hardware, software, source code, firmware, etc.) are made completely open to the public and also subjected to scientific analysis by independent and objective experts to determine that they are secure from manipulation or intrusion, in my professional opinion as a computer expert, electronic voting systems should not even be considered for use in any future elections, as they cannot be relied upon to generate secure and transparent election results free from the very real



possibility of unauthorized manipulation. My professional opinion as a computer expert is therefore that hand-marked hand-counted paper ballots should be used instead.

61. I have personal knowledge of the foregoing and am fully competent to testify to it at trial.

I declare under penalty of perjury that the foregoing is true and correct. Executed on August 17, 2022.

Walter C. Daugherty

Walter C. Daugherty

EXHIBIT A

Curriculum Vitae of Walter C. Daugherity

Walter C. Daugherity
10895 Lakefront Drive
College Station, TX 77845
(979) 845-1308 (Office)
Walter.Daugherity@post.Harvard.edu

EDUCATION

Ed.D., Mathematical Education, Harvard University, Cambridge, Massachusetts, 1977.
Dissertation: "On the Ordering of Topics in the Teaching of Mathematics."
Advisor: Marc Lieberman.

M.A.T., Mathematics, Harvard University, Cambridge, Massachusetts, 1967 (age 20).

B.S., Mathematics, Oklahoma Christian College, Oklahoma City, Oklahoma, 1966 (3 years). Minors: Physics and chemistry, German.

EXPERIENCE

1973 to present

Daugherity Brothers, Inc., (Computer consultants), Bethany, Oklahoma. Co-founder, chairman, and president. Clients include IBM Federal Systems Division, New York Times, Washington Post, Los Angeles Times, Cheyenne and Arapaho Tribes of Oklahoma, Southwestern Bell Telephone, Fulbright & Jaworski (Houston), Texas Department of Agriculture, Phonogram B.V. (Amsterdam), and U. S. Customs Service.

1987 to present

Texas A & M University, College Station, Texas. Visiting Assistant Professor/Senior Lecturer/Senior Lecturer Emeritus, Departments of Computer Science and Engineering and Electrical and Computer Engineering, College of Engineering.

1989-91

Texas A & M University System, College Station, Texas. Director, Knowledge Systems Research Center, Computer Science Division of the Texas Engineering Experiment Station.

1984-87 Blinn College, Brenham, Texas. Computer science instructor. Part-time 1984-86, full-time 1986-87.

1978-80 Rose State College, Midwest City, Oklahoma. Data processing instructor (part-time).

1971-73 ECRM, Bedford, Massachusetts. Systems programmer.

1970-71 Harvard Computing Center, Cambridge, Massachusetts. Telecommunications specialist.

1969-70 Computer-Aided Instruction Laboratory, Harvard University, Cambridge, Massachusetts. Systems programmer.

1968-70 Harvard University, Division of Engineering and Applied Physics, Cambridge, Massachusetts. Teaching fellow (for George Mealy and Thomas Bartee).

1967 Driscoll Junior High School, Brookline, Massachusetts. Mathematics teacher.

1967 University of Oklahoma Medical Center Computing Facility, Oklahoma City, Oklahoma. Programmer.

1966 University of Central Oklahoma Data Processing Center, Edmond, Oklahoma. Programmer.

1965 Oklahoma Christian University of Science and Arts, Oklahoma City, Oklahoma. Statistical programmer.

1963 University of Oklahoma Computer Center, Norman, Oklahoma. Lab instructor.

RESEARCH AND DESIGN

1. Refereed Publications

Daugherity, W. C., and Kish, L. B., “More on the Reference-Grounding-Based Search in Noise-Based Logic,” *Fluctuation and Noise Letters*, Vol. 21, No. 3, 2250023, 2022.

Kish, L. B., and Daugherity, W. C., “Entanglement, and Unsorted Database Search in Noise-Based Logic,” *Applied Sciences*, Vol. 9, No. 15, 3029, 2019.

Kish, L. B., and Daugherity, W. C., “Noise-Based Logic Gates by Operations on the Reference System,” *Fluctuation and Noise Letters*, Vol. 17, No. 4, 1850033, 2018.

Daugherity, W. C., and Coulson, R. N., “Knowledge Engineering for Sustainable Agriculture Management,” *Proceedings of ICAST 2001 Conference* (Beijing, China, November 2001), 2:266, 2001.

Coulson, R. N., Saarenmaa, H., Daugherity, W. C., Rykiel, E. J., Saunders, M. C., and Fitzgerald, J. W., “A Knowledge System Environment for Ecosystem Management,” book chapter in Klopatek, J. and Gardner, R. (eds.), *Landscape Ecological Analysis: Issues and Applications*, Springer-Verlag, 57-79, 1999.

Coulson, R. N., Daugherity, W. C., Rykiel, E. J., Saarenmaa, H., and Saunders, M. C., “The Pragmatism of Ecosystem Management: Planning, Problem Solving and Decision Making with Knowledge-Based Systems,” *Proceedings of Eco-Informa ’96 Global Networks for Environmental Information Conference* (Lake Buena Vista, Florida, November 1996), 10:342-50, 1996.

Coulson, R. N., Fitzgerald, J. W.*, Daugherity, W. C., Oliveria, F. L., and Wunneburger, D. F., “Using Spatial Data for Integrated Pest Management in Forest Landscapes,” *Proceedings of the 11th Conference on Geographic Information Systems: Integrating Spatial Information Technologies for Tomorrow* (Vancouver, British Columbia, Canada, 1997).

Daugherity, W. C.; Harris, C. E., Jr.; and Rabins, M. J., “Introducing Ethics and Professionalism in REU Programs,” *Proceedings of the 1995 World Conference on Engineering Education* (Minneapolis, Minnesota, October 1995).

Coulson, R. N., Daugherity, W. C., Vidlak, M. D.*, Fitzgerald, J. W.*, Teh, S. H.*, Oliveria, F. L., Drummond, D. B., and Nettleton, W. A., “Computer-based Planning, Problem Solving, and Decision Making in Forest Health Management: An Implementation of the Knowledge System Environment for the Southern Pine Beetle, ISPBEX-II,” *Proceedings of the IUFRO Symposium on Current Topics in Forest Entomology* (Maui, Hawaii), 1995.

Yen, J., Daugherity, W. C., Wang, H.*, and Rathakrishnan, B.*, “Self-Tuning and Self-Learning Fuzzy Systems,” book chapter in Yen, J., Langari, R., and Zadeh, L. (eds.), *Industrial Applications of Fuzzy Logic and Intelligent Systems*, IEEE Press, 1995.

* Graduate Research Assistant I funded

Daugherity, W. C., Video review of *Introduction to Biological and Artificial Neural Networks for Pattern Recognition,* by Steven K. Rogers, in *IEEE Transactions on Neural Networks*, Vol. 5, No. 5, 1994.

Teh, S. H.*, Daugherity, W. C., and Coulson, R. N., "A User-Centric Methodology for Building Usable Expert Systems," *Proceedings of the 7th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems* (Austin, Texas, May-June 1994), 45-48, 1994.

Daugherity, W. C., "A Neural-Fuzzy System for the Protein Folding Problem," *Proceedings of the Third International Workshop on Industrial Fuzzy Control & Intelligent Systems (IFIS `93)* (Houston, Texas, December 1993), 47-49, 1993.

Daugherity, W. C., "A Partially Self-Training System for the Protein Folding Problem," *Proceedings of the World Congress on Neural Networks (WCNN `93)*, (Portland, Oregon, July 1993). Invited paper.

Yen, J., Wang, H.*, and Daugherity, W. C., "Design Issues of Reinforcement-Based Self-Learning Fuzzy Control," *Proceedings of the World Congress on Neural Networks (WCNN `93)*, (Portland, Oregon, July 1993).

Daugherity, W. C., "Characterizations of Fuzzy Operations," *Proceedings of the Second International Workshop on Industrial Fuzzy Control & Intelligent Systems* (College Station, Texas, December 1992), 234, 1992.

Yen, J., Wang, H.*, and Daugherity, W. C., "Design Issues of a Reinforcement-Based Self-Learning Fuzzy Controller for Petrochemical Process Control," *Proceedings of North American Fuzzy Information Processing Society* (Puerto Vallarta, December 1992), 1992.

Yen, J., Wang, H.*, and Daugherity, W. C., "An Adaptive Fuzzy Controller with Application to Petroleum Processing," *Proceedings of IFAC Workshop on Intelligent Manufacturing Systems* (Dearborn, October 1992), 1992.

Yen, J., Daugherity, W. C., and Rathakrishnan, B.*, "Fuzzy Logic and Its Application to Process Control," *Proceedings of CAPA Technology Conference* (Houston, May 1992), 78-86, 1992.

* Graduate Research Assistant I funded

Daugherity, W. C., Rathakrishnan, B.*, and Yen, J., “Performance Evaluation of a Self-Tuning Fuzzy Controller,” *Proceedings of the IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)* (San Diego, March 1992), 1992.

Daugherity, W. C., “An Application of Geometrical Reasoning to a Combinatorial Problem,” *Proceedings of the Seventh Annual Conference on Applied Mathematics* (Edmond, Oklahoma, April 1991), pp. 226-232, 1991.

Daugherity, W. C., Review of *Data Communications Dictionary*, by Charles J. Sippl, in *Computing Reviews*, Vol. 17, No. 9, pp. 335-336, 1976.

Daugherity, W. C., “Circuits for Dial-up and Local Use of a Stand-alone PDP-8,” *Proceedings of the Digital Equipment Computer Users Society*, Vol. 2, No. 2 (Los Angeles, December 1975), pp. 413-414, 1976.

Daugherity, W. C., Review of *Effective Use of ANS COBOL Computer Programming Language*, by Laurence S. Cohn, in *Computing Reviews*, Vol. 16, No. 10, p. 441, 1975.

Manwell, T., Daugherity, W., Desch, S., and Stolurow, L., “Tom Swift and His Electric Bilingual Grandmother,” *ACM SIGCUE Bulletin*, Vol. 7, No. 1, pp. 5-17, 1973.

Daugherity, W. C., “A Telephone Amplifier,” *Transactions of the Oklahoma Junior Academy of Science*, Vol. IV, pp. 130-132, 1961.

* Graduate Research Assistant I funded

2. Other Publications

Daugherity, W. C., “Honors Section,” in Rabins, M. J., and Harris, C. E. Jr. (eds.), *Engineering Ethics Teaching Manual*, 1997.

Daugherity, W. C., “Honors Section,” in Rabins, M. J., and Harris, C. E. Jr. (eds.), *Engineering Ethics Teaching Manual*, 1996.

Allen, G. D., Nelson, P., Jarvis, R. D., and Daugherity, W. C., “System Impact of Hit Assessment Capability for NPB Discrimination: Analysis of the Case of No-Hit Assessment,” *Weapons Lab/TALN Technical Report*, Kirtland Air Force Base, May, 1990.

3. Other Conference Papers and Presentations

Coulson, R. N., and Daugherity, W. C., "A Knowledge Engineering Approach for Ecosystem Management," 11th Annual Landscape Ecology Symposium, International Association for Landscape Ecology - Integration of Cultural and Natural Ecosystems Across Landscapes: Applications of the Science, Galveston, Texas, 1996.

Coulson, R. N., and Daugherity, W. C., "Decision Support Systems for Forest Pests: Where Do All the Knowledge-Based Systems Go?", North American Forest Insect Work Conference, San Antonio, Texas, 1996.

Daugherity, W. C. and Coulson, R. N., SPBEBE (Economic and Environmental Impact Assessment for Southern Pine Beetle Suppression Projects), computer code, developed for the USDA Forest Service, Forest Health Protection, 1996-1997.

Coulson, R. N., and Daugherity, W. C., "Knowledge System Environment for Ecosystem Management," Global Studies Seminar, Battelle Pacific Northwest Laboratories, Richland, Washington, 1995.

Daugherity, W. C. and Coulson, R. N., ISPBEX-II (Integrated Southern Pine Beetle Expert System), computer code, developed for the USDA Forest Service, Forest Health Protection, 1994.

Daugherity, W. C., and Yen, J., "Tutorial on Neuro-Fuzzy Systems," Third International Workshop on Industrial Fuzzy Control & Intelligent Systems Houston, Texas, December 1993.

Daugherity, W. C., "Introduction to LISP with an On-line Demonstration," Houston Geotech '91, Houston, Texas, 1991.

Daugherity, W. C., "The Universal Classification Problem," South Central Regional Conference of the Association for Computing Machinery, Austin, Texas, 1984.

4. Research Projects

"Remote Laboratory Data Entry and Retrieval System," Texas Department of Agriculture, Walter C. Daugherity, 1986, $3,000 (Daugherity 100%).

"Electrochemical Modeling of a Sinter Plate, Sealed Design Nickel-Cadmium (Ni-Cd) Battery Cell," National Aeronautics and Space Administration, Ralph E. White, Walter C. Daugherity, 1 graduate student, 1989, 25% of my salary 1989-90 (Daugherity 100%).

"Application of Reasoning under Uncertainty to Process Control," Texaco, Walter C. Daugherity and John Yen, 1 graduate student; competitive and peer-reviewed, September 1990, $18,000.

"Design of a Computational Classroom," Texas A & M University, Walter C. Daugherity, September 1990-May 1991, $60,000 (Daugherity 100%).

"Design of a Second Computational Classroom," Texas A & M University, Walter C. Daugherity, January 1991-December 1992, $153,000 (Daugherity 100%).

"Development of Honors Courses in Artificial Intelligence and Analysis of Algorithms," Texas A & M University, Walter C. Daugherity, James Abello and Arkady Kanevsky, 2 graduate students, competitive, September 1991-May 1991, $11,000 (Daugherity 50%).

"Integrated Southern Pine Beetle Expert System"; USDA Forest Service; Robert N. Coulson, Walter C. Daugherity, and Jeffrey W. Fitzgerald; 5 graduate students; competitive and peer-reviewed; 1985-1992, $974,120.

"Distributed Data-Base Support for the ISPBEX Expert System"; USDA Forest Service; Robert N. Coulson, Walter C. Daugherity, and Jeffrey W. Fitzgerald; 1 graduate student; competitive and peer-reviewed; 1992-93; $35,000.

"Integrated Southern Pine Beetle Expert System II"; USDA Forest Service; Robert N. Coulson, Walter C. Daugherity, and Jeffrey W. Fitzgerald; competitive and peer-reviewed; March 1993-February 1994; competitive and peer-reviewed; $170,000.

"Ecological Modelling of Regional Responses to Global Changes: A Knowledge System Environment for Planning, Problem-Solving and Decision Making"; Battelle Pacific Northwest Laboratory; Robert N. Coulson and Walter C. Daugherity; competitive and peer-reviewed; June-December 1995; $39,996.

"Fitness of a Genetically Modified *Gliocladium virens* in Soil and Rhizosphere"; USDA Cooperative State Research Service; Charles M. Kenerley and Walter C. Daugherity; 1 senior associate, 2 graduate students, and 1 undergraduate student; competitive and peer-reviewed; September 1996-August 2001; $254,450 (Daugherity 50%).

“Southern Pine Beetle Biological Evaluation and Economic Evaluation Program Conversion”; USDA Forest Service, Forest Health Protection; Robert N. Coulson (PI) and Walter C. Daugherity (Co-PI); competitive and peer-reviewed; 1996-1997; $16,421.

“The Texas Imported Fire Ant Survey: The Fire Ant Spatial Information Management System (FASIMS)”; Texas Agricultural Experiment Station; Robert N. Coulson (PI) and S. Bradleigh Vinson, Maria D. Guzman, Douglas F. Wunneburger, and Walter C. Daugherity (Co-PI’s); competitive and peer-reviewed; January 1998-December 1998; $50,000.

“Special Topics in Computer Science Concepts and Programming”; Academy for Advanced Telecommunications and Learning Technologies; Walter C. Daugherity; competitive and peer-reviewed; June 1998-May 1999; $5,000 (Daugherity 100%).

“Object Modeling Techniques Support for National Simulation Center Tactical Directorate”; U. S. Army through prime contractor Cubic Applications, Inc.; Walter C. Daugherity, James A. Wall, and José Salinas; competitive; September 1998-April 1999; $74,498 (Daugherity 20%).

“The Fire Ant Spatial Information Management System (FASIMS)”; Texas Department of Agriculture, Texas Imported Fire Ant Research and Management Plan; Robert N. Coulson (PI) and Douglas F. Wunneburger, S. Bradleigh Vinson, and Walter C. Daugherity (Co-PI’s); competitive and peer-reviewed; 1999-2001; $220,000.

“Evaluating the Impact of Southern Pine Beetle on Ecologically Sustainable Forest Management”; USDA Forest Service; Robert N. Coulson and Walter C. Daugherity; 1 graduate student and 1 undergraduate student; competitive and peer-reviewed; 2000-2003, $90,000.

“Honey Bee Initiative”; State of Texas; Robert N. Coulson (PI), Walter C. Daugherity (Consultant); 2 graduate students; competitive; September 2001-August 2002; $40,000.

“Increasing Computer Science Retention by Developing and Deploying Self-Paced Learning Modules”; State of Texas; Jennifer Welch and Frank Shipman (Co-PI’s), Lawrence Petersen, Walter C. Daugherity, and Lauren Cifuentes (Key

Personnel); 10 undergraduate students; competitive; June 2002-August 2004; $422,692.

“Facilitating the Transition to Java in High School Computer Programming Classes”; Texas A&M University System Academy for Educator Development; Walter C. Daugherity; 1 graduate student; competitive and peer-reviewed; December 2003-September 2004; $2,966 (Daugherity 100%).

“Instructional Technology Enhancements for Computer Teaching Labs,” Texas A&M University, Walter C. Daugherity, competitive, January 2004-August 2004, $20,000 (Daugherity 100%).

“Increasing Computer Science Retention with Peer Teachers and Learning Modules”; State of Texas; Valerie Taylor and Jennifer Welch (Co-PI’s), Lawrence Petersen, Walter C. Daugherity, and Joseph Hurley (Key Personnel); undergraduate students; competitive; September 2004-August 2005; $173,158.

Cumulative total: $2,845,801

5. Research Proposals
   Note: Funded proposals are listed in section 4 above.

   “Automated Support for VLSI Standard Cell Optimization,” Texas Advanced Technology Program, Walter C. Daugherity, competitive and peer-reviewed, July 1989, not funded, $233,887.

   “Integration of Computer Software Models for NiCd Battery Design,” National Aeronautics and Space Administration, Ralph E. White and Walter C. Daugherity, competitive and peer-reviewed, 1990, not funded, $125,000.

   “Innovative Use of Supercomputers and Parallel Computers in Grades K-8,” Department of Energy, Paul Nelson, Walter C. Daugherity and Bahram Nassersharif, competitive and peer-reviewed, December 1990, preproposal submitted, $885,000.

   “Integration of Texas Junior Colleges into State and National Computer Networks,” Texas Advanced Technology Program, Walter C. Daugherity and Charles H. Beard, competitive and peer-reviewed, July 1991, not funded, $174,219.

“Adaptive Fuzzy Control for Industrial Processes,” Texas Advanced Research Program, John Yen and Walter C. Daugherity, competitive and peer-reviewed, July 1991, not funded, $177,064.

“Development of a Fuzzy Logic Tuner for a PID Controller,” Texaco, John Yen and Walter C. Daugherity, 1992-93, not funded, $200,000.

"National Center For Ecological Analysis and Synthesis," National Science Foundation; Robert N. Coulson, Walter C. Daugherity *et al.*, competitive and peer-reviewed, July 1994, not funded, $10,000,000.

"Development of a Fungal Growth Model for Risk Assessment," Texas Advanced Research Program, Charles M. Kenerley and Walter C. Daugherity, competitive and peer-reviewed, July 1995, not funded, $203,792.

"Intelligent Vehicle Navigation System," Texas Advanced Technology Program, Walter C. Daugherity and Jeffrey W. Fitzgerald, competitive and peer-reviewed, July 1995, not funded, $195,058.

"Innovative Programs to Increase the Enrollment in Computer Science," Texas Technology Workforce Development Grant Program, Valerie Taylor and Frank Shipman (co-PI's), Lawrence Petersen, Walter C. Daugherity, and Joseph Hurley (Key Personnel), competitive and peer-reviewed, March 2005, pending, $69,760.

6. New Design Methods, Techniques, or Concepts Developed

Null Modem

I independently invented the null modem in 1969 and constructed one for Harvard University (which is still operational!).

Computer Keyboard National Standard

As a member of the Harvard-MIT Terminal Committee, I participated in the development of the national standard for computer keyboards (*e.g.*, putting braces above brackets for the benefit of programming languages). Nearly every computer terminal and keyboard since then (*e.g.*, VT100, PC) uses this layout.

Integrated User Training

I invented the method of training users about additional features of an application program by integrating the information with the operation of the program (see Manwell, Daugherity, *et al.* under Publications, above). This is now widely adopted, *e.g.*, by Microsoft for its Windows operating systems in the "Getting Started" panel.

Object-Oriented Database

I independently invented and implemented an object-oriented database to support arbitrary combinations of data types.

Self-Organizing Fuzzy Controller

In collaboration with Balaji Rathakrishnan (a Graduate Research Assistant I funded) and John Yen, I developed a new systematic methodology for constructing and tuning fuzzy logic controllers. The research project was funded by Texaco (see the preceding section for details) for use in its refineries.

TEACHING

1. New Courses Developed

CPSC 111/211/311 Java and C-based sequence - Member of curriculum subcommittee, taught 111 and 211
CPSC 210 (Honors) - Data Structures
CPSC 320 (Honors) - Artificial Intelligence
CPSC 489 - Object-Oriented Programming, Systems, and Languages
CPSC 635 - Natural Language Processing (taught by Dr. P. Mayer)
CPSC 689 - Symbolic and Algebraic Computation (not taught)
CSCE 489/PHIL 382 (with Glen Miller [PHIL]) - Ethics and Cybertechnology
ENGR/PHIL 482 (Honors) - Ethics and Engineering
PHIL 282 (with Glen Miller [PHIL]) – Ethics in a Digital Age
PHYS/ELEN 674 (with David Church [PHYS]) - Special Topics in Quantum Computing (the first course at Texas A&M in quantum computing, and, to the best of my knowledge, the first course in quantum computing anywhere in Texas), taught Spring, 2005, for the fifth time.
A Distance Learning section of CPSC 601 - Programming in C and Java, taught Spring, 2003.
Two sections of CPSC 111 - Computer Science Concepts and Programming taught with student peer teachers as assistants, Fall, 2002.
Honors section of CPSC 111 - Computer Science Concepts and Programming taught with student peer teachers as assistants, Fall, 2004.
Developed (with Lawrence Petersen) an intensive summer training program in Java and Software Engineering for high-school computer science teachers, taught Summer, 2003.
Developing an intensive summer training program in Data Structures for high-school computer science teachers, taught Summer, 2004; I was also completely responsible for recruiting teachers, getting them admitted, arranging for housing, and so on.

2. Courses Taught

A. Graduate

CPSC 601	Programming in C and Java
CPSC 602	Object-Oriented Programming, Development, and Software Engineering

CPSC 614	Computer Architecture
CPSC 625	Artificial Intelligence
CPSC 632	Expert Systems
CPSC 681	Graduate Seminar
CPSC 685	Problems
CPSC 691	Research
PHYS/ELEN 674	Quantum Computing (co-teacher)

B. Undergraduate

CPSC 111	Computer Science Concepts and Programming
CPSC 111H	Computer Science Concepts and Programming (Honors)
CPSC 120	Programming II
CPSC 120H	Programming II (Honors)
CPSC 203	Introduction to Computing
CPSC 206	Structured Programming in C
CPSC 210	Data Structures
CPSC 210H	Data Structures (Honors)
CPSC 211	Data Structures and Implementations
CPSC 211H	Data Structures and Implementations (Honors)
CPSC 285	Special Topics - Data Structures for Teachers
CPSC 289	Special Topics - Java and Software Engineering for Teachers
CPSC 311	Analysis of Algorithms
CPSC 320/420	Artificial Intelligence
CPSC 320H/420H	Artificial Intelligence (Honors)
CPSC 321	Computer Architecture
CPSC 464	Integrated Systems Design Automation
CPSC 485	Problems
CPSC/ELEN 485H	Problems (Honors theses)
CPSC 489	Object-Oriented Programming, Systems, and Languages
CSCE 113	Intermediate Programming and Design
CSCE 121	Introduction to Program Design and Concepts
CSCE 121H	Introduction to Program Design and Concepts (Honors)
CSCE 315	Programming Studio
CSCE 410	Operating Systems
CSCE 489	Cyberethics (co-teacher)
ENGR 112	Foundations of Engineering II
ENGR 112H	Foundations of Engineering II (Honors)
ENGR/PHIL 482H	Ethics and Engineering (Honors)

PROFESSIONAL OUTREACH

1. Director, Knowledge Systems Research Center

2. Invited Significant Seminars or Lectures

Daugherity, W. C., “Computers and Privacy,” Phi Theta Kappa Honor Society State Convention, Blinn College, Brenham, Texas, 1985.

Daugherity, W. C., and DeSoi, J. F., “Objected-Oriented Programming,” Second Annual Texaco Artificial Intelligence Symposium, Houston, Texas, 1989.

Daugherity, W. C., “A Self-Tuning Fuzzy Controller,” ARRI Conference on Fuzzy Logic, Arlington, Texas, March 1992.

Daugherity, W. C., Yen, J., and Langari, R., “Tutorial on Fuzzy Logic,” Second International Workshop on Industrial Fuzzy Control & Intelligent Systems, College Station, Texas, December 1992.

Daugherity, W.C., “A Partially Self-Training System for the Protein Folding Problem,” World Congress on Neural Networks, Portland, Oregon, July 1993.

Daugherity, W.C., “Neuro-fuzzy Systems,” Third International Workshop on Industrial Fuzzy Control & Intelligent Systems, Houston, Texas, December 1993.

Daugherity, W.C. and Harris, C.E., “Ethics and Engineering,” NSF Research Experience for Undergraduates, College Station, Texas, Summer 1994.

Daugherity, W.C. and Harris, C.E., “Ethics and Engineering,” NSF Research Experience for Undergraduates, Austin, Texas, Summer 1994.

Daugherity, W.C. and Harris, C.E., “Ethics and Engineering,” NSF Research Experience for Undergraduates, College Station, Texas, Summer 1995.

Daugherity, W.C. and Harris, C.E., “Ethics and Engineering,” NSF Research Experience for Undergraduates, Austin, Texas, Summer 1995.

Daugherity, W.C., “Public-Key Cryptography Meets Quantum Computing: Why Secret Agencies are Quaking in their Boots.” Quantum Computing Seminar, Texas A&M University, April 9, 2001.

Daugherity, W.C., “Quantum Computing 101: How to Crack RSA.” DefCon X, Las Vegas, NV, August 4, 2002.

Daugherity, W.C., “Computer Ethics.” ENGR 482 Ethics and Engineering, Texas A&M University, April 14-16, 2003.

Daugherity, W.C., “Incorporating Computer Ethics into an Engineering Ethics Course.” University of Texas Ethics Conference, Austin, Texas, April 16, 2004.

Daugherity, W.C., “Computer Ethics.” ENGR 482 Ethics and Engineering, Texas A&M University, November 8-10, 2004.

Daugherity, W.C., “[My] 53 Years of Computing History,” CSCE 681 Open Graduate Seminar, Texas A&M University, November 18, 2015.

3. Consulting

St. Joseph’s Hospital, Bryan, Fall 1990, at no charge.
Other clients include IBM Federal Systems Division, New York Times, Washington Post, Los Angeles Times, Cheyenne and Arapaho Tribes of Oklahoma, Southwestern Bell Telephone, Fulbright & Jaworski (Houston), Texas Department of Agriculture, Phonogram B.V. (Amsterdam), and U. S. Department of the Treasury.

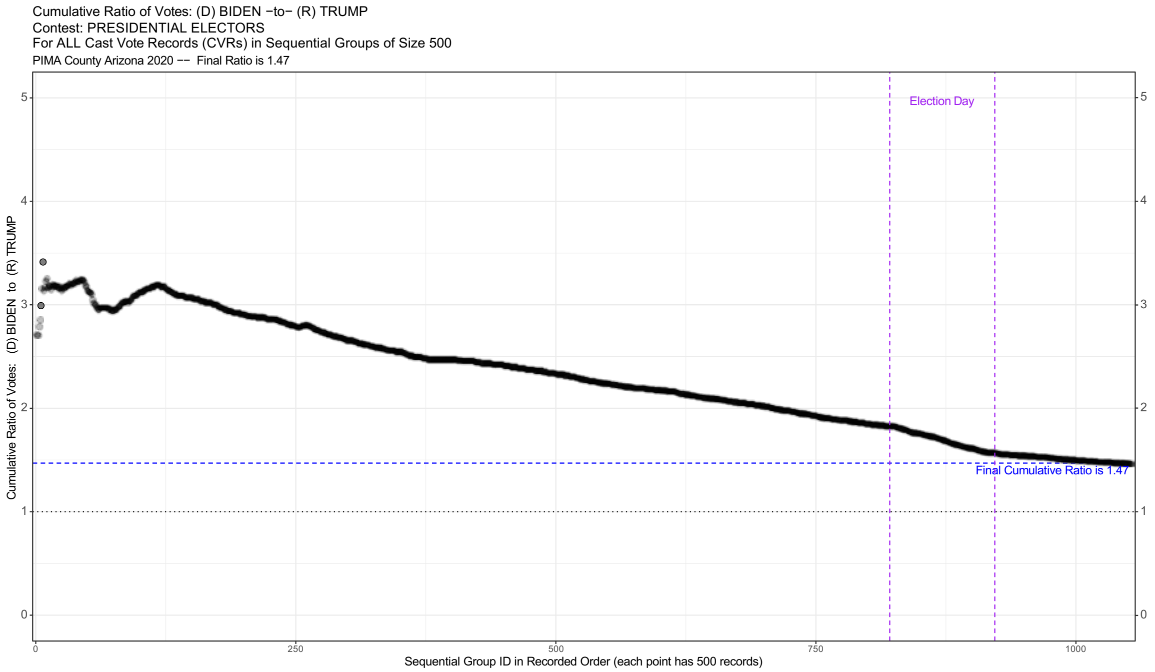
HONORS AND AWARDS

Oklahoma Junior Academy of Science, elected to membership, 1961, Oklahoma State University
National Science Foundation, Institute for High Ability Secondary School Students, 1962, University of Oklahoma
Westinghouse, Science Talent Search national finalist, 1963
National Merit Scholarship test, highest score in Oklahoma,
1963 Frontiers of Science, scholarship, 1963, Oklahoma
City, Oklahoma
Engineering Club of Oklahoma City, award, 1963, Oklahoma City,
Oklahoma Oklahoma Christian College, full scholarship (top entering
freshman), 1963,
Oklahoma City, Oklahoma
National Science Foundation, Undergraduate Research Participation Program, 1965, University of Oklahoma, Norman, Oklahoma
Alpha Delta Tau, National Honor Society, 1966
Who’s Who in American Colleges and Universities,
1966 Graduate Record Exam in Mathematics,

scored 800, 1966 Harvard University, Prize
Fellowship, 1966
National Science Foundation, Academic Year
Institute, 1967 Phi Delta Kappa, National Honor
Society, 1967
Harvard University, Class Marshal for the Graduate School of Education,
1967 Harvard University, Bowdoin Prize, bronze medal and cash award
for outstanding writing, 1973
Association for Computing Machinery, selected as a reviewer for
Computing Reviews, 1975
Association for Computing Machinery, Outstanding Regional
Intercollegiate Programming Contest Director Award, 1993,
Indianapolis, Indiana
World Congress on Neural Networks, Neural Systems Session Co-
chair,
1993, Portland, Oregon
Graduate Student Council, 1997 Outstanding Graduate Faculty Award
citation: “For your time and dedication to graduate students at
Texas A&M.”
Named by the TAMU System to The Academy for Educator Development, a
major component of The Texas A&M University System’s Regents’
Initiative for Excellence in Education, 2003 (one of only two faculty
members selected from the entire College of Engineering).
Winner, $500 cash prize, Texas A&M University Academic Integrity Week
Essay Competition (Faculty Category), 2004.
Texas A&M University, Department of Computer Science & Engineering,
2009 Undergraduate Faculty Award citation: “In grateful
appreciation of dedicated service, exemplary attitude, and
significant contribution.”
Qualified for American MENSA, 2015.
Oklahoma Christian University, Department of Mathematics and Computer Science,
2015
Distinguished Alumnus Award citation: “For outstanding vision, dedication, and
commitment to excellence.”

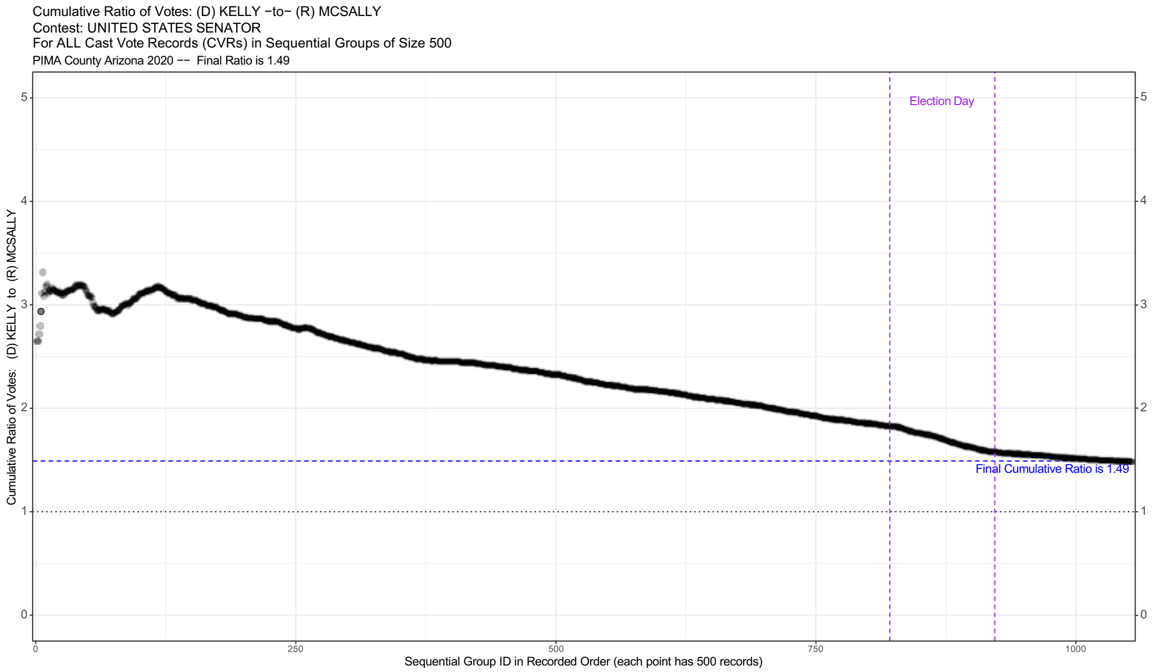
EXHIBIT B

page 3 of 51



Cumulative Ratio of Votes: (D) BIDEN −to− (R) TRUMP
Contest: PRESIDENTIAL ELECTORS
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 1.47

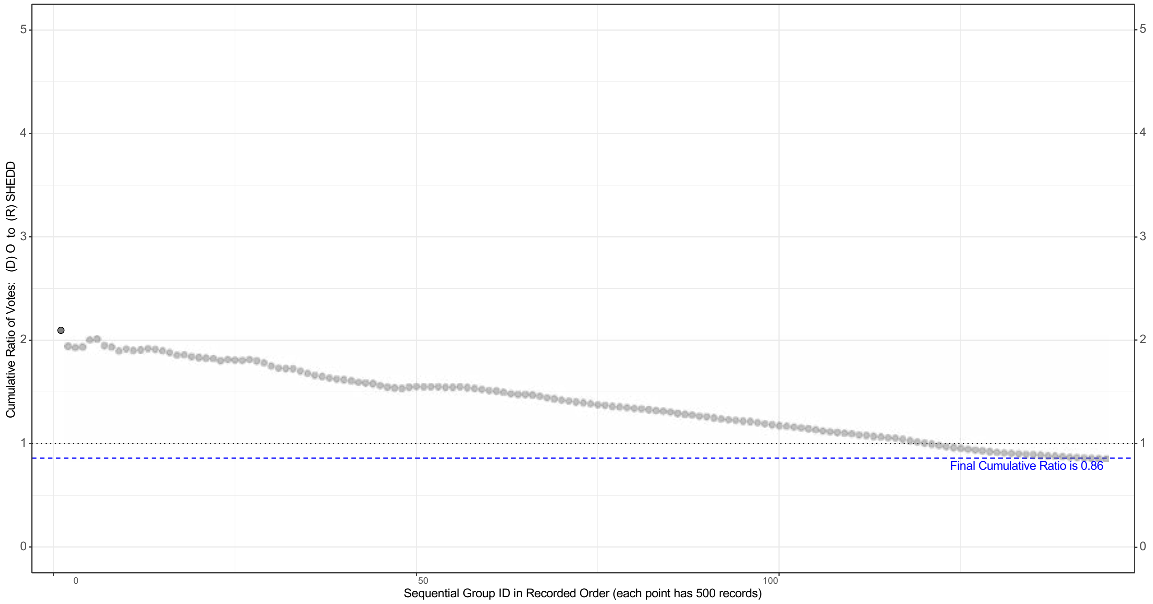
page 6 of 51



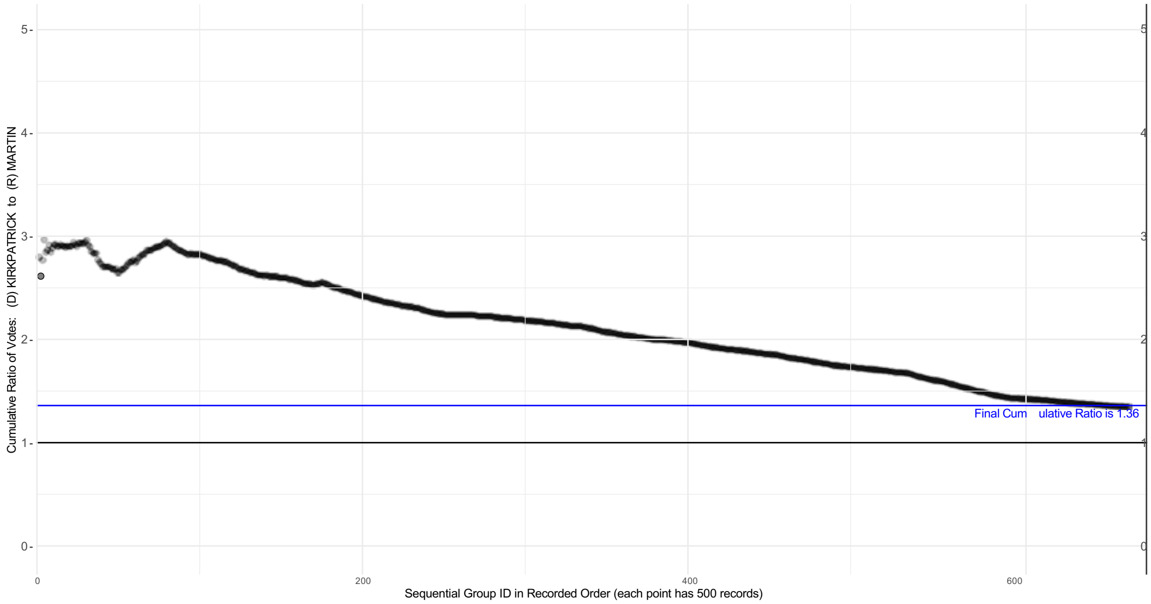
Cumulative Ratio of Votes: (D) KELLY −to− (R) MCSALLY
Contest: UNITED STATES SENATOR
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 1.49

page 9 of 51

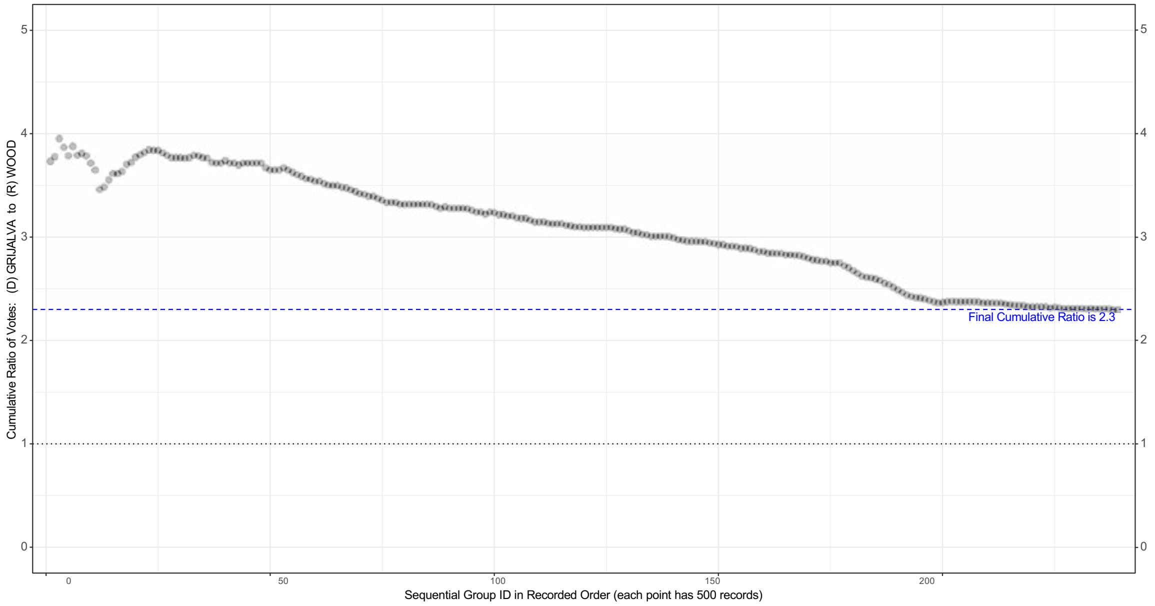
Cumulative Ratio of Votes: (D) O −to− (R) SHEDD
Contest: U.S. REPRESENTATIVE IN CONGRESS, DIST. 1
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 0.86



Cumulative Ratio of Votes: (D) KIRKPATRICK −to− (R) MARTIN
Contest: U.S. REPRESENTATIVE IN CONGRESS, DIST. 2
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 1.36

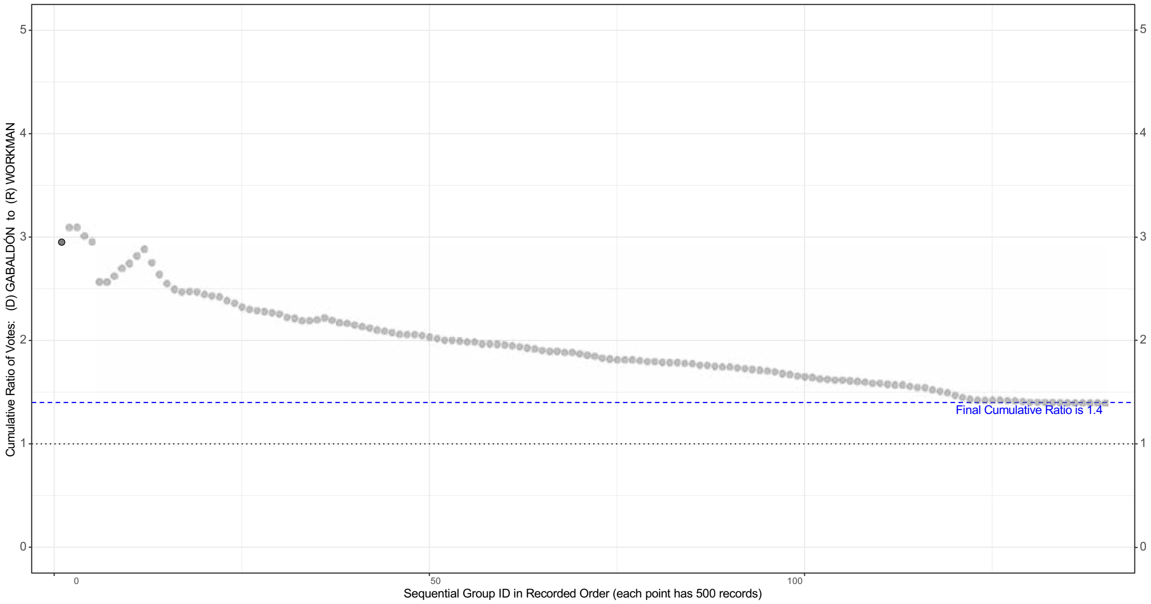


Cumulative Ratio of Votes: (D) GRIJALVA −to− (R) WOOD
Contest: U.S. REPRESENTATIVE IN CONGRESS, DIST. 3
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 2.3

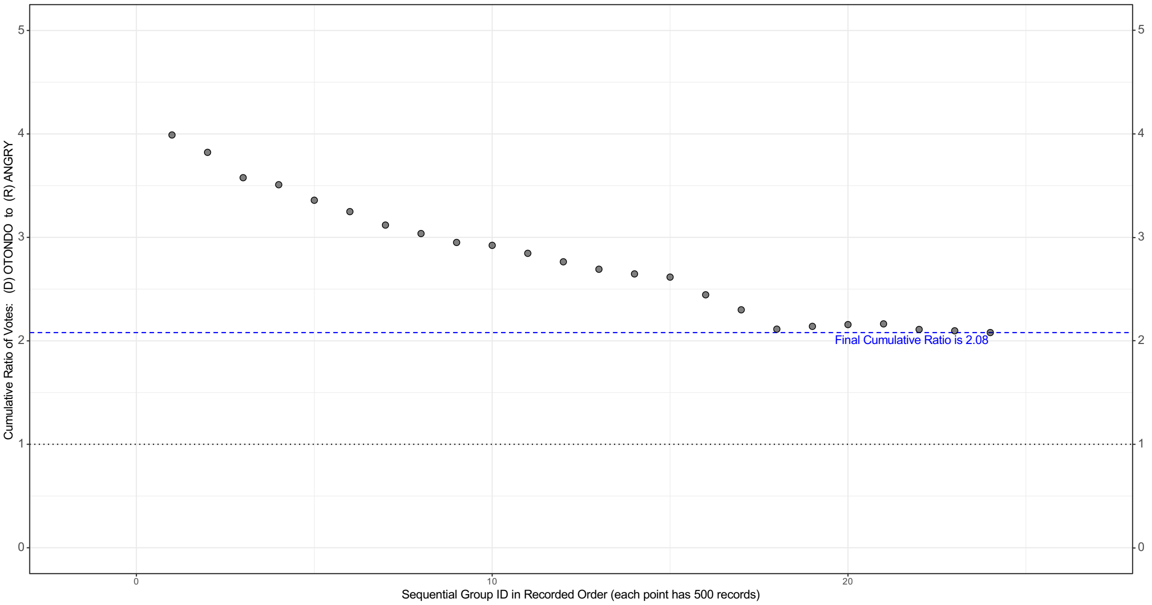


page 18 of 51

Cumulative Ratio of Votes: (D) GABALDÓN −to− (R) WORKMAN
Contest: STATE SENATOR, DIST. 2
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 1.4

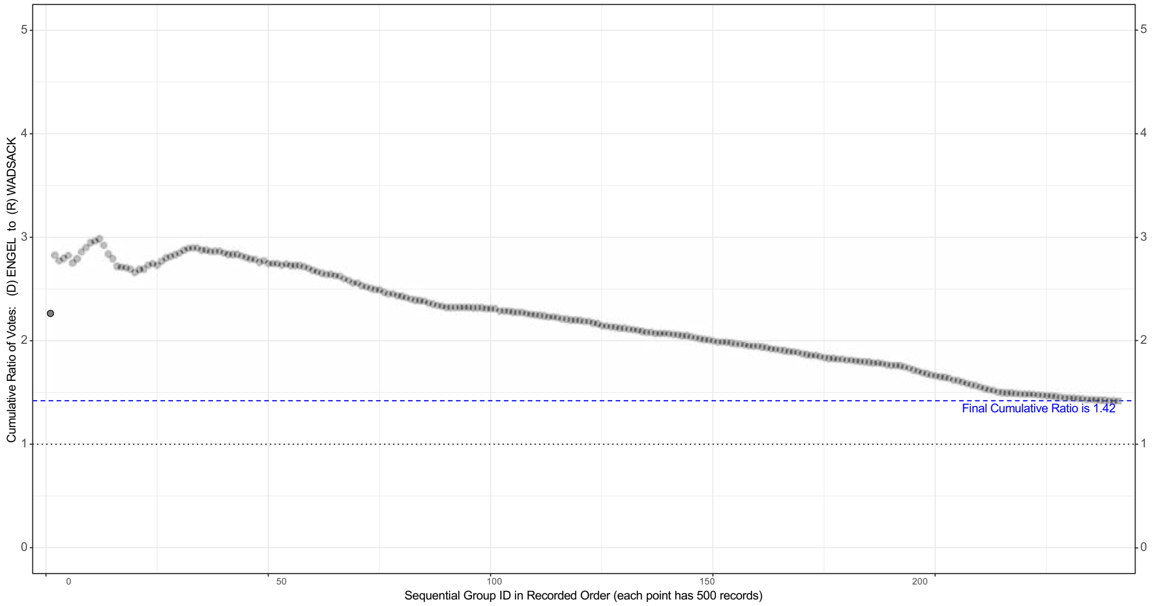


Cumulative Ratio of Votes: (D) OTONDO −to− (R) ANGRY
Contest: STATE SENATOR , DIST. 4
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 2.08



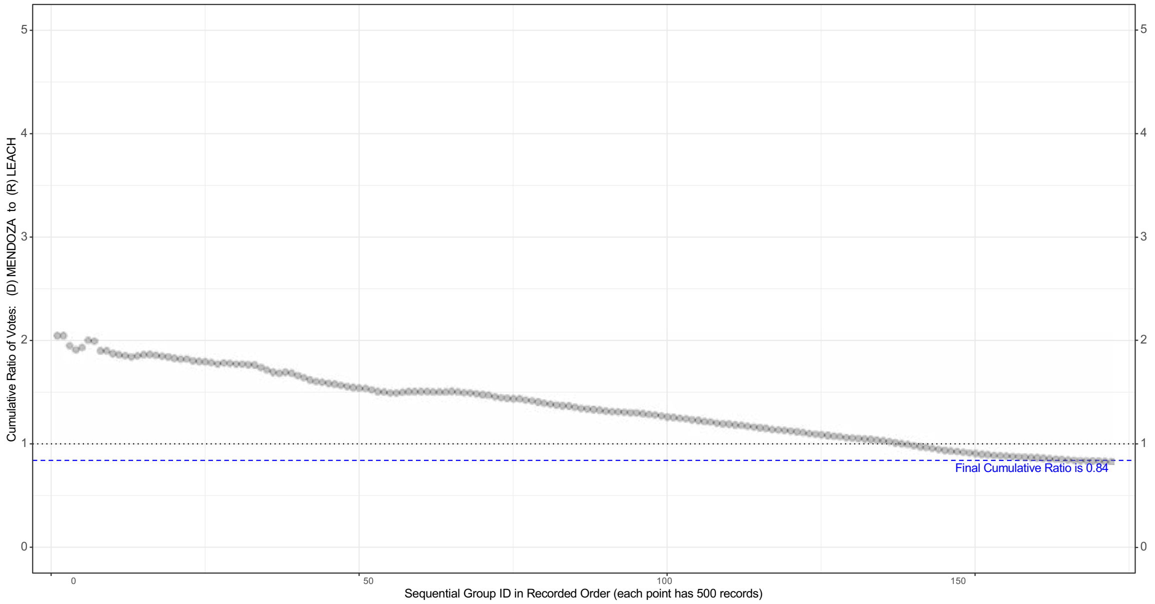
page 24 of 51

Cumulative Ratio of Votes: (D) ENGEL −to− (R) WADSACK
Contest: STATE SENATOR, DIST. 10
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 1.42



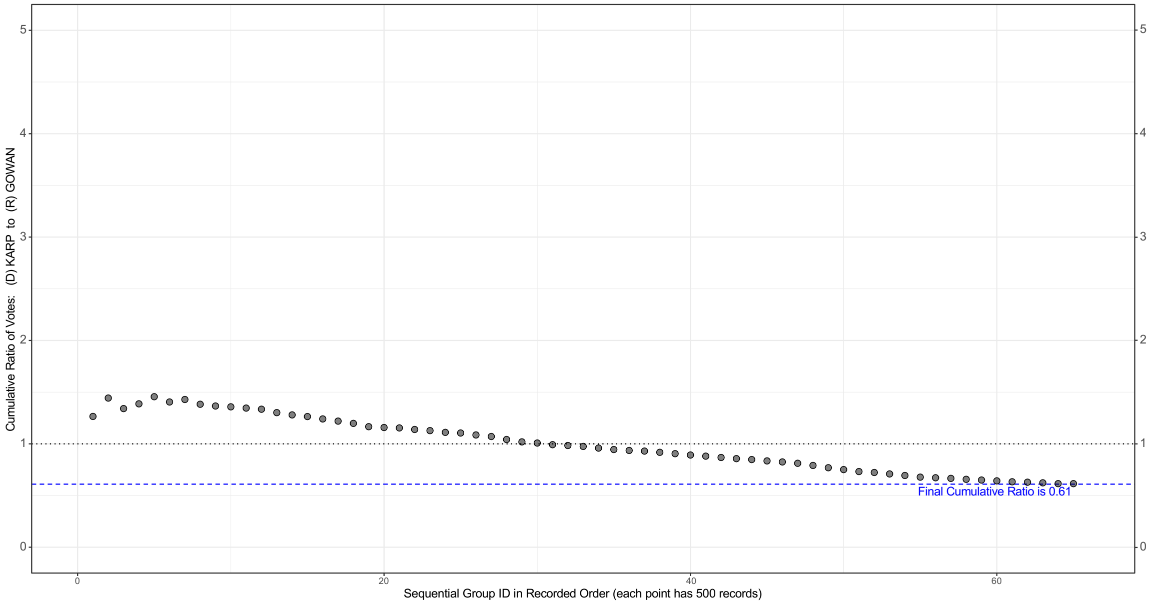
page 27 of 51

Cumulative Ratio of Votes: (D) MENDOZA −to− (R) LEACH
Contest: STATE SENATOR, DIST. 11
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 0.84

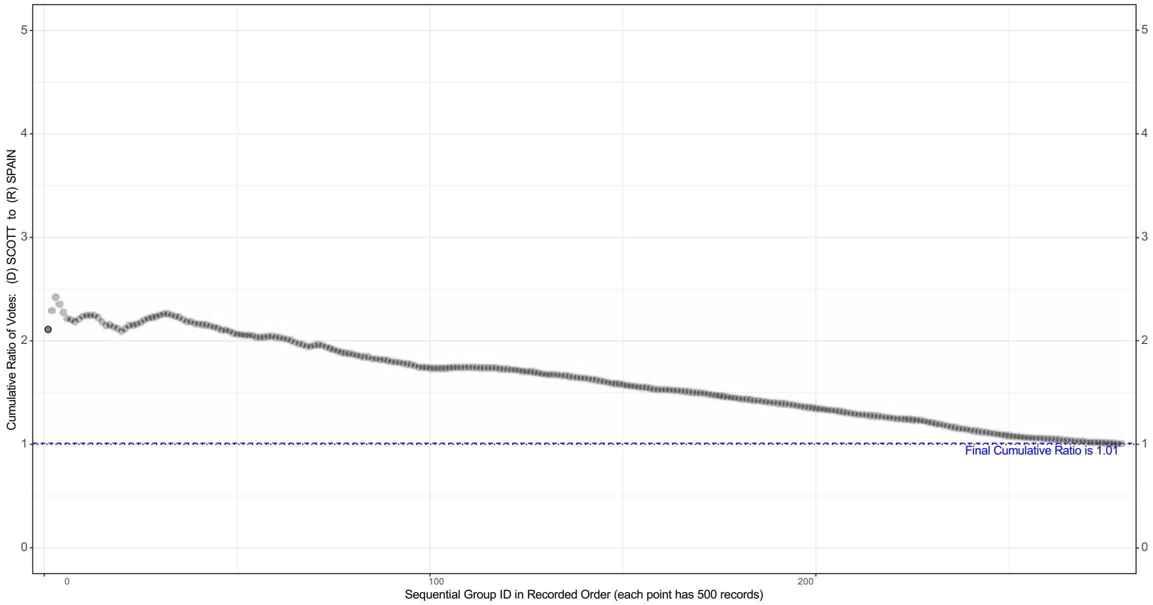


page 30 of 51

Cumulative Ratio of Votes: (D) KARP −to− (R) GOWAN
Contest: STATE SENATOR, DIST. 14
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 0.61

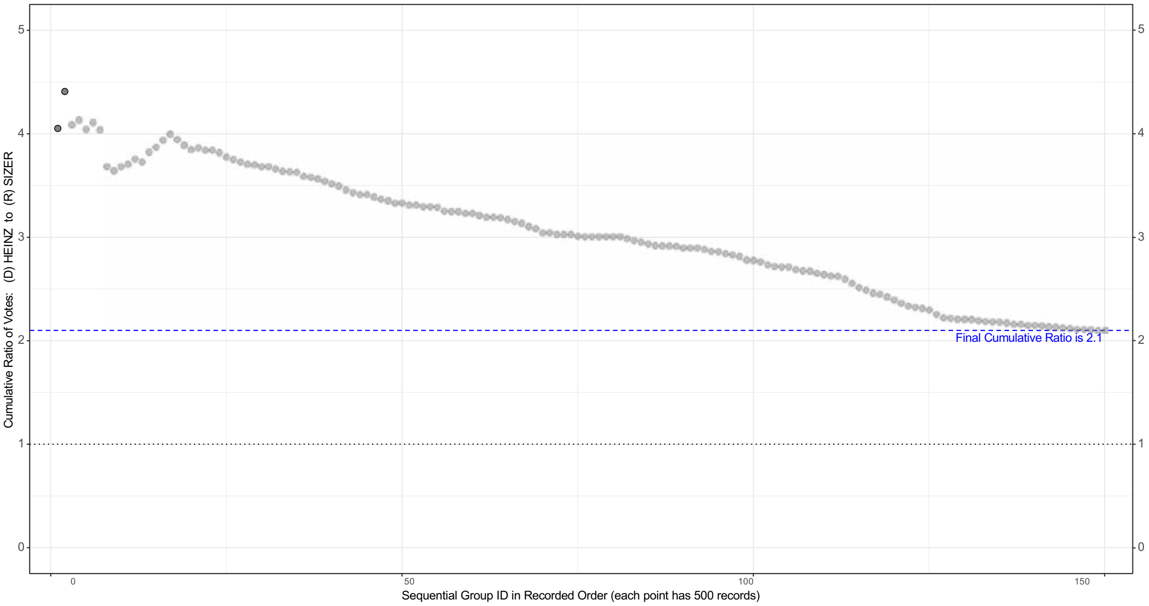


Cumulative Ratio of Votes: (D) SCOTT −to− (R) SPAIN
Contest: BOARD OF SUPERVISORS, DIST. 1
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 1.01

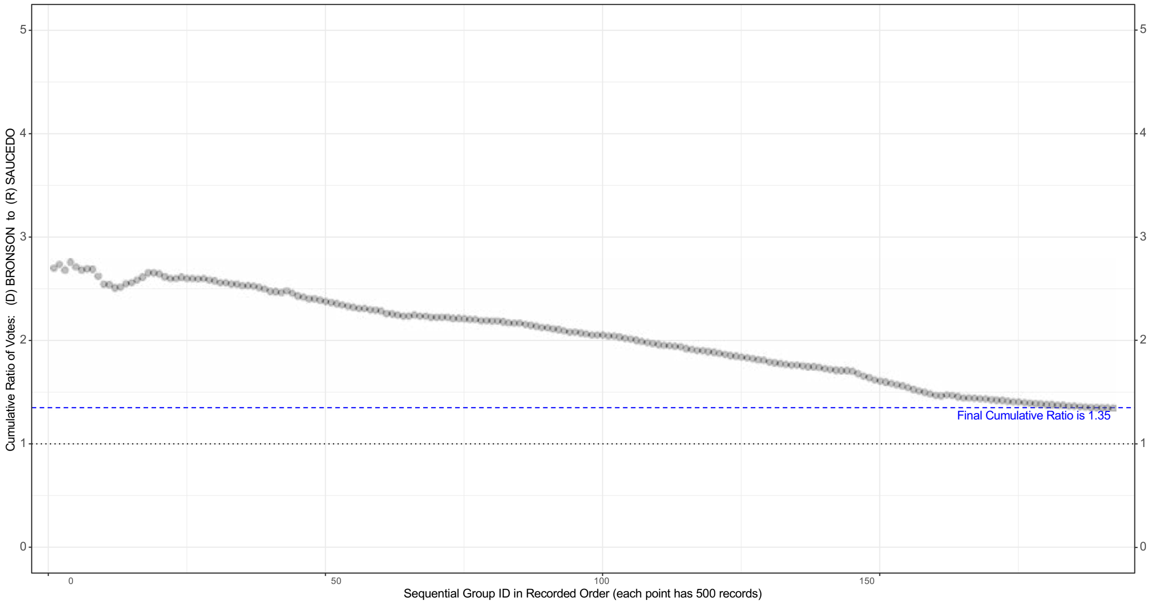


page 36 of 51

Cumulative Ratio of Votes: (D) HEINZ −to− (R) SIZER
Contest: BOARD OF SUPERVISORS, DIST. 2
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 2.1

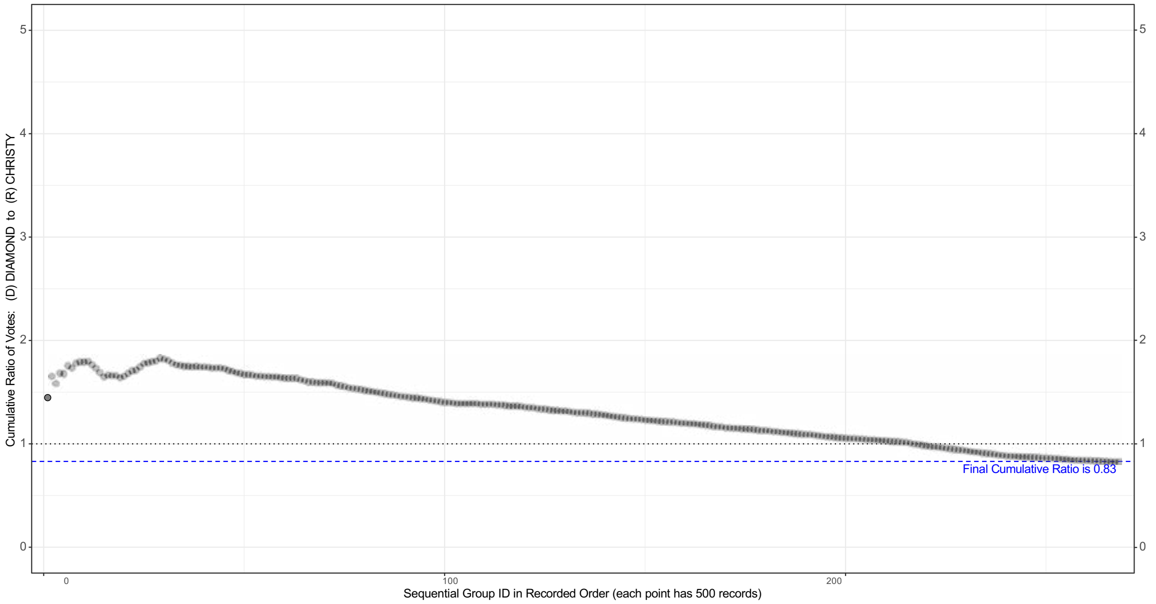


Cumulative Ratio of Votes: (D) BRONSON −to− (R) SAUCEDO
Contest: BOARD OF SUPERVISORS, DIST. 3
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 1.35



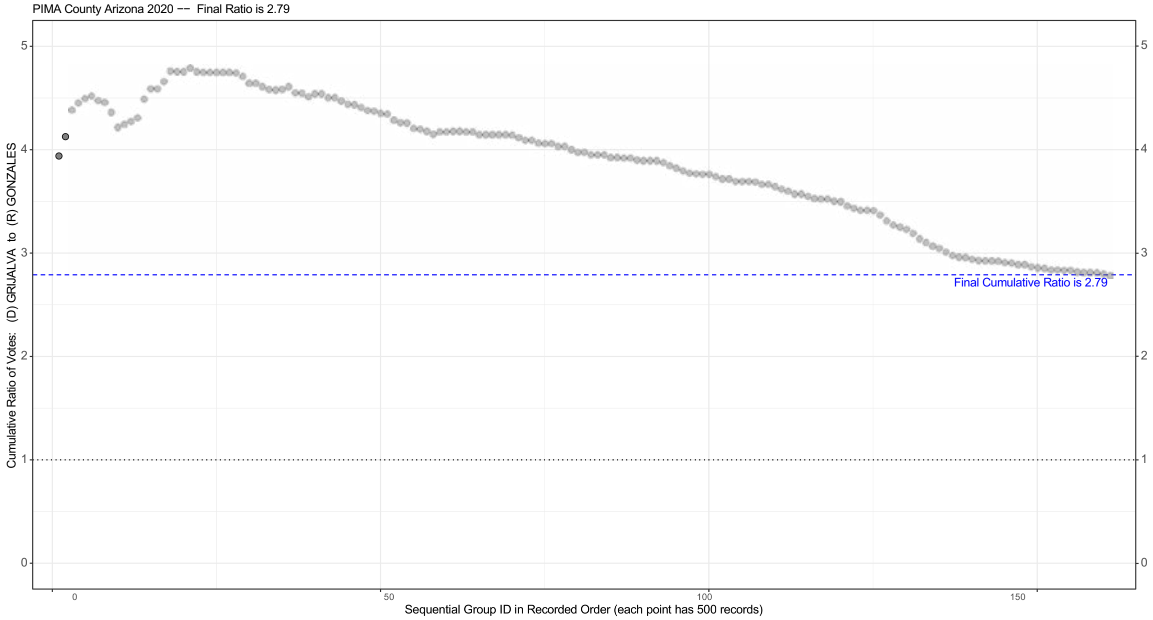
page 42 of 51

Cumulative Ratio of Votes: (D) DIAMOND −to− (R) CHRISTY
Contest: BOARD OF SUPERVISORS, DIST. 4
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 0.83



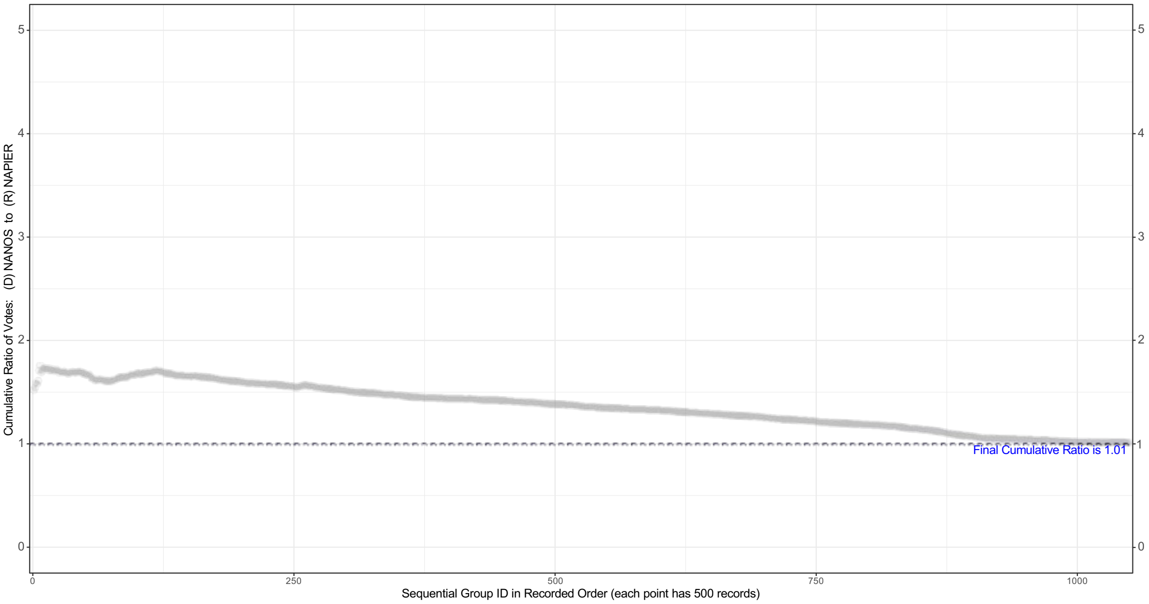
page 45 of 51

Cumulative Ratio of Votes: (D) GRIJALVA −to− (R) GONZALES
Contest: BOARD OF SUPERVISORS, DIST. 5
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 2.79



page 48 of 51

Cumulative Ratio of Votes: (D) NANOS −to− (R) NAPIER
Contest: SHERIFF
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 1.01



page 51 of 51

Cumulative Ratio of Votes: (D) CÁZARES −to− (R) WHITE
Contest: COUNTY RECORDER
For ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 −− Final Ratio is 1.42

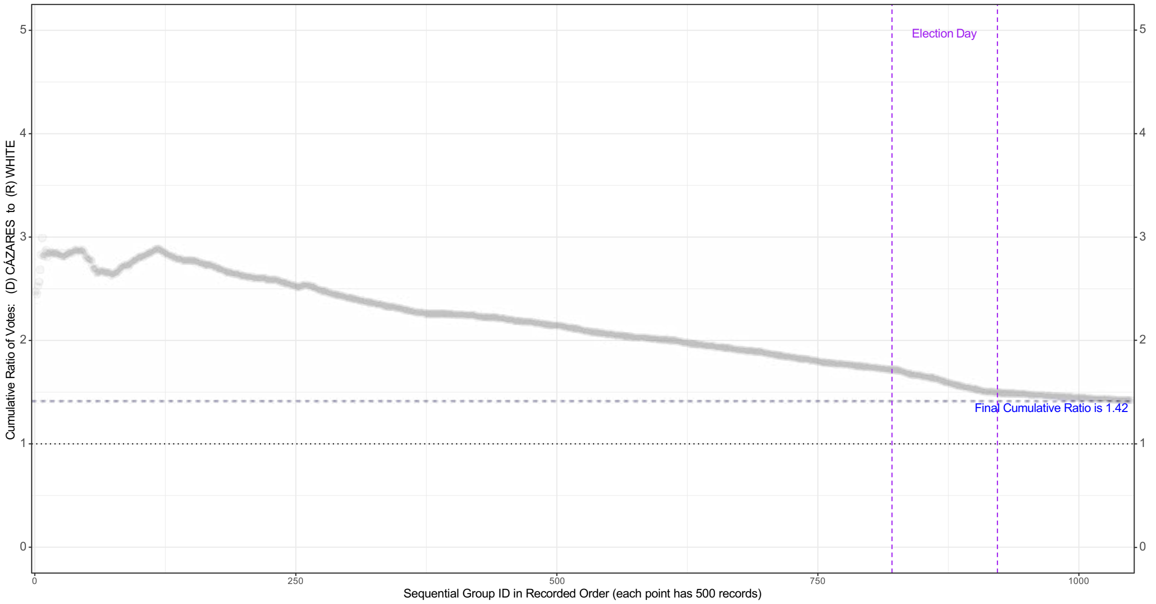


EXHIBIT C

From: Brian Watson [redacted]>
Sent: Thursday, November 12, 2020 2:33 PM
To: Sylvia Allen; Sonny Borrelli; Paul Boyer; Kate Brophy McGee; Heather Carter; Karen Fann; David Farnsworth; Eddie Farnsworth; David Gowan; Rick Gray; Sine Kerr; Vince Leach; David Livingston; J.D. Mesnard; Tyler Pace; Frank Pratt; Michelle Ugenti-Rita; John Allen; Nancy Barto; Leo Biasiucci; Walter Blackman; Shawnna Bolick; Russell Bowers; Noel Campbell; Frank Carroll; Regina Cobb; David Cook; Tim Dunn; John Fillmore; Mark Finchem; Travis Grantham; Gail Griffin; John Kavanagh; Anthony Kern; Jay Lawrence; Becky Nutt; Joanne Osborne; Kevin Payne; Warren Petersen; Steve Pierce; Tony Rivero; Bret Roberts; Thomas T.J. Shope; Bob Thorpe; Ben Toma; Kelly Townsend; Michelle Udall; Jeff Weninger
Subject: Fwd: Meeting held by Pima County Democrats (Voter Fraud Planning meeting)

asking you to void all elections in the state! This includes local, county, state and federal elections! Each ballot contains all these races in it!

The State Legislature has the power to null and void all Nov 3rd election results if AZSOS and the county recorder and elections office will not provide full transparency.
See forwarded message!

---------- Forwarded message ---------
From: **Brian Watson** <[redacted]>
Date: Tue, Nov 10, 2020 at 9:38 AM
Subject: Meeting held by Pima County Democrats (Voter Fraud Planning meeting)
To: <Criminal.Division@usdoj.gov>

US Department of Justice,

This is anonymous reporting and do not want to be included in this investigation! Thank you!

Please be advised that Pima County Recorder, located at 240 N Stone Ave, Tucson, AZ 85701 in Pima County Arizona and the Democratic Party added "fraud votes" in the initial count to the Vote-By-Mail (VBM) totals released at 8pm on Nov 3rd 2020.

There were approximately 35,000 fraud votes added to each democrat candidate's vote totals. Candidates impacted include county, state and federal election candidates. Through the utilization of the automated ballot count machines in Pima County Elections, my understanding is that 35,000 was embedded into each democrat candidate's total votes.

Below are the meeting notes:

In a meeting I was invited to by the democrat party in Pima County Arizona on Sept 10th 2020, no phones or recording devices were allowed, a presentation was given including detailed plans to embed 35,000 in a "spread configured distribution" to each democrat candidate's vote totals.

When I asked "how in the world will 35,000 be kept hidden or from being discovered", it was stated that "spread distribution will be embedded across the total registered voter range and will not exceed the registered voter count, and the 35,000 was determined allowable for pima county based on our county registered voter count". It was also stated that "total voter turnout versus total registered voters determine how many votes we can embed. The embedding will auto adjust based on voter turn-out." Because the "embed votes are distributed sporadically all embedded votes will not be found, if audited, because the embeds are in groups of approximately 1,000. This is so the county recorder can declare an orversite issue or error as a group of 1,000 is a normal and acceptable error." "Maricopa County's embed totals will be substantially higher than Pima due to embeds being calculated based on the total number of registered voters."

When I asked "has this ever been tested? and how do we know it works?" The response was "Yes, this has been testing and has shown significant success in Arizona Judicial Retention Elections since 2014 even undetectable in post audits because no candidate will spend the kind of funds needed to audit and contact voters to verify votes in the full potential of total registered voters which is more then 500,000 registered voter. This year our Secretary of State has removed precinct level detail for election night releases so canidates can't see precinct over-votes".

This is what I have from this meeting.
Just thought I'd report this. Not sure if you can do anything since I was unable to have a recording device at this meeting...

Thank you!
B.Watson

From: Travis Eubanks [redacted]
Sent: Sunday, November 19, 2023 10:16 AM
To: Secretary; GeneralCounsel
Cc: [redacted] Amanda Eubanks
Subject: Election Contest for Constitutional Amendments 1, 3, 4, 11, 12, 13, and 14
Attachments: Constitutional_Amendment_Election_Contest_w_Exhibits_Eubanks.pdf

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear Secretary of State,

Attached is our petition filed in the Travis County District Court (Civil) on 11/18/2023 asserting an election contest for Constitutional Amendments 1, 3, 4, 11, 12, 13, and 14 from the November 2023 election. Once we receive a case number, we will serve this document to you.

Thank you for working with us to enable our votes to be counted properly.

Cheers,

Travis Eubanks
Pro Se Petitioner
1823 Lookout Forest
San Antonio, TX 78260
505-506-1050

CAUSE NO. ____________

	§	IN THE DISTRICT COURT
	§	
	§	
TRAVIS EUBANKS,	§	
AMANDA EUBANKS, AND	§	
JARRETT WOODWARD	§	
VOTERS OF BEXAR COUNTY	§	
CONTESTANTS	§	TRAVIS COUNTY, TEXAS
v.	§	
	§	
JANE NELSON, IN HER	§	____ JUDICIAL DISTRICT
OFFICIAL CAPACITY AS	§	
TEXAS SECRETARY OF STATE	§	
CONTESTEE	§	

VOTERS' ORIGINAL PETITION
ASSERTING AN ELECTION CONTEST

TO THE HONORABLE JUDGE OF SAID COURT:

1. Travis Eubanks, Amanda Eubanks, and Jarrett Woodward who were and are registered voters residing in Bexar County, hereby file this Original Petition asserting an Election Contest. As is required by the Texas Election Code §233.003(a)(1), Contestants names Jane Nelson, Texas Secretary of State, in her official capacity, as the Contestee.

ELECTION CONTEST

2. This petition initiating an election contest is filed pursuant to Chapter 233 of the Texas Election Code. An election contest is a special statutory proceeding that provides a remedy for elections tainted by fraud, illegality, or irregularity. *Blum v. Lanier*, 997 S. W.2d 259, 262 (Tex. 1999). It includes all suits where the validity of the election, or of any part of the elective process, are subject to litigation. *In re Bishop*,_S.W.3d.___, 05-18-01333-CV, 2018 WL 6599196 at * 2 (Tex. App.—Dallas Dec. 17, 2018, orig. proceeding).

3. Any question relating to the validity or outcome of a constitutional amendment election may be raised in an election contest. A contest is the exclusive method for adjudicating such questions. Tex. Elec. Code §233.014(g)

4. Of concern, are the specific proposed constitutional amendments Proposition 1, Proposition 3, Proposition 4, Proposition 11, Proposition 12, Proposition 13, and Proposition 14.

PARTIES AND SERVICE

5. Pursuant to Tex. Elec. Code §233.002, Contestants Travis Eubanks, Amanda Eubanks, and Jarrett Woodward, have standing to bring an election contest into this district court for a proposed constitutional amendment included in the November 7, 2023 election.

6. Contestants are required to be qualified voters at the time of the election, per Texas Election Code §233.002, and confirmed by the Texas Supreme Court. “It is not disputed ...that they have standing as registered qualified voters” (*Dacus v. Parker*, 466 S.W.3d 820 (Tex. 2015). See also, *Brown v. Blum*, 9 S.W.3d 840 (Tex. App. 1999); since

"Blum was a qualified voter in the City of Houston at the time of the election on Proposition A, we hold that he has standing to contest that election."

7. Contestants can be served in their name and at the addresses below:

Travis Eubanks
1823 Lookout Forest
San Antonio, TX 78260
505-506-1050
travis.eubanks@gmail.com

Amanda Eubanks
1823 Lookout Forest
San Antonio, TX 78260
505-818-8824
amanda.eubanks710@gmail.com

Jarrett Woodward
8910 N Loop 1604 W Apt 1633
San Antonio, TX 78249
210-693-7457
Digging4au@protonmail.com

8. Contestee Jane Nelson may be served through personal service at:

Service of Process
Secretary of State
James E. Rudder Building
1019 Brazos, Room 105
Austin, Texas 78701

9. Jane Nelson is the presiding officer of the final canvassing authority for the contested election. Tex. Elec. Code § 67.010(b).

JURISDICTION AND VENUE

10. This Court has exclusive jurisdiction of this contest Tex. Elec. Code §221.002(a), and venue is proper in Travis County, Tex. Elec. Code §233.005(1).

DISCOVERY-CONTROL PLAN

11. Contestants intend to conduct discovery IAW Tex. Elec. Code § 221.008 and as permitted by the Texas Rules of Civil Procedure under Level 3 due to the timeframe and complexity of the material and will file a motion asking that the Court enter an order setting forth a suitable discovery control plan.

SUMMARY OF THE CASE

12. Contestants assert that the outcome of the contested election, as shown by the official results and official canvass, is not the true outcome. Tex. Elec. Code § 221.003(a).

13. Contestants contend that illegal votes were counted. Tex. Elec. Code § 221.003(a)(1).

14. "In this title, 'illegal vote' means a vote that is not legally countable." Tex. Elec. Code § 221.003(b).

15. Contestants will show that the ES&S and Hart InterCivic voting systems used across the state of Texas in this election do not meet the requirements for certification by the Election Assistance Commission (EAC) and the Office of the Texas Secretary of State as they have not been tested by a properly accredited Voting System Test Laboratory (VSTL) IAW the EAC Voluntary Voting System Guidelines (VVSG), Tex. Elec. Code § 122.001(a)(3), and Tex. Admin. Code §§ 81.60 and 81.61.

16. Contestants will show that voting systems are connected to the internet.

17. Therefore, all votes counted using illegally certified substandard voting systems were illegal votes and not to be counted according to legislative intent; the true outcome of the election cannot be ascertained. Tex. Elec. Code § 1.0015.

18. Contestants contend Texas Election Code Title 8 is unconstitutional under the Texas Constitution, Art VI, § 4.

SOVEREIGN IMMUNITY

19. Counties have governmental immunity, as the Texas Supreme Court explained in Wasson Interests, Ltd. v. City of Jacksonville, 489 S.W.3d 427 (Tex. 2016).

> Political subdivisions of the state—such as counties, municipalities, and school districts—share in the state's inherent immunity. *Reata Constr. Corp. v. City of Dallas*,197 S.W.3d 371, 374 (Tex.2006). But "[t]hey represent no sovereignty distinct from the state and possess only such powers and privileges as have been expressly or impliedly conferred upon them." *Payne v. Massey*, 145 Tex. 237, 196 S.W.2d 493, 495 (1946). Therefore, in the realm of sovereign immunity as it applies to such political subdivisions—referred to as governmental immunity—this Court has distinguished between those acts performed as a branch of the state and those acts performed in a proprietary, non-governmental capacity. See *Dilley v. City of Houston*, 148 Tex. 191, 222 S.W. 2d 992, 993 (1949) ; *City of Galveston v. Posnainsky*, 62 Tex. 118, 127 (1884). *Id.*

20. When the Texas Supreme Court has not found magic words waiving immunity, it has given guidance that they "have found waiver when the provision in question would be meaningless unless immunity were waived. Kerrville State Hosp. v. Fernandez, 28 S.W.3d 1, 8 (Tex. 2000)." Wichita Falls State Hosp v. Taylor, 106 S.W.3d 692, 697 (Tex. 2003).

21. This implied waiver of governmental or sovereign immunity applies to an election contest, since the contestee of a ballot measure will normally be the presiding officer of the authority ordering or canvasing the election — who is often representing a city or school district — or the secretary of state for a statewide measure. Texas Election Code § 233.003.

THE FACTS AND THE LAW OF THIS CASE

22. The Help America Vote Act of 2002 (HAVA2002, now (52 U.S.C. §§ 20901–21145) was passed by the United States Congress to implement improvements to voting systems/procedure and voter access.

23. HAVA creates minimum standards for states to follow for several areas of election administration.

24. The Texas Legislature codified HAVA making the standards mandatory in Texas. Tex. Elec. Code § 122.001(a)(3).

25. HAVA provides funds to help states meet new standards, replace, and purchase new voting systems, and improve election administration and security.

26. HAVA established the Election Assistance Commission (EAC) to assist states in HAVA compliance and to distribute HAVA funds.

27. The EAC is also charged with creating and regulating voluntary voting system guidelines (VVSG) as well as managing and operating the federally run voting system testing and certification program.

28. The overwhelming majority of ES&S and Hart InterCivic voting systems used across Texas to conduct elections were tested to VVSG 1.0 **standards**. [1] (Emphasis added).

29. VVSG 1.0 Vol. 1 section 1.1 – Purpose and Scope states: "The VVSG and the test lab accreditation process are essential components of the EAC National Certification Program for voting systems. This program applies the **standards** and **procedures** documented in the EAC voting system certification manual." [2] (page 3) (Emphasis added).

[1] https://www.eac.gov/voting-equipment/certified-voting-systems (last viewed November 8, 2023)

[2] https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF (last viewed November 8, 2023)

30. "Volume 2 describes the testing process to provide a documented independent verification by an **accredited testing laboratory** that a voting system has been demonstrated to conform to the Volume 1 requirements and therefore should receive national certification. It provides the specific detail about the testing process and documentation requirements required to support the national certification program." [3] (page 4) (Emphasis added).

31. The procedural requirements of this program are contained in:

   a. EAC Voting System Testing and Certification Program Manual Version 3.0 [4]

   b. EAC Voting System Test Laboratory Program Manual, Version 3.0 [5]

32. Section 1.4 of the VSTL Program Manual states: "This manual provides the **procedural requirements** of the EAC Voting System Laboratory Program. Although participation in the program is voluntary, **adherence to the program's procedural requirements is mandatory** if VSTLs choose to participate…This manual is intended to be read in conjunction with the Voting System Testing and Certification Program Manual." (Emphasis added).

33. The EAC's VSTL Program Manual and Voting System Testing and Certification Program Manual are clearly incorporated as standards of the Voluntary Voting System Guidelines adopted by the Election Assistance Commission and applicable to Tex. Elec. Code § 122.001(a)(3).

[3] https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF (last viewed November 8, 2023)

[4] https://www.eac.gov/sites/default/files/TestingCertification/Testing_and_Certification_Program_Manual_Version_3_0.pdf (last viewed November 8, 2023)

[5] https://www.eac.gov/sites/default/files/TestingCertification/VSTL_Program_Manual_Version_3_0.pdf (last viewed November 8, 2023)

34. The Election Assistance Commission has not complied with procedures regarding the Voting System Test Laboratories (VSTL) accreditation certificates, and therefore the voting system Certificates of Conformance are all invalid.

35. The VSTL Program Manual, ver. 3.0 (extract at Exhibit A), 3.6.1, states: "Certificate of Accreditation. A Certificate of Accreditation will be issued to each accredited laboratory. The certificate will be **signed by the Chair of the Commission** and state:

- The name of the VSTL;
- The scope of accreditation, by stating the VVSG version(s) to which the VSTL is competent to test;
- The effective date of the certification; and
- The technical standards to which the laboratory was accredited.

36. The previous Voting System Test Laboratory Program Manuals (ver. 2.0[6] and ver. 1.0[7]) also had the same procedural requirement requiring the certificates to be signed by the Chair of the Commission.

37. The Voting System Test Laboratory Program Manual, ver. 3.0, Appendix A-Glossary defines Commission: "The U.S. Election Assistance Commission, as an agency."

38. The EAC has previously issued an accreditation certificate for SysTest Labs, LLC in 2009 demonstrating their knowledge of and ability to comply with the requirements of 3.6.1 of the Voting System Test Laboratory Program Manual. [8] (Exhibit B)

[6] https://www.eac.gov/sites/default/files/eac_assets/1/28/VSTLManual%207%208%2015%20FINAL.pdf (last viewed November 8, 2023)

[7] https://www.eac.gov/sites/default/files/eac_assets/1/28/EAC%20Voting%20System%20Test%20Laboratory%20Program%20Manual%20discontinued%201%200.pdf (last viewed November 8, 2023)

[8] https://www.eac.gov/sites/default/files/voting_system_test_lab/files/SysTest%202009%20Certificate%20of%20Accreditation.pdf (last viewed November 8, 2023)

39. The two VSTLs, SLI Compliance and Pro V&V, have certificates of accreditation posted on the EAC website which **all lack the required signature** from at least 2015 to present date.[9] [10] (Exhibit C)

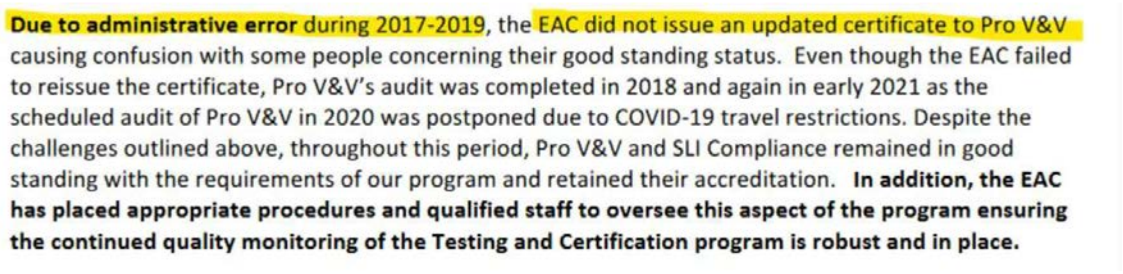
40. The SLI Compliance and Pro V&V accreditation certificates issued an posted at the time of the testing for all ES&S and Hart InterCivic voting systems are therefore not in compliance with HAVA 2002 (52 U.S.C. §§ 20901–21145) resulting in **any testing and/or reports being invalid for the purposes of certification** by both the EAC and the Office of the Texas Secretary of State.

41. Voting System Testing and Certification Program Manual Version 3.0, 1.6.3, states: "State or local officials are responsible for deciding if an EAC-certified voting system complies with state laws and making the final acquisition decision based on which voting system offers the best fit and value for their specific state or local jurisdiction."

42. The Office of the Texas Secretary of State has been approving contracts for counties to acquire voting systems that do not meet the standards outlined in Tex Elec Code § 122.001 for over 8 years since HB 2900 of the 84th Texas Legislature was passed in 2015.

[9] https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl/sli-compliance-division-gaming-laboratories (last viewed November 8, 2023)

[10] https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl/pro-vv (last viewed November 8, 2023)



Due to administrative error during 2017-2019, the EAC did not issue an updated certificate to Pro V&V causing confusion with some people concerning their good standing status. Even though the EAC failed to reissue the certificate, Pro V&V's audit was completed in 2018 and again in early 2021 as the scheduled audit of Pro V&V in 2020 was postponed due to COVID-19 travel restrictions. Despite the challenges outlined above, throughout this period, Pro V&V and SLI Compliance remained in good standing with the requirements of our program and retained their accreditation. **In addition, the EAC has placed appropriate procedures and qualified staff to oversee this aspect of the program ensuring the continued quality monitoring of the Testing and Certification program is robust and in place.**

Figure 1. Portion of EAC Letter, July 22, 2021.

43. The EAC (see Figure 1) admitted to "administrative error" (the Accardi doctrine), therefore violating the laws set by HAVA; "Applying the Accardi doctrine to the facts, the Court in Heffner said: 'An agency of the government must scrupulously observe rules, regulations, or procedures which it has established. When it fails to do so, its actions cannot stand and courts will strike it down ...'" (*United States v. Toussaint*, 456 F. Supp. 1069, 1074 (S.D. Tex. 1978)).

44. The voting system adopting authority is the decision maker on whether to adopt a voting system. Tex. Elec. Code § 123.001(b).

45. "Before a voting system may be used in elections, the authority designated by this section, by resolution, order, or other official action of the authority, must adopt the system for use in the elections. Tex. Elec. Code § 123.001(a).

46. Commissioners Courts across the entire state of Texas have adopted these substandard, illegally certified voting systems and used them to conduct the constitutional amendment election. Tex. Elec. Code § 123.001(b)(3)(A).

47. The Texas Constitution requires elections to be regulated and protected by law from "improper practice" with regulations to "detect and punish fraud".

48. Art. 6, § 2(c): "The privilege of free suffrage shall be protected by laws regulating elections and prohibiting under adequate penalties all undue influence in elections from power, bribery, tumult, **or other improper practice**." (Emphasis added).

a. Art. 6, § 4 "ELECTIONS BY BALLOT; PURITY OF ELECTIONS; REGISTRATION OF VOTERS. In all elections by the people, the vote shall be by ballot, and the Legislature shall provide for the numbering of tickets and make such other regulations as may be necessary **to detect and punish fraud** and preserve the purity of the ballot box; and the Legislature shall provide by law for the registration of all voters." (Emphasis added).

49. These Texas Statutes **require voting system testing by accredited testing laboratories**:

a. TX Election Code § 122.001 VOTING SYSTEM STANDARDS "(a)(3) **operates safely, efficiently, and accurately and complies with the voting system standards adopted by the Election Assistance Commission**;" (Emphasis added).

b. TX Administrative Code, Rule § 81.60 VOTING SYSTEM CERTIFICATION PROCEDURES "In addition to the procedures prescribed by the Texas Election Code, Chapter 122, **compliance with the following procedures is required for certification of a voting system**." "(3) The applicant must have the **nationally accredited voting system test laboratory** (VSTL) deliver a copy of all nationally qualified software/firmware and source codes for the system and/or system components requested for Texas certification, directly to the Secretary of State no later than 45 days prior to examination." (Emphasis added).

c. TX Administrative Code, Rule § 81.61 "Condition for Approval of Electronic Voting Systems. For any voting machine, voting device, voting tabulation device and any software used for each, including the programs and procedures for vote tabulation and testing, or any modification to any of the above, to be certified for use in Texas elections, the system shall have been certified, if applicable, by means of qualification testing by a **Nationally Recognized Test Laboratory** (NRTL) and shall meet or exceed the minimum requirements set forth in the Performance and Test Standards for Punch Card, Mark Sense, and Direct Recording Electronic Voting Systems, or in any successor voluntary standard document developed and promulgated by the Federal Election Commission. This section applies only to systems and modifications to previously certified systems submitted after the effective date of this rule." (Emphasis added).

50. The lack of properly accredited VSTLs and therefore, legal certification of voting systems, is not a mere disenfranchisement based on errors or mistakes of election workers. Election officials from county-level up to the state have been informed of the lack of VSTL accreditation for over two years, have continuously failed to comply with Texas Election Code and have continued the use of illegal voting systems to conduct elections in Texas. (*Kyle Strongin, et al., v. John B. Scott, et al., 4:22-cv-576-P-BJ, N. D. Tex., 2022; Heather Couchman, et al., v. Jacquelyn Callanen, et al., 5:22-cv-00929-OLG, W. D. Tex, 2022; In Re Cope, 22-0954, SC of Texas, 2022; Travis Wayne Eubanks v. Javier Salazar, et al., 2022CI00636, 131st JDC, Bexar Co., 2022*). (Exhibit D)

51. "Voting system" means a method of casting and processing votes that is designed to function wholly or partly by us of mechanical, electromechanical, or electronic apparatus

and includes the procedures for casting and processing votes and the programs, operating manuals, tabulating cards, printouts, and other software necessary for the system's operation. Tex Elec Code § 121.003(1).

52. Electronic voter registration databases/electronic poll pads/poll books are used to check voters in at vote centers across Texas.

53. The Office of the Texas Secretary of State is on video admitting these poll pads are connected to the internet. [11]

54. Electronic poll pads work in conjunction with the ballot on-demand printers to put barcodes/QR codes on the blank ballot stock prior to the voter inserting the ballot into the voting machine.

55. These barcodes/QR codes communicate with the voting machine which ballot style to pull up for the voter to be able to cast their vote. Without them, the machines do not function properly, and voters cannot cast votes.

56. Because the poll pads are a part of the procedure for casting votes, they are considered part of a voting system connected to the internet. This violates Tex Elec Code § 129.054(a).

57. "Our sister courts have determined it is appropriate to void elections where...the official disregard of the election laws is...pervasive[,]" *Alvarez v. Espinoza*, 844 S.W.2d 238, 249 (Tex.App. 1992). The Court in *Rogers v. Holder*, 636 So.2d 645, 651 (Miss. 1994), went even farther, holding when mandatory procedural requirements are willfully violated and there is a reasonable inference of fraud, a court is warranted in holding a new election." (*Adair Cntv .Bd. of Elections v. Arnold*, No. 2015-CA-000661-MR, at *25-26 (Ky. Ct. App. Sep. 11, 2015)).

[11] https://youtu.be/h_KqIVmykWw?si=Cupu6OI3G0DKfsl9 (last viewed November 8, 2023)

CONSTITUTIONAL CHALLENGES

58. Contestants present a constitutional challenge under Texas Government Code § 402.010. Texas Election Code § 231.002 where, “Except as otherwise provided by this subtitle, the rules governing civil suits in the district court apply to an election contest in the district court,” and also see Hotze v. Turner, No. 21-1037, at *9 (Tex. Apr. 21, 2023), where “Constitutional challenges to invalid municipal lawmaking are not confined to election contests.”

Title 8 “Voting Systems”

59. Contestants challenge the constitutionality of Title 8 “Voting Systems”, of the Texas Election Code, which became effective in January 1986. The secrecy of the ballot, as required by Tex Elec Code §§ 1.0015, 122.001 (a) (1), and 125.004 is compromised due to the use of electronic voting systems. The facts show the ballot is secret from the voter who marked and scanned it or selected, but not from political parties, government agencies, and private vendors who desire to use the data. (Exhibits E, F and G)

60. Due to the purported secrecy of the ballot, as required by the Texas Election Code, voters are not able to verify their vote was counted because it goes into an encrypted voting machine system. Voters do not know how the system is programmed. Voters are not able to verify the cast ballot is secret or counted as voters intended. Voters cannot read proprietary QR codes/barcodes, nor can they take a photo of the ballot with the QR codes/barcodes.

61. For a voter observing the scanning of a paper ballot, or the recording of an electronic ballot, there is a lack of transparency about what transpires next. For example, voters have requested digital copies of a cast vote record (CVR) and have been denied since courts

have determined that a CVR is the same as a ballot image. Pressley v. Casar, No. 17-0052 (Tex. Jan. 25, 2019).

62. The Texas Constitution does not require a secret ballot: "Art VI, § 4. ELECTIONS BY BALLOT; PURITY OF ELECTIONS; REGISTRATION OF VOTERS. In all elections by the people, the vote shall be by ballot, and the Legislature shall provide for the numbering of tickets and make such other regulations as may be necessary to detect and punish fraud and preserve the purity of the ballot box; and the Legislature shall provide by law for the registration of all voters."

63. Denton County Commissioners Court executed a memorandum of agreement with DHS/CIS entitled "MEMORANDUM OF AGREEMENT BETWEEN THE CENTER FOR INTERNET SECURITY/ELECTION INFRASTRC[sic]TURE INFORMATION SHARING AND ANALYSIS CENTER AND DENTON COUNTY, TEXAS FOR CYBERSECURITY SERVICES". One term of this agreement states "Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity's information system." (Exhibit E)

64. The Department of Homeland Security (DHS) has not always asked permission before accessing election-related computer systems, as the state of Georgia experienced in 2016[12]. (Exhibit F)

65. The Cybersecurity and Infrastructure Security Agency, also an agency within DHS, has recently been the subject of a U.S. House Judiciary Committee's Select Subcommittee on the Weaponization of the Federal Government report. [13]

[12] https://www.dhs.gov/sites/default/files/publications/Correspondence%20between%20DHS%20and%20U.S.%20Representative%20Jason%20Chaffetz%20%28R-UT%29.pdf (last viewed July 28, 2023).

[13] https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/cisa-staff-report6-26-23.pdf (last viewed July 28, 2023).

66. Contestants allege political parties in Texas also have access to voters' electronic ballots. The Republican Party of Texas GOP DataCenter demonstrates the ability to categorize a recent voter as a "swing voter" after voting in only one election. The voter portrayed did not vote in a primary election, which should be how the system determines a voter's tendency. (Exhibit G)

67. The use of electronic voting machine systems (which is not required by Texas Election Code) in conjunction with secret ballots (which is required by Texas Election Code) is a violation of the constitution as it is counter to "preserving the purity of the ballot box".

CAUSE OF ACTION ASSERTING AN ELECTION CONTEST

68. Contestants incorporate all previous paragraphs of this Petition by this reference. Based upon the facts and law developed herein, Contestants assert that the tribunal hearing this election contest must find that the outcome of the contested election, as shown by the final canvass, is not the true outcome because the voting systems were connected to the internet in violation of Tex Elec Code § 129.054(a) and were never tested by an accredited voting system test laboratory as required by Tex. Elec. Code § 122.001, Tex. Admin. Code, Rule §§ 81.60 and 81.61 causing every vote counted that was cast on a voting system to be illegal.

69. Because it is not possible to determine the true outcome of this election, the tribunal must declare the election result to be void, per Tex. Elec. Code §§ 233.011 and 233.012.

CONCLUSION

70. Contestants rely on Texas Election Code to argue that voting machine systems used in the November 7, 2023, election were not certified (see also Terpsehore Maras' affidavit in Exhibit Q). Contestants use Help America Vote Act of 2002 (HAVA) to explain how the voting system test laboratory is not accredited.

71. The Texas legislature codified portions of HAVA, to include testing by an accredited voting system test laboratory, making it mandatory.

72. While the United States Supreme Court could likely not have foreseen in 1941 the voting machine systems of today, this decision addresses them anyway:

> Included within the right to choose, secured by the Constitution, is the right of qualified voters within a State to cast their ballots and have them counted at Congressional elections. P. 315. Since the constitutional command is without restriction or limitation, this right, unlike those guaranteed by the Fourteenth and Fifteenth Amendments, is secured against the action of individuals as well as of States. 5. Where the state law has made the primary election an integral part of the procedure of choosing Representatives, or where in fact the primary effectively controls the choice, the right of the qualified elector to vote and have his ballot counted at the primary, is part of the right to choose Representatives secured by Art. I, § 2. P. 316. In determining whether a provision of the Constitution applies to a new subject matter, it is of little significance that it is one with which the framers were not familiar. For in setting up an enduring framework of government they undertook to carry out for the indefinite future and in all the vicissitudes of the changing affairs of men, those fundamental purposes which the instrument itself discloses. *United States v. Classic*, 313 U.S. 299 (1941)

73. Alex Halderman (Exhibit X) also shows that the ballot marking devices (BMDs) similar to those that Contestants were forced to use for voting in 2023 contain multiple severe security flaws including the opportunity to install malicious software locally or remotely. Halderman explains how "such malware, once installed, could alter voters' votes while subverting all the procedural protections

practiced by the State, including acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs)."

PRAYER

74. Based on the foregoing, Contestants request that the Court declare the contested election results cannot be ascertained and thus declare the constitutional amendment election void for Propositions 1, 3, 4, 11, 12, 13, and 14.

75. Issue a declaratory judgment that Texas Election Code Title 8 is unconstitutional under the Texas Constitution, Article VI, § 4.

76. Contestants do not seek costs for this election contest, but do request consideration for all other relief, in law and in equity, that they may be entitled to.

Respectfully Submitted,

/s/ Travis Eubanks
Pro Se Petitioner
1823 Lookout Forest
San Antonio, TX 78260
travis.eubanks@gmail.com

/s/ Amanda Eubanks
Pro Se Petitioner
1823 Lookout Forest
San Antonio, TX 78260
amanda.eubanks710@gmail.com

/s/ Jarrett Woodward
Pro Se Petitioner
8910 N Loop 1604 W Apt 1633
San Antonio, TX 78249
Digging4au@protonmail.com

EXHIBIT A

3.5.1. Notice of Nonconformity. In the event the Program Director identifies (1) missing documentation or information and/or (2) issues of noncompliance, the Program Director must notify the laboratory of the deficiencies. The written notice of nonconformity must identify missing documentation or information and issues of noncompliance. The laboratory will have 10 business days to amend the application package or submit additional information in response to identified nonconformities.

3.5.2. Action on Notice of Nonconformity. A laboratory's response to a notice of nonconformity must include any missing documents identified in the notice, as well as any additional or clarifying information or documentation responsive to an issue of noncompliance. If a laboratory fails to provide required information or documentation within the required timeframe, the Program Director will reject the application as incomplete and return the package to the laboratory for resubmission consistent with the requirements of this chapter.

3.5.3. Recommendation to Commissioners. After final review of the application package, the Program Director must forward the application package to the Chair of the Commission with a recommendation of disposition.

3.5.4. Vote by Commissioners. Upon receipt of an application package and recommendation from the Program Director, the Chair of the Commission will forward the information to each EAC Commissioner. The Chair of the Commission will bring the matter to a vote, consistent with the rules of the Commission. The measure presented for a vote will take the form of a written Commissioners' Decision which (1) makes a clear determination as to accreditation and (2) states the basis for the determination.

3.6. Grant of Accreditation. Upon a vote of the EAC Commissioners to accredit a laboratory, the Program Director must inform the laboratory of the decision, issue a Certificate of Accreditation, and post information regarding the laboratory on www.eac.gov.

3.6.1. Certificate of Accreditation. A Certificate of Accreditation will be issued to each accredited laboratory. The certificate will be signed by the Chair of the Commission and state:

- The name of the VSTL;
- The scope of accreditation, by stating the VVSG version(s) to which the VSTL is competent to test;
- The effective date of the certification; and
- The technical standards to which the laboratory was accredited.

3.6.2. Post Information on Web Site. The Program Director will make the following

EXHIBIT B

United States Election Assistance Commission

U.S. Election Assistance Commission

VSTL

Certificate of Accreditation

SysTest Labs, LLC
Denver, CO

is recognized by the US. Election Assistance Commission for the testing of voting systems to the 2005 Voluntary Voting Systems Guidelines under the criteria set forth in the EAC Voting System Testing and Certification Program and Laboratory Accreditation Program. SysTest is also recognized as having successfully completed assessments by the National Voluntary Laboratory Accreditation Program for conformance to the requirements of ISOIIEC 17025 and the criteria set forth in NIST Handbooks 150 and 150-22.

Effective Through

July 16, 2011

&k /LL : 7/16/09

Chair, U.S. Election Assistance Commission

EAC Lab Code: **0701**

EXHIBIT C

United States Election Assistance Commission

Certificate of Accreditation

SLI Compliance, Division of Gaming Laboratories International, LLC Wheat Ridge, Colorado

is recognized by the U.S. Election Assistance Commission for the testing of voting systems to the 2002 Voting Systems Standards, the Voluntary Voting Systems Guidelines versions 1.0 and 1.1 under the criteria set forth in the EAC Voting System Testing and Certification Program and Laboratory Accreditation Program. SLI Compliance is also recognized as having successfully completed assessments by the National Voluntary Laboratory Accreditation Program for conformance to the requirements of ISO/IEC 17025 and the criteria set forth in NIST Handbooks 150 and 150-22.

Effective Through

January 10, 2021

Date: 1/10/18

Brian Newby,
Executive Director, U.S. Election Assistance Commission

EAC Lab Code: **0701**

United States Election Assistance Commission

Certificate of Accreditation

SLI Compliance
Division of Gaming Laboratories International, LLC
Wheat Ridge, Colorado

is recognized by the U.S. Election Assistance Commission for the testing of voting systems to the 2005 and 2015 Voluntary Voting Systems Guidelines (VVSG 1.0 & 1.1) under the criteria set forth in the EAC Voting System Testing and Certification Program and Laboratory Accreditation Program. SLI Compliance is also recognized as having successfully completed assessments by the National Voluntary Laboratory Accreditation Program for conformance to the requirements of ISO/IEC 17025 and the criteria set forth in NIST Handbooks 150 and 150-22.

Original Accreditation Issued on: 2/28/2007

Accreditation remains effective until revoked by a vote of the EAC pursuant to 52 U.S.C. § 20971(c)(2).

Mona Harrington

Date: 2/1/21

Mona Harrington
Executive Director, U.S. Election Assistance Commission

EAC Lab Code: **0701**

United States Election Assistance Commission

Certificate of Accreditation

SLI Compliance
Division of Gaming Laboratories International, LLC
Wheat Ridge, Colorado

is recognized by the U.S. Election Assistance Commission for the testing of voting systems to the Voluntary Voting Systems Guidelines VVSG 1.0, 1.1 & 2.0 under the criteria set forth in the EAC Voting System Testing and Certification Program and Laboratory Accreditation Program. SLI Compliance is also recognized as having successfully completed assessments by the National Voluntary Laboratory Accreditation Program for conformance to the requirements of ISO/IEC 17025 and the criteria set forth in NIST Handbooks 150 and 150-22.

Original Accreditation Issued on: 2/28/2007

Accreditation remains effective until revoked by a vote of the EAC pursuant to 52 U.S.C. § 20971(c)(2).

Mark A. Robbins

Date: 11/15/22

Mark A. Robbins
Interim Executive Director, U.S. Election Assistance Commission

EAC Lab Code: **0701**

United States Election Assistance Commission

Certificate of Accreditation

Pro V&V, Inc.
Huntsville, Alabama

is recognized by the U.S. Election Assistance Commission for the testing of voting systems to the 2005 Voluntary Voting Systems Guidelines under the criteria set forth in the EAC Voting System Testing and Certification Program and Laboratory Accreditation Program. Pro V&V is also recognized as having successfully completed assessments by the National Voluntary Laboratory Accreditation Program for conformance to the requirements of ISO/IEC 17025 and the criteria set forth in NIST Handbooks 150 and 150-22.

Effective Through

February 24, 2017

Date: 2/24/15

Acting Executive Director, U.S. Election Assistance Commission

EAC Lab Code: **1501**

United States Election Assistance Commission

Certificate of Accreditation

Pro V&V, Inc.
Huntsville, Alabama

is recognized by the U.S. Election Assistance Commission for the testing of voting systems to the 2005 and 2015 Voluntary Voting Systems Guidelines (VVSG 1.0 & 1.1) under the criteria set forth in the EAC Voting System Testing and Certification Program and Laboratory Accreditation Program. Pro V&V is also recognized as having successfully completed assessments by the National Voluntary Laboratory Accreditation Program for conformance to the requirements of ISO/ IEC 17025 and the criteria set forth in NIST Handbooks 150 and 150-22.

Original Accreditation Issued on: 2/24/2015

Accreditation remains effective until revoked by a vote of the EAC pursuant to 52 U.S.C. § 20971(c)(2).

Mona Harrington

Date: 2/1/21

Mona Harrington
Executive Director, U.S. Election Assistance Commission

EAC Lab Code: **1501**

United States Election Assistance Commission

Certificate of Accreditation

Pro V&V, Inc.
Huntsville, Alabama

is recognized by the U.S. Election Assistance Commission for the testing of voting systems to the Voluntary Voting Systems Guidelines VVSG 1.0, 1.1 & 2.0 under the criteria set forth in the EAC Voting System Testing and Certification Program and Laboratory Accreditation Program. Pro V&V is also recognized as having successfully completed assessments by the National Voluntary Laboratory Accreditation Program for conformance to the requirements of ISO/IEC 17025 and the criteria set forth in NIST Handbooks 150 and 150-22.

Mark A. Robbins

Date: 12/21/22

Original Accreditation Issued on: 2/24/2015

Accreditation remains effective until revoked by a vote of the EAC pursuant to 52 U.S.C. § 20971(c)(2).

Mark A. Robbins
Interim Executive Director, U.S. Election Assistance Commission

EAC Lab Code: **1501**

EXHIBIT D

DENTON COUNTY
COMMISSIONERS COURT

08/06/2019

Month Day Year

19·0539

Court Order Number

14.A.
THE ORDER:

Approval of Memorandum of Agreement between the Center for Internet Security (CIS) / Election Infrastructure Infonnation Sharing and Analysis Center (EI-ISAC) and Denton County for Cybersecurity Services as recommended by Kevin Carr, Chieflnfonnation Officer, and any appropriate action.

Motion by tJ\)\n'ftt,

Seconded by__ ---------------------- !\:_
..x

County Judge
Andy Eads
Yes
Abstain
No
Absent

Commil!sioner Pet No 1
Hugh Coleman
Yes
Abslllin
No
Absent

Commjssjoner Pct No 2
Ron Marchant
Yes
Abst-ain
No
Absent

Commissioner Pct No3
Bobbie J. Mitchell
Yes
Absmin _
No
Absent

CommissionerPctNo4
Dianne Edmondson
Yes X
Ab. tain
No
[\•(\Absent

Motion Carried –

Other Action: **Pulled from Consent __** No Action Postponed

BY ORDER OF THE COMMISSIONERS COURT:

AITEST:

Andy Eads

Presiding Officer

APPROVED AS TO FORM:

Assistant District Attorney

TEXAS COMMISSIONERS COURT OF DENTON COUNTY

Juli Luke, County Clerk and Ex-Officio Clerk of the Commissioners Court of Denton County, Texas

BY:

Deputy County Clerk

MEMORANDUM OF AGREEMENT
BETWEEN THE CENTER FOR INTERNET SECURITY /ELECTION INFRASTRCTURE INFORMATION SHARING AND ANALYSIS CENTER
AND
Denton county, Texas
FOR
CYBERSECURITY SERVICES
(Federally Funded Election Services)

This MEMORANDUM OF AGREEMENT ("Agreement") by and between the Center for Internet Security, Inc. ("CIS"), operating in its capacity as the Elections Infrastructure Information Sharing and Analysis Center ("EI-ISAC"), located at 31 Tech Valley Drive, East Greenbush, NY 12061-4134, and Denton county, Texas ("Entity") with its principal place of business at: 701 Kimberly Drive, suite 285, Denton, TX 76208 for Cybersecurity Services, as defined herein below (CIS and Entity each a "Party" and collectively referred to as the "Parties").

WITNESSETH:

WHEREAS, CIS operates a twenty-four hours a day, seven days per week (24/7) Security Operations Center ("SOC"); and

WHEREAS, CIS has entered into an agreement with the US Department of Homeland Security ("DHS") to provide Cybersecurity Services, including Cybersecurity Services for state election entities; and

WHEREAS, the Entity is a state election entity designated to receive Cybersecurity Services.

NOW, THEREFORE, in consideration of the mutual covenants contained herein, the Parties do hereby agree as follows:

I. Purpose

The purpose of this agreement is to set forth the mutual understanding between Entity and CIS with respect to the provision of Cybersecurity Services to Entity.

II. Definitions

A. Security Operation Center (SOC) - 24 X 7 X 365 watch and warning center that provides network monitoring, dissemination of cyber threat warnings and vulnerability identification and mitigation recommendations.

8/6/2019 14.A

B. Cybersecurity Services or CSS - Combined Netfl.ow and intrusion detection system monitoring and analysis of related data, and delivery and management of associated devices, hardware and software necessary for delivery of CSS. Also referred to as Albert monitoring services.

III. Consideration

Pursuant to the agreement with DHS, CIS is providing Cybersecurity Services and associated security devices at no charge to Entity.

IV. Responsibilities

Appendix A, which is attached hereto and incorporated herein, contains the specific responsibilities for Entity and CIS regarding the CSS. Entity understands and agrees that, as a condition to commencement of CSS under the terms of this Agreement, it must:

A. agree to comply with the terms and conditions applicable to Entity as set forth in Appendix A; and

B. execute the Entity Certification form attached as part of Appendix A.

V. Title

CIS will at all times retain title to hardware and/or software provided to Entity during the Term of this Agreement. Upon termination or expiration of this Agreement, Entity will return all hardware and/or software provided under this Agreement within thirty (30) days of such expiration or termination.

VI. Term of this Agreement

This Agreement will commence on the date it is signed by both Parties, and shall continue in full force and effect until terminated (the "Term"). Either Party may terminate this Agreement by providing written notice to the other Party ninety (90) days prior to termination.

Additionally, if during the Term of this Agreement, Entity makes changes to its hardware or network configuration in such a manner that CIS is no longer able to provide the CSS to Entity, CIS shall have the ability to terminate this Agreement upon written notice to Entity.

The ability and obligation of CIS to provide these Cybersecurity Services and devices to the Entity is, at all times, contingent on the availability and allocation of federal funds for this purpose.

VII. Amendments to this Agreement

This Agreement may only be amended as agreed to in writing by both Parties.

VIII. No Third Party Rights

Nothing in this Agreement shall create or give to third parties any claim or right of action of any nature against Entity or CIS.

IX. Disclaimer

Both Parties disclaim all express and implied warranties with regard to the CSS provided for herein, and neither Party assumes any responsibility or liability for the accuracy of the information that is the subject of this Agreement, or for any act or omission or other performance related to the CSS provided under this Agreement.

X. Confidentiality Obligation

CIS acknowledges that information regarding the infrastructure and security of Entity information systems, assessments and plans that relate specifically and uniquely to the vulnerability of Entity information systems, the results of tests of the security of Entity information systems insofar as those results may reveal specific vulnerabilities or otherwise marked as confidential by Entity ("Confidential Information") may be provided by Entity to CIS in connection with the services provided under this Agreement. The Entity acknowledges that it may receive from CIS trade secrets and confidential and proprietary information ("Confidential Information"). Both Parties agree to hold each other's Confidential Information in confidence to the same extent and the same manner as each Party protects its own confidential information, but in no event will less than reasonable care be provided and a Party's information will not be released in any identifiable form without the express written permission of such Party or as required pursuant to lawfully authorized subpoena or similar compulsive directive or is required to be disclosed by law, provided that the Entity shall be required to make reasonable efforts, consistent with applicable law, to limit the scope and nature of such required disclosure. CIS shall, however, be permitted to disclose relevant aspects of such Confidential Information to its officers, employees, agents and CIS's cybersecurity partners, including federal partners, provided that such partners have agreed to protect the Confidential Information to the same extent as required under this Agreement. The Parties agree to use all reasonable steps to ensure that Confidential Information received under this Agreement is not disclosed in violation of this Section. These confidentiality obligations shall survive any future non-availability of federal funds to continue the program that supports this Agreement or the termination of this Agreement.

XI. Notices

A. All notices permitted or required hereunder shall be in writing and shall be transmitted either:

1. via certified or registered United States mail, return receipt requested;
2. by facsimile transmission;
3. by personal delivery;
4. by expedited delivery service; or
5. by e-mail with acknowledgement of receipt of the notice.

Such notices shall be addressed as follows or to such different addresses as the Parties may from time-to-time designate:

<u>CIS</u>

Name: Mark Perry
Title: Program Executive
Address: Center for Internet Security, Inc.
Elections Infrastructure Information Sharing and Analysis Center
31 Tech Valley Drive
East Greenbush, NY 12061-4134

Telephone Number: (518) 266-3476
Facsimile Number: (518) 283-3087
E-Mail Address: Mark.Perry@cisecurity.org

<u>Entity</u>

Name: Kevin carr
Title: chief Information officer
Address:701 Kimberly Drive, suite 285, Denton, TX 76208
Telephone Number: (940) 349-4500
Facsimile Number:
E-Mail Address: kevi n.carr@dentoncounty.com

B. Any such notice shall be deemed to have been given either at the time of personal delivery or, in the case of expedited delivery service or certified or registered United States mail, as of the date of first attempted delivery at the address and in the manner provided herein, or in the case of facsimile transmission or email, upon receipt.

C. The Parties may, from time to time, specify any new or different contact information as their address for purpose of receiving notice under this Agreement by giving fifteen (15) days written notice to the other Party sent in accordance herewith. The Parties agree to mutually designate individuals as their respective representatives for the purposes of receiving notices under this Agreement. Additional individuals may be designated in writing by the Parties for purposes of implementation and administration, resolving issues and problems and/ or for dispute resolution.

The foregoing has been agreed to and accepted by the authorized representatives of each Party whose signatures appear below:

CENTER FOR INTERNET SECURITY, INC.

By: —

Name: B.e.-")••I""' '" S"e-ev

Title: Dat"+ t l-tJO(

Date: ll / 19

Denton County, TX

By: Andy Eads

Name: Andy Eads

Title: County Judge

Date: August 6, 2019

Appendix A

CSS Responsibilities

I. **Entity Responsibilities** - Entity acknowledges and agrees that CIS's ability to perform the Cybersecurity Services provided by CIS for the benefit of Entity is subject to Entity fulfilling certain responsibilities listed below. Entity acknowledges and agrees that neither CIS nor any third party provider shall have any responsibility whatsoever to perform the Cybersecurity Services in the event Entity fails to meet its responsibilities described below.

A. For purposes of this Agreement, Entity acknowledges and agrees that only those security devices supported by CIS fall within the scope of this Agreement. Entity will ensure the correct functioning of devices except where Entity elects to have CIS manage the devices.

B. Entity shall provide logistic support in the form of rack space, electricity, Internet connectivity, and any other infrastructure necessary to support communications at Entity's expense.

C. Entity shall provide the following to CIS prior to the commencement of service and at any time during the term of the Agreement if the information changes:

1. Current network diagrams to facilitate analysis of security events on the portion(s) of Entity's network being monitored. Network diagrams will need to be revised whenever there is a substantial network change;
2. In-band access via a secure Internet channel to manage the device(s).
3. Outbound access via a secure Internet channel for log transmission.
4. Reasonable assistance to CIS as necessary, to enable CIS to deliver and perform the CSS for the benefit of Entity;
5. Maintenance of all required hardware, virtual machines, or software necessary for the sensor located at Entity's site, and enabling access to such hardware, virtual machines, or software as necessary for CIS to provide the CSS;
6. Public and Private IP address ranges including a list of servers being monitored including the type, operating system and configuration information; and list of IP ranges and addresses that are not in use by the Entity (DarkNet space);
7. Completed Pre-Installation Questionnaires (PIQ). The PIQ will need to be revised whenever there is a change that would

affect CIS's ability to provide the Cybersecurity Services;

8. Accurate and up-to-date information, including the name, email, landline, mobile, and pager numbers for all designated, authorized Point of Contact(s) who will be provided access to the portals, and;
9. The name, email address, and landline, mobile, and pager numbers for all shipping, installation and security points of contact.

D. With respect to the shipping and delivery of any required hardware, Entity agrees to the following:

1. For any hardware shipped directly to Entity, upon receipt of the hardware, Entity shall contact CIS to confirm the serial number of the hardware. Upon confirmation of the serial number, CIS will ship an identification tag to Entity. Entity agrees to place the identification tag on the hardware as per the accompanying instructions, and upon placement of the identification tag, to confirm in writing to CIS that the tag has been placed on the hardware.
2. In certain instances, CIS may ship hardware and software to Entity prior to the final execution of this Agreement. Notwithstanding the foregoing, Entity acknowledges that commencement of CSS is contingent on the execution of this Agreement by the parties.

E. During the term of this Agreement Entity shall provide the following:

1. Written notification to CIS SOC (SOC(@MSISAC.ORG) at least thirty (30) days in advance of changes in hardware or network configuration affecting CIS's ability to provide Cybersecurity Services, or a change to the physical location of the hardware; any notice relating to change in physical location shall include the new physical address of the hardware;
2. Written notification to CIS SOC (SOC@MSISAC.ORG) at least twelve (12) hours in advance of any scheduled downtime or other network and system administration scheduled tasks that would affect CIS's ability to provide the service;
3. A completed Escalation Procedure Form including the name, e-mail address and 24/7 contact information for all designated Points of Contact (POC). A revised Form must be submitted when there is a change in status forany POC;
4. Sole responsibility for maintaining current maintenance and technical support contracts with Entity's software and hardware vendors for any device affected by CSS that has not

been supplied by CIS;

5. Active involvement with CIS SOC to resolve any tickets requiring Entity input or action;
6. Reasonable assistance in remotely installing and troubleshooting devices including hardware and communications,
7. Upon reasonable notice from CIS and during normal business hours, access for CIS to inspect the hardware.

8. Response to biennial written confirmation notice from MS-ISAC as to the physical location of all hardware provided by CIS.

F. Certification. Entity shall complete the attached Entity Certification documenting compliance with the following:

1. That the Entity provides notice to its employees, contractors and other authorized internal network users (collectively, "Computer Users") that contain in sum and substance the following provisions:

   (a) Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity's information system; and
   (b) Any communications or data transiting, stored on or traveling to or from the Entity's information system may be monitored, disclosed or used for any lawful government purpose; and

2. That all Entity Computer Users execute some form of documentation or electronic acceptance acknowledging his/her understanding and consent to the above notice. Examples of notice documentation include, but are not limited to:

   a) log-on banners for computer access with an "I Agree" click through;
   b) consent form signed by the Computer User acknowledging Entity's computer use policy; or
   c) computer use agreement executed by the Computer User.

II. CIS Responsibilities

A. CIS will be responsible for the correct functioning of managed devices.

B. CIS shall be responsible for the purchase of certain hardware, and shall arrange for the shipping of such hardware to a location designated by Entity. Upon notice from Entity that the hardware has been delivered and upon confirmation of the serial number of the hardware, CIS shall be responsible for providing Entity with an identification tag to be placed on the hardware.

C. CIS will provide the following as part of the service:

1. Analysis of logs from monitored security devices for attacks and malicious traffic;
2. Analysis of security events;
3. Correlation of security data/logs/events with information from other sources;
4. Notification of security events per the Escalation Procedures provided by Entity.
5. Ensuring that all upgrades, patches, configuration changes and signature upgrades are applied to managed devices. CIS will provide the appropriate license and support agreements for the upgrade for devices provided by CIS. The Entity is responsible for maintaining the appropriate license and support agreements for devices own by the Entity.

D. Access to Stored Flow Data. CIS shall provide access to normalized logs, security events and netflow data through batch queries.

E. CIS Security Operation Center. CIS will provide 24/7 telephone (1-866-787-4722) availability for assistance with events detected by the CSS.

F. Biennial Confirmation for Hardware Location. Every two years, CIS will send Entity a request for confirmation of the physical location of the hardware provided as part of the CSS, including description, serial number and address of physical location of hardware.

ENTITY CERTIFICATION

On behalf of _o_e_n_t_o_n_c_o_u_nt_Y_,_T_ex_a_s____________ ("Entity"), I hereby certify the following:

1. Entity provides notice to its employees, contractors and other authorized internal network users ("collectively "Computer Users") that contain in sum and substance the following provisions:

   -Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity's information system; and

   -Any communications or data transiting, stored on or traveling to or from the Entity's information system may be monitored, disclosed or used for any lawful government purpose.

2. All Entity Computer Users execute a form of documentation or electronic acceptance acknowledging his/her understanding and consent to the above notice.

3. I am authorized to execute this Certification on behalf of Entity.

Dated this 6th day of August, 2019.

Andy Eads

Name: Andy Eads
Title: County Judge

EXHIBIT E

The Office of Secretary of State

Brian P. Kemp
SECRETARY OF STATE

December 8, 2016

The Honorable Jeh Johnson
Secretary of Homeland Security
Department of Homeland Security
Washington, D.C. 20528

Secretary Johnson,

On November 15, 2016, an IP address associated with the Department of Homeland Security made an unsuccessful attempt to penetrate the Georgia Secretary of State's firewall. I am writing you to ask whether DHS was aware of this attempt and, if so, why DHS was attempting to breach our firewall.

The private-sector security provider that monitors the agency's firewall detected a large unblocked scan event on November 15 at 8:43 AM. The event was an IP address (216.81.81.80) attempting to scan certain aspects of the Georgia Secretary of State's infrastructure. The attempt to breach our system was unsuccessful.

At no time has my office agreed to or permitted DHS to conduct penetration testing or security scans of our network. Moreover, your Department has not contacted my office since this unsuccessful incident to alert us of any security event that would require testing or scanning of our network. This is especially odd and concerning since I serve on the Election Cyber Security Working Group that your office created.

As you may know, the Georgia Secretary of State's office maintains the statewide voter registration database containing the personal information of over 6.5 million Georgians. In addition, we hold the information for over 800,000 corporate entities and over 500,000 licensed or registered professionals.

As Georgia's Secretary of State, I take cyber security very seriously. That is why I have contracted with a global leader in monitored security services to provide immediate responses to these types of threats. This firm analyzes more than 180 billion events a day globally across a 5,000+ customer base which includes many Fortune 500 companies. Clearly, this type of resource and service is necessary to protect Georgians' data against the type of event that occurred on November 15.

Georgia was one of the only few states that did not seek DHS assistance with cyber hygiene scans or penetration testing before this year's election. We declined this assistance due to having already implemented the security measures suggested by DHS. Under 18 U.S.C. § 1030, attempting to gain access or exceeding authorized access to protected computer systems is illegal. Given all these facts, a number of very important questions have been raised that deserve your attention:

1. Did your Department in fact conduct this unauthorized scan?
2. If so, who on your staff authorized this scan?
3. Did your Department conduct this type of scan against any other states' systems without authorization?
4. If so, which states were scanned by DHS without authorization?

I am very concerned by these facts provided by our security services provider, as they raise very serious questions. I would appreciate your prompt and thorough response.

Sincerely,

Brian P. Kemp

CC:

The Honorable Johnny Isakson
United States Senate

The Honorable David Perdue
United States Senate

The Honorable Buddy Carter
United States House of Representatives

The Honorable Sanford Bishop
United States House of Representatives

The Honorable Lynn Westmoreland
United States House of Representatives

The Honorable Hank Johnson
United States House of Representatives

The Honorable John Lewis
United States House of Representatives

The Honorable Tom Price
United States House of Representatives

The Honorable Rob Woodall
United States House of Representatives

The Honorable Austin Scott
United States House of Representatives

The Honorable Doug Collins
United States House of Representatives

The Honorable Jody Hice
United States House of Representatives

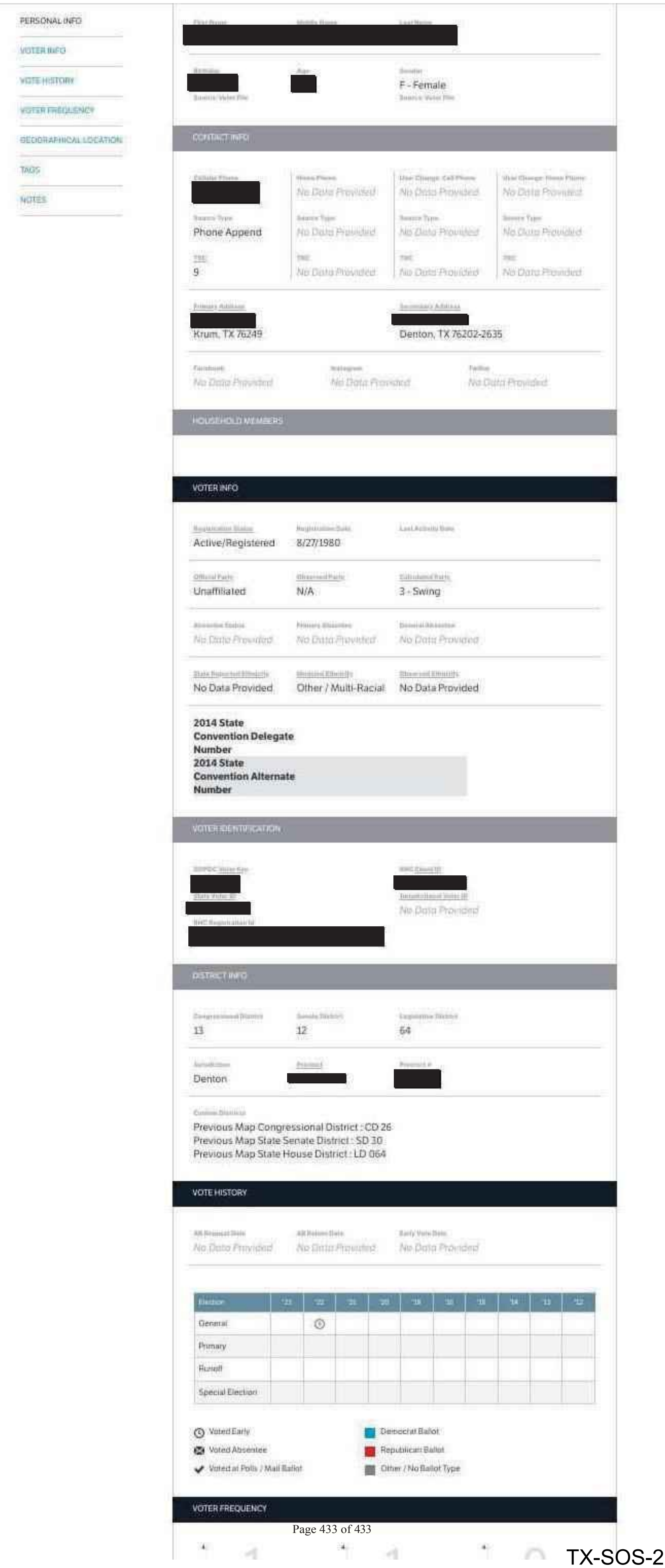
The Honorable Barry Loudermilk
United States House of Representatives

The Honorable Rick Allen
United States House of Representatives

The Honorable David Scott
United States House of Representatives

The Honorable Tom Graves
United States House of Representative

EXHIBIT F



First Name Middle Name Last Name
[redacted]

Birthdate	Age	Gender
[redacted]	[redacted]	F - Female
Source: Voter File		Source: Voter File

CONTACT INFO

Cellular Phone	Home Phone	User Change: Cell Phone	User Change: Home Phone
[redacted]	No Data Provided	No Data Provided	No Data Provided
Source Type	Source Type	Source Type	Source Type
Phone Append	No Data Provided	No Data Provided	No Data Provided
TRC	TRC	TRC	TRC
9	No Data Provided	No Data Provided	No Data Provided

Primary Address	Secondary Address
[redacted] Krum, TX 76249	[redacted] Denton, TX 76202-2635

Facebook	Instagram	Twitter
No Data Provided	No Data Provided	No Data Provided

HOUSEHOLD MEMBERS

VOTER INFO

Registration Status	Registration Date	Last Activity Date
Active/Registered	8/27/1980	

Official Party	Observed Party	Calculated Party
Unaffiliated	N/A	3 - Swing

Absentee Status	Primary Absentee	General Absentee
No Data Provided	No Data Provided	No Data Provided

State Reported Ethnicity	Modeled Ethnicity	Observed Ethnicity
No Data Provided	Other / Multi-Racial	No Data Provided

2014 State Convention Delegate Number
2014 State Convention Alternate Number

VOTER IDENTIFICATION

SOPDC Voter Key [redacted]	RNC Count ID [redacted]
State Voter ID [redacted]	Jurisdictional Voter ID No Data Provided
RNC Registration Id [redacted]	

DISTRICT INFO

Congressional District	Senate District	Legislative District
13	12	64

Jurisdiction	Precinct	Precinct #
Denton	[redacted]	[redacted]

Custom Districts
Previous Map Congressional District : CD 26
Previous Map State Senate District : SD 30
Previous Map State House District : LD 064

VOTE HISTORY

AB Request Date	AB Return Date	Early Vote Date
No Data Provided	No Data Provided	No Data Provided

Election	'23	'22	'21	'20	'19	'18	'16	'14	'13	'12
General		🕓								
Primary										
Runoff										
Special Election										

🕓 Voted Early
✉ Voted Absentee
✓ Voted at Polls / Mail Ballot

🟦 Democrat Ballot
🟥 Republican Ballot
⬛ Other / No Ballot Type

VOTER FREQUENCY

EXHIBIT G

09:34AM interest -- interest in these contracts. And not only
09:34AM that, we also asked for the signed certificates for SLI
09:34AM and Hart. You know, we didn't get that either.

09:34AM So, I mean, we're asking for the
09:34AM certification, you know, for these electronic voting
09:34AM systems. They're not certified. They're not legally
09:34AM certified. We all know that.

09:34AM THE COURT: Okay. So, from what little I
09:34AM know about this case, it does seem to revolve around
09:34AM these certifications. You either have those, or you
09:34AM don't. But, if you do, certainly, those would be
09:34AM discoverable?

09:34AM MR. SHOVLIN: Yes. And they've -- I mean,
09:34AM they were attached to our response to our motion to
09:34AM dismiss. I mean those are attached as exhibits to
09:34AM the --

09:34AM THE COURT: Did you furnish them in
09:34AM response to their discovery?

09:34AM MR. SHOVLIN: Yes, also in response to
09:35AM their discovery.

09:35AM MR. LINCOLN ACHILLI: Your Honor, I'm a
09:35AM plaintiff in this case, Lincoln Achilli. The items that
09:35AM we have received were letters from inspectors who had
09:35AM recommended certifications. We were not actually
09:35AM furnished a copy of the certificate itself.

09:35AM THE COURT: Do you --
09:35AM MR. SHOVLIN: The Secretary of State is, by
09:35AM statute, 100 percent in charge of the certification
09:35AM process for these. I mean I -- I don't --
09:35AM Frank, do you have a certificate?
09:35AM MR. FRANK PHILLIPS: Judge, if I may?
09:35AM MR. SHOVLIN: Frank Phillips is the
09:35AM Election Administrator.
09:35AM THE COURT: Okay.
09:35AM MR. FRANK PHILLIPS: I've never seen any
09:35AM such certificate. The county does not certify
09:35AM equipment. The State of Texas certifies equipment, and
09:35AM they -- if there's such a document, they would be the
09:35AM ones holding that document.
09:35AM THE COURT: Okay. So what is your response
09:36AM to their position that -- that there are -- her words,
09:36AM quo warranto letters, or something, that would be
09:36AM responsive to Request No. 7? Okay.
09:36AM MR. FELDT: Judge, I'm John Feldt. So the
09:36AM district attorney's office received letters from
09:36AM citizens requesting a quo warranto action to be filed.
09:36AM And the district attorney's office responded to the
09:36AM individuals that sent the letters with the letter and --
09:36AM signed by me. So I don't know that that actually has
09:36AM anything to do with the type of communications that

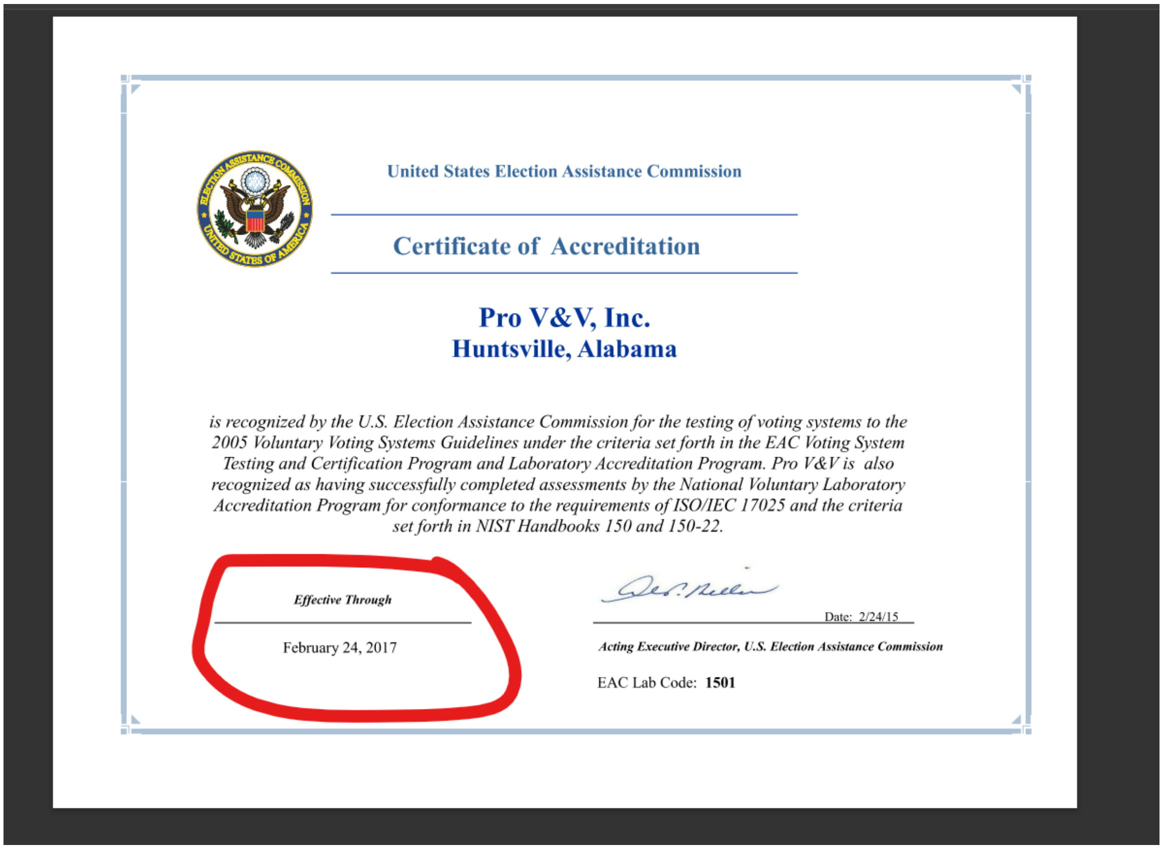
EXHIBIT Q

Declaration of Terpsehore P Maras

Pursuant to 28 U.S.C Section 1746, I, Terpsehore P Maras, make the following declaration.

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

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



United States Election Assistance Commission

Certificate of Accreditation

Pro V&V, Inc.
Huntsville, Alabama

is recognized by the U.S. Election Assistance Commission for the testing of voting systems to the 2005 Voluntary Voting Systems Guidelines under the criteria set forth in the EAC Voting System Testing and Certification Program and Laboratory Accreditation Program. Pro V&V is also recognized as having successfully completed assessments by the National Voluntary Laboratory Accreditation Program for conformance to the requirements of ISO/IEC 17025 and the criteria set forth in NIST Handbooks 150 and 150-22.

Effective Through

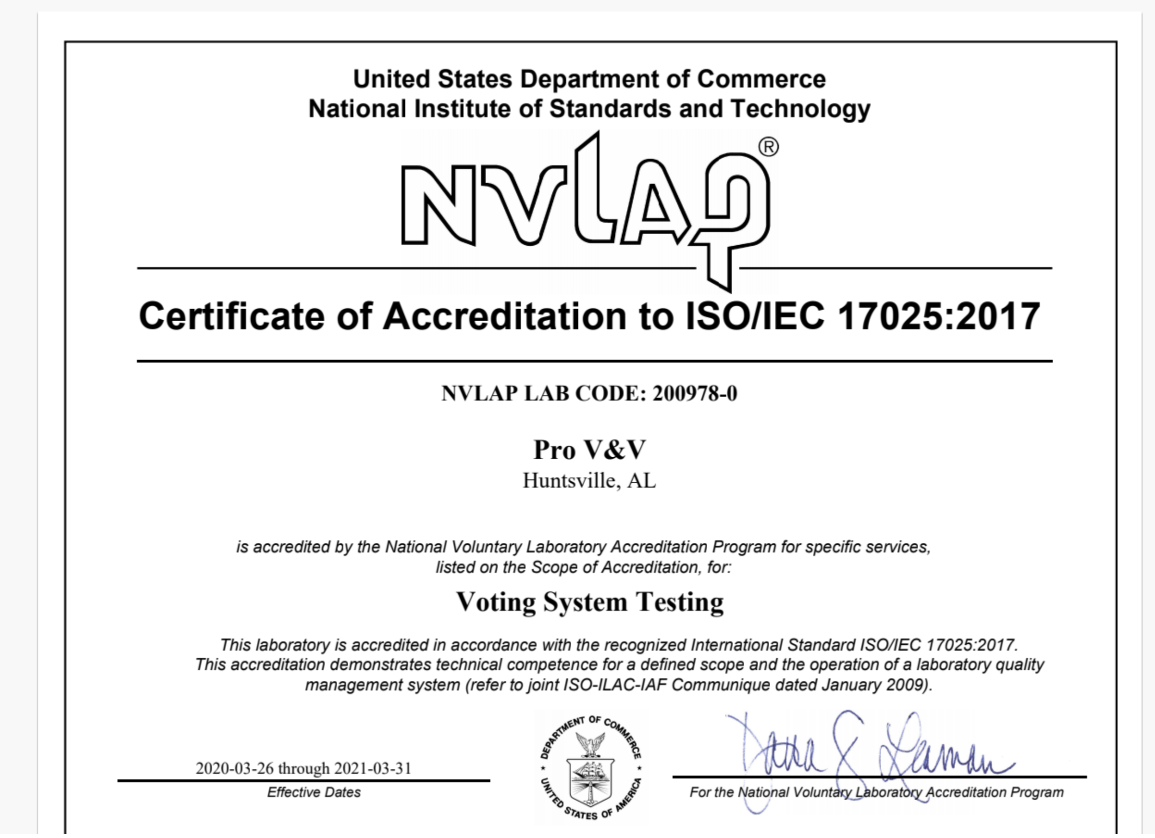
February 24, 2017

Date: 2/24/15

Acting Executive Director, U.S. Election Assistance Commission

EAC Lab Code: **1501**

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

10. 

United States Department of Commerce
National Institute of Standards and Technology

NVLAP®

Certificate of Accreditation to ISO/IEC 17025:2017

NVLAP LAB CODE: 200978-0

Pro V&V
Huntsville, AL

is accredited by the National Voluntary Laboratory Accreditation Program for specific services, listed on the Scope of Accreditation, for:

Voting System Testing

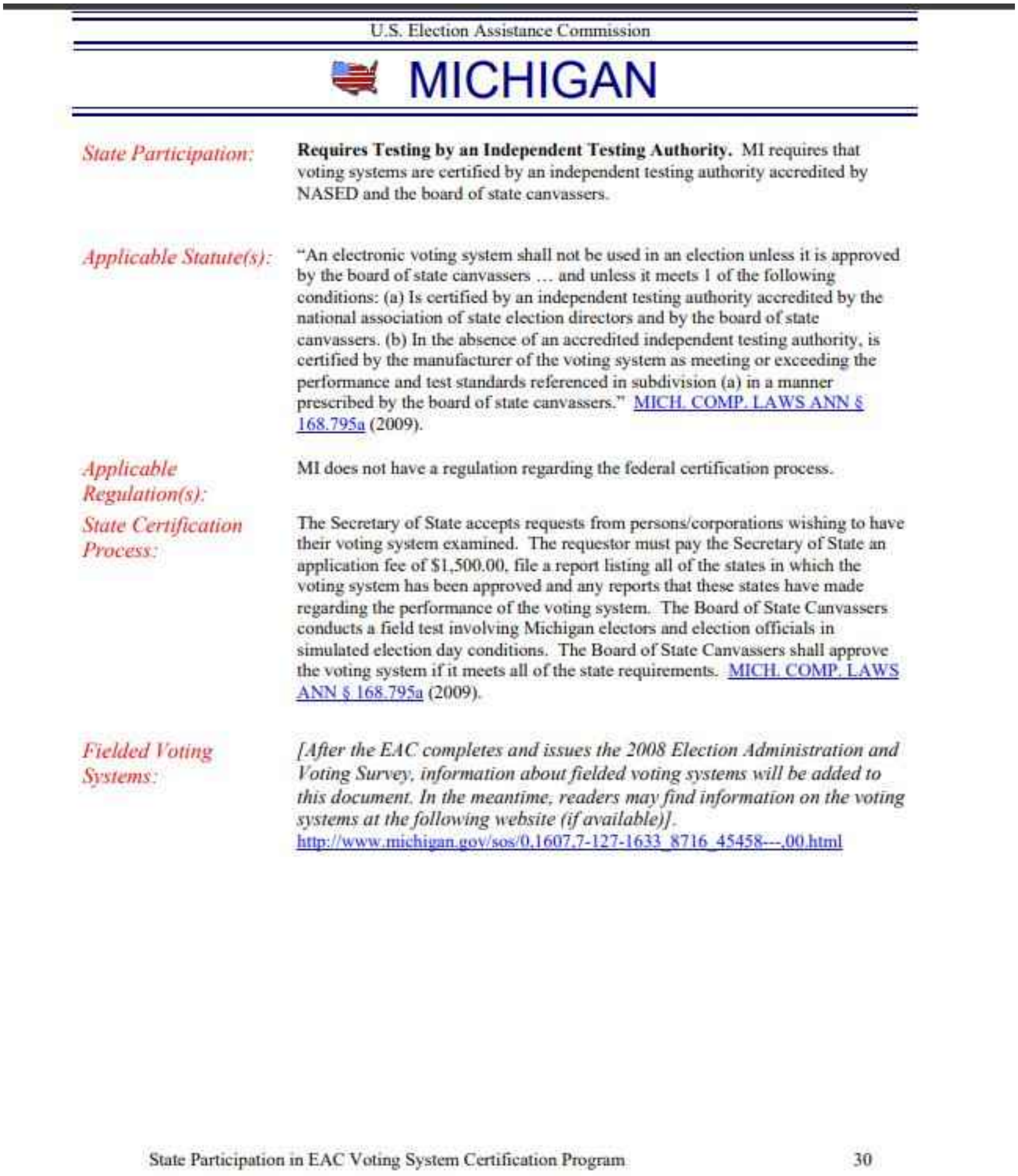
This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2017. This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality management system (refer to joint ISO-ILAC-IAF Communique dated January 2009).

DEPARTMENT OF COMMERCE • UNITED STATES OF AMERICA

2020-03-26 through 2021-03-31
Effective Dates

Dana S Leaman
For the National Voluntary Laboratory Accreditation Program

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



MICHIGAN

State Participation:

Requires Testing by an Independent Testing Authority. MI requires that voting systems are certified by an independent testing authority accredited by NASED and the board of state canvassers.

Applicable Statute(s):

"An electronic voting system shall not be used in an election unless it is approved by the board of state canvassers … and unless it meets 1 of the following conditions: (a) Is certified by an independent testing authority accredited by the national association of state election directors and by the board of state canvassers. (b) In the absence of an accredited independent testing authority, is certified by the manufacturer of the voting system as meeting or exceeding the performance and test standards referenced in subdivision (a) in a manner prescribed by the board of state canvassers." MICH. COMP. LAWS ANN § 168.795a (2009).

Applicable Regulation(s):

MI does not have a regulation regarding the federal certification process.

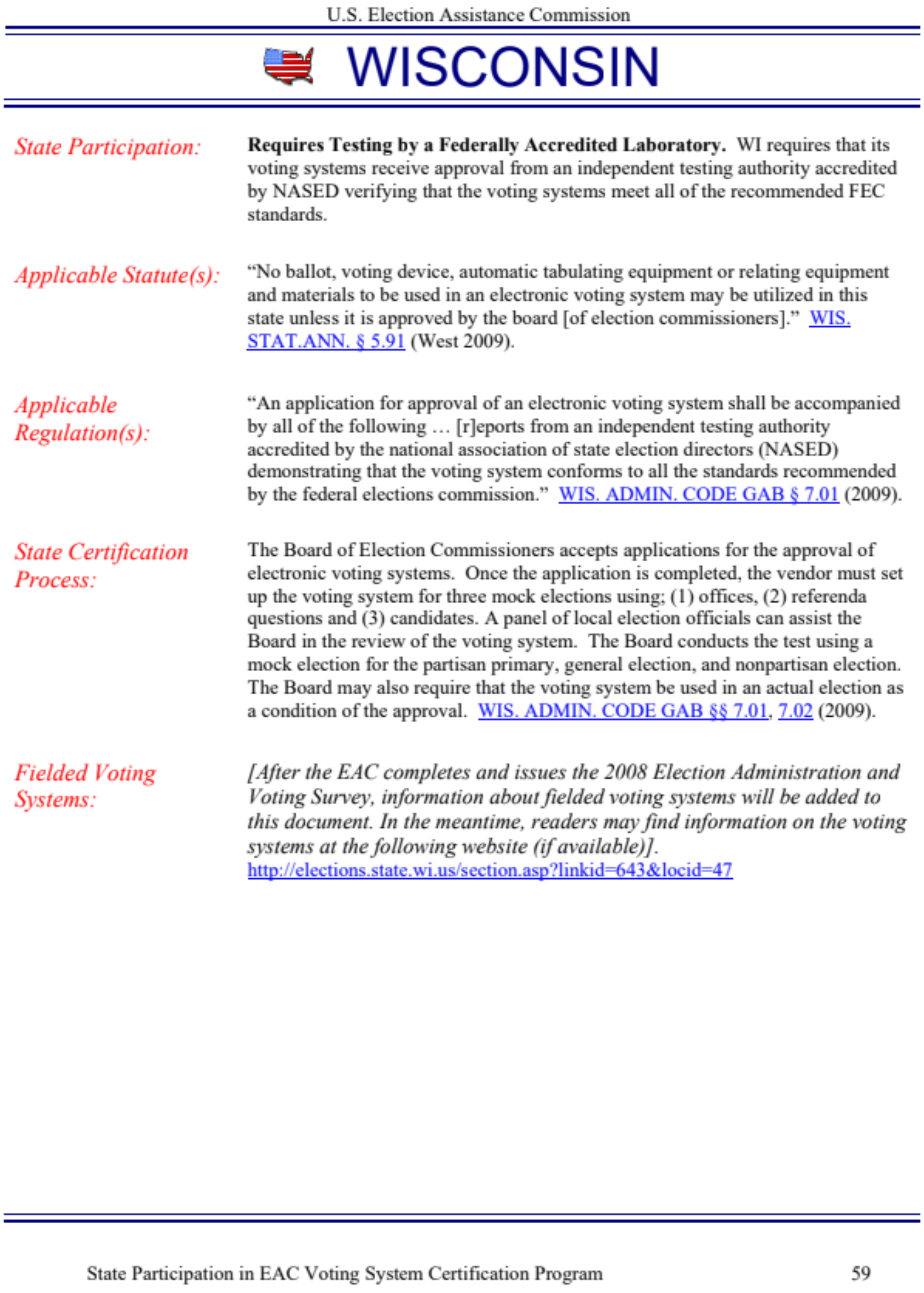
State Certification Process:

The Secretary of State accepts requests from persons/corporations wishing to have their voting system examined. The requestor must pay the Secretary of State an application fee of $1,500.00, file a report listing all of the states in which the voting system has been approved and any reports that these states have made regarding the performance of the voting system. The Board of State Canvassers conducts a field test involving Michigan electors and election officials in simulated election day conditions. The Board of State Canvassers shall approve the voting system if it meets all of the state requirements. MICH. COMP. LAWS ANN § 168.795a (2009).

Fielded Voting Systems:

[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].
http://www.michigan.gov/sos/0,1607,7-127-1633_8716_45458---,00.html

13.



WISCONSIN

State Participation: **Requires Testing by a Federally Accredited Laboratory.** WI requires that its voting systems receive approval from an independent testing authority accredited by NASED verifying that the voting systems meet all of the recommended FEC standards.

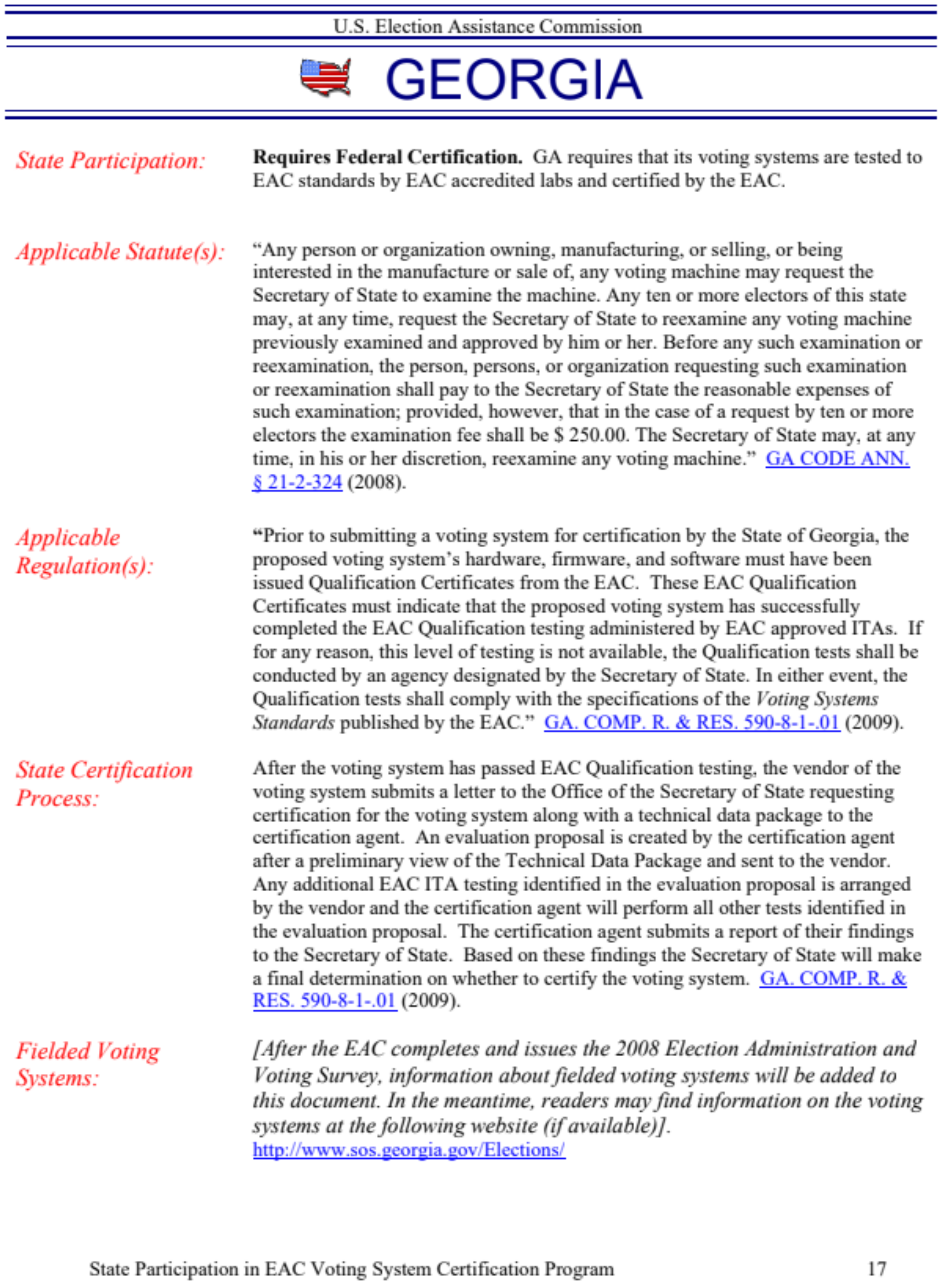
Applicable Statute(s): "No ballot, voting device, automatic tabulating equipment or relating equipment and materials to be used in an electronic voting system may be utilized in this state unless it is approved by the board [of election commissioners]." WIS. STAT.ANN. § 5.91 (West 2009).

Applicable Regulation(s): "An application for approval of an electronic voting system shall be accompanied by all of the following … [r]eports from an independent testing authority accredited by the national association of state election directors (NASED) demonstrating that the voting system conforms to all the standards recommended by the federal elections commission." WIS. ADMIN. CODE GAB § 7.01 (2009).

State Certification Process: The Board of Election Commissioners accepts applications for the approval of electronic voting systems. Once the application is completed, the vendor must set up the voting system for three mock elections using; (1) offices, (2) referenda questions and (3) candidates. A panel of local election officials can assist the Board in the review of the voting system. The Board conducts the test using a mock election for the partisan primary, general election, and nonpartisan election. The Board may also require that the voting system be used in an actual election as a condition of the approval. WIS. ADMIN. CODE GAB §§ 7.01, 7.02 (2009).

Fielded Voting Systems: *[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].* http://elections.state.wi.us/section.asp?linkid=643&locid=47

14.



GEORGIA

State Participation:

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

Applicable Statute(s):

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

Applicable Regulation(s):

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

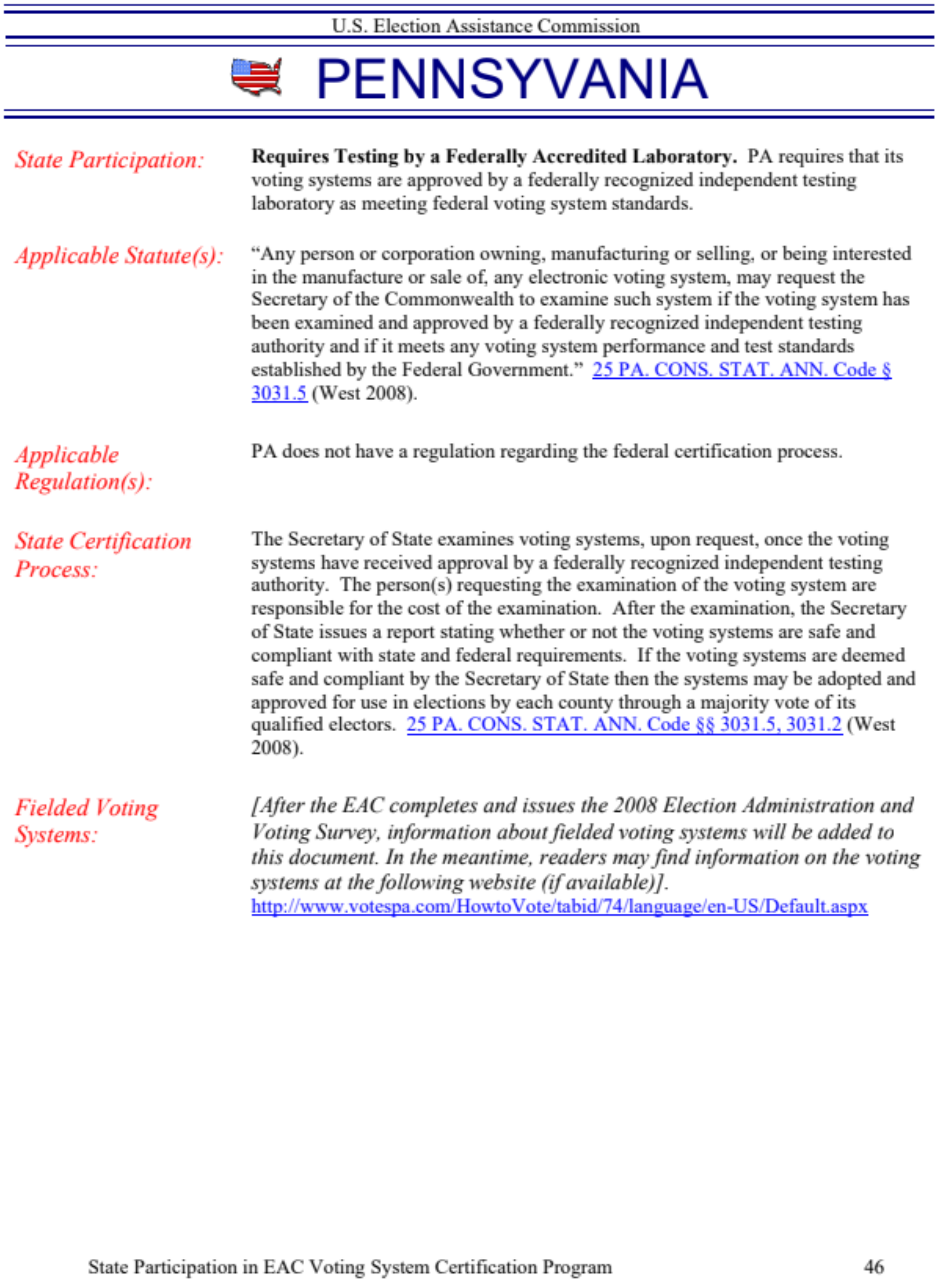
State Certification Process:

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

Fielded Voting Systems:

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

15.



PENNSYVANIA

State Participation:

Requires Testing by a Federally Accredited Laboratory. PA requires that its voting systems are approved by a federally recognized independent testing laboratory as meeting federal voting system standards.

Applicable Statute(s):

"Any person or corporation owning, manufacturing or selling, or being interested in the manufacture or sale of, any electronic voting system, may request the Secretary of the Commonwealth to examine such system if the voting system has been examined and approved by a federally recognized independent testing authority and if it meets any voting system performance and test standards established by the Federal Government." 25 PA. CONS. STAT. ANN. Code § 3031.5 (West 2008).

Applicable Regulation(s):

PA does not have a regulation regarding the federal certification process.

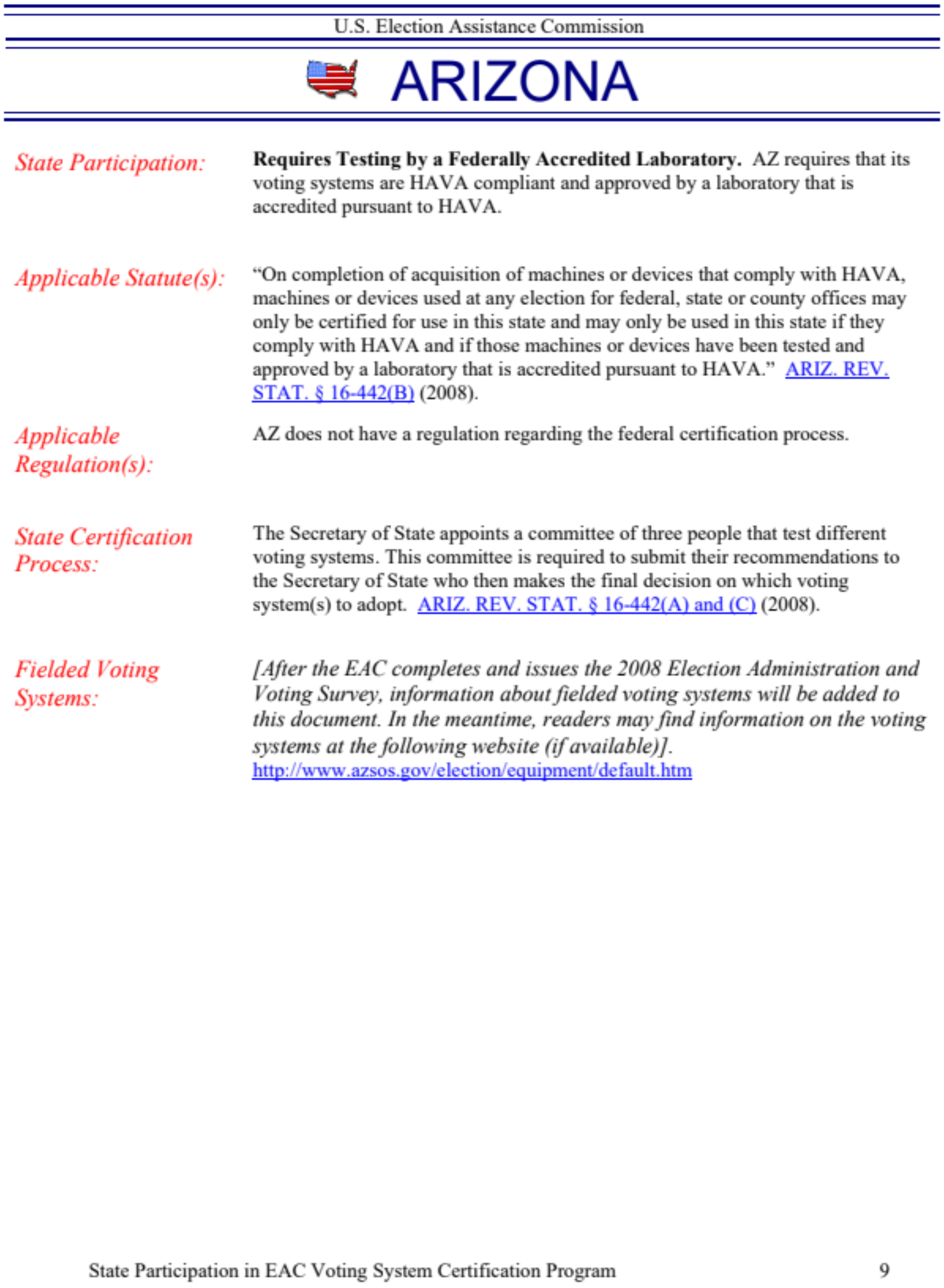
State Certification Process:

The Secretary of State examines voting systems, upon request, once the voting systems have received approval by a federally recognized independent testing authority. The person(s) requesting the examination of the voting system are responsible for the cost of the examination. After the examination, the Secretary of State issues a report stating whether or not the voting systems are safe and compliant with state and federal requirements. If the voting systems are deemed safe and compliant by the Secretary of State then the systems may be adopted and approved for use in elections by each county through a majority vote of its qualified electors. 25 PA. CONS. STAT. ANN. Code §§ 3031.5, 3031.2 (West 2008).

Fielded Voting Systems:

[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)]. http://www.votespa.com/HowtoVote/tabid/74/language/en-US/Default.aspx

16.



U.S. Election Assistance Commission

ARIZONA

State Participation:

Requires Testing by a Federally Accredited Laboratory. AZ requires that its voting systems are HAVA compliant and approved by a laboratory that is accredited pursuant to HAVA.

Applicable Statute(s):

"On completion of acquisition of machines or devices that comply with HAVA, machines or devices used at any election for federal, state or county offices may only be certified for use in this state and may only be used in this state if they comply with HAVA and if those machines or devices have been tested and approved by a laboratory that is accredited pursuant to HAVA." ARIZ. REV. STAT. § 16-442(B) (2008).

Applicable Regulation(s):

AZ does not have a regulation regarding the federal certification process.

State Certification Process:

The Secretary of State appoints a committee of three people that test different voting systems. This committee is required to submit their recommendations to the Secretary of State who then makes the final decision on which voting system(s) to adopt. ARIZ. REV. STAT. § 16-442(A) and (C) (2008).

Fielded Voting Systems:

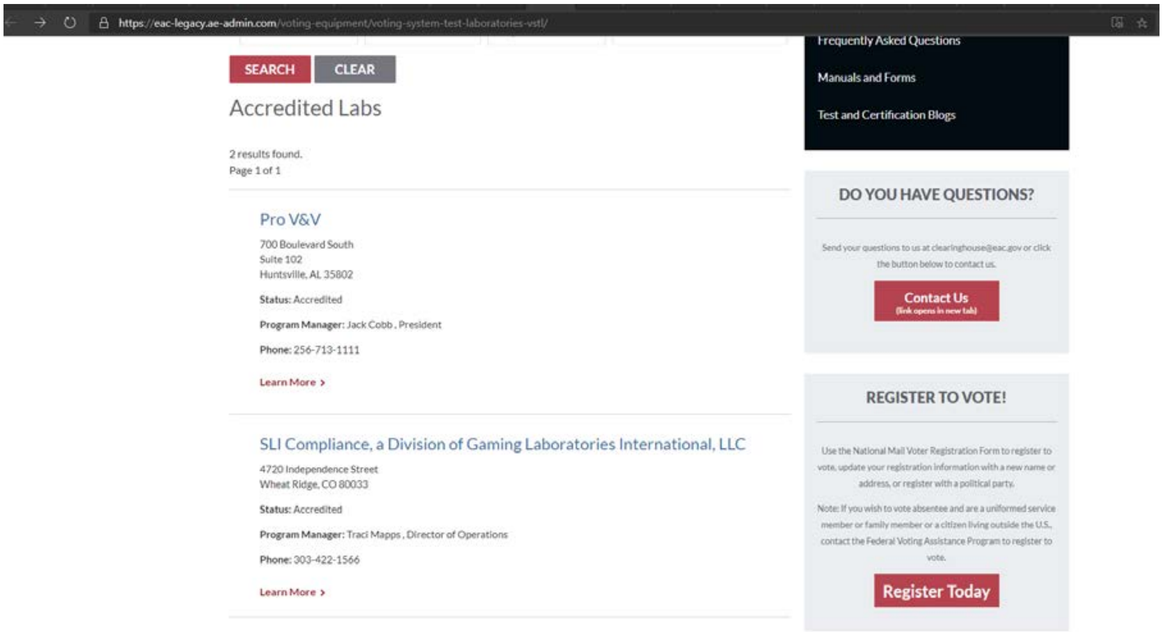
[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].
http://www.azsos.gov/election/equipment/default.htm

State Participation in EAC Voting System Certification Program 9

17.

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

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


https://eac-legacy.ae-admin.com/voting-equipment/voting-system-test-laboratories-vstl/
SEARCH
CLEAR
Frequently Asked Questions
Manuals and Forms
Test and Certification Blogs
Contact Us
(link opens in new tab)
Register Today

Accredited Labs

2 results found.
Page 1 of 1

Pro V&V

700 Boulevard South
Suite 102
Huntsville, AL 35802

Status: Accredited

Program Manager: Jack Cobb , President

Phone: 256-713-1111

Learn More ›

SLI Compliance, a Division of Gaming Laboratories International, LLC

4720 Independence Street
Wheat Ridge, CO 80033

Status: Accredited

Program Manager: Traci Mapps , Director of Operations

Phone: 303-422-1566

Learn More ›

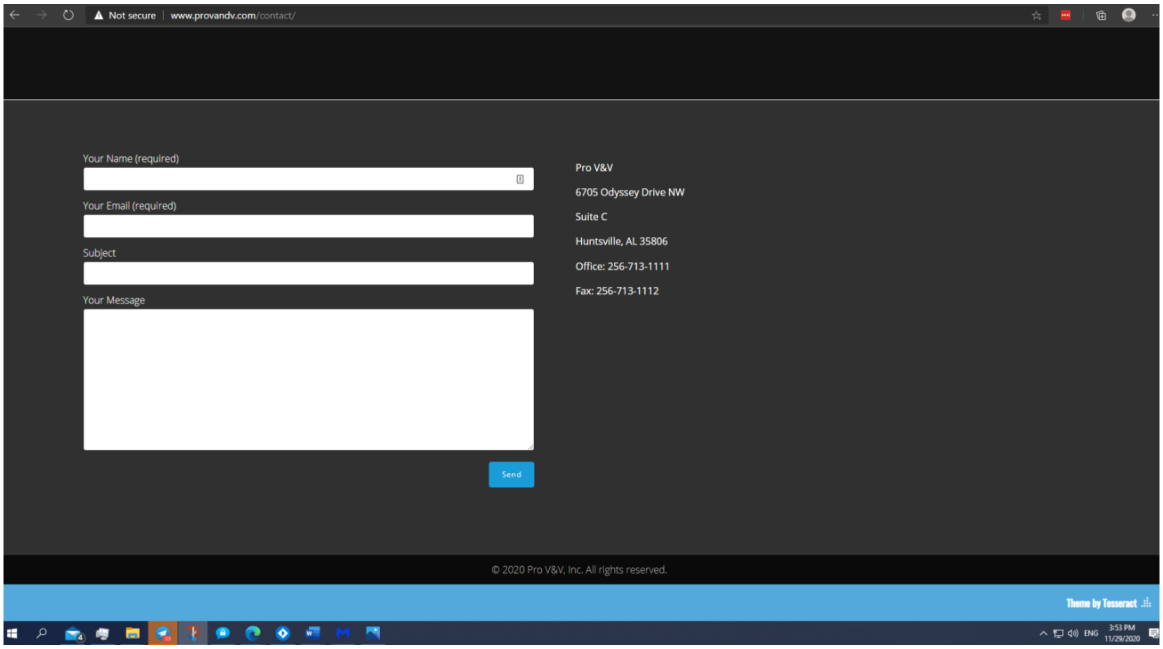
DO YOU HAVE QUESTIONS?

Send your questions to us at clearinghouse@eac.gov or click the button below to contact us.

REGISTER TO VOTE!

Use the National Mail Voter Registration Form to register to vote, update your registration information with a new name or address, or register with a political party.

Note: If you wish to vote absentee and are a uniformed service member or family member or a citizen living outside the U.S., contact the Federal Voting Assistance Program to register to vote.



Your Name (required)

Your Email (required)

Subject

Your Message

Pro V&V
6705 Odyssey Drive NW
Suite C
Huntsville, AL 35806
Office: 256-713-1111
Fax: 256-713-1112

© 2020 Pro V&V, Inc. All rights reserved.

20. VSTLs are the most important component of the election machines as they examine the use of COTS (Commercial Off–The-Shelf)

21. "Wyle became involved with the testing of electronic voting systems in the early 1990's and has tested over 150 separate voting systems. Wyle was the first company to obtain accreditation by the National Association of State Election Directors (NASED). Wyle is accredited by the Election Assistance Commission (EAC) as a Voting System Testing Laboratory (VSTL). Our scope of accreditation as a VSTL encompasses all aspects of the hardware and software of a voting machine. Wyle also received NVLAP accreditation to ISO/IEC 17025:2005 from NIST." Testimony of Jack Cobb 2009

22. COTS are preferred by many because they have been tried and tested in the open market and are most economic and readily available. COTS are also the SOURCE of vulnerability therefore VSTLs are VERY important. COTS components by voting system machine manufacturers can be used as a "Black Box" and changes to their specs and hardware make up change continuously. Some changes can be simple upgrades to make them more efficient in operation, cost efficient for production, end of life (EOL) and even complete reworks to meet new standards. They key issue in this is that MOST of the COTS used by Election Machine Vendors like Dominion, ES&S, Hart Intercivic, Smartmatic and others is that such manufacturing for COTS have been outsourced to China which if implemented in our Election Machines make us vulnerable to BLACK BOX antics and backdoors due to hardware changes that can go undetected. This is why VSTL's are VERY important.

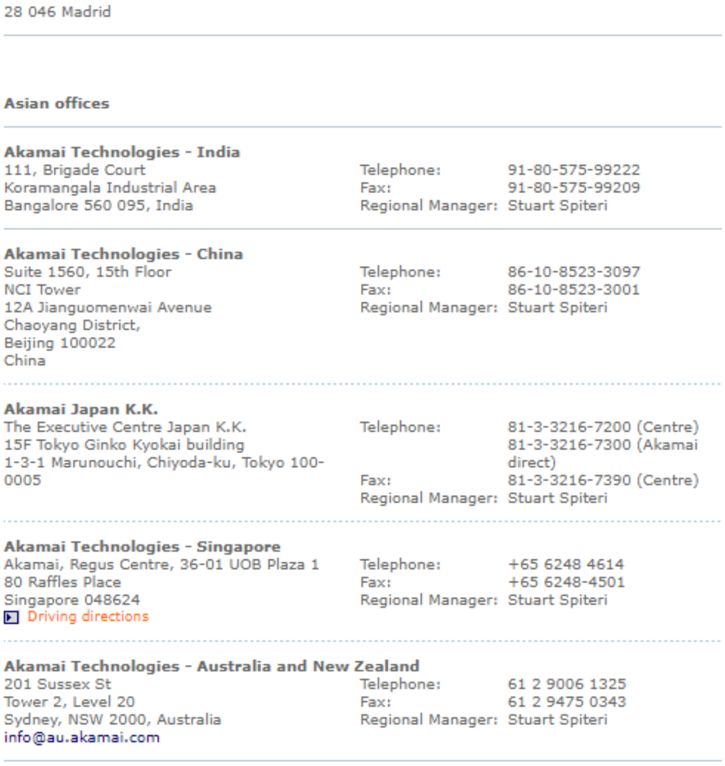
23. The proprietary voting system software is done so and created with cost efficiency in mind and therefore relies on 3rd party software that is AVAILABLE and HOUSED on the HARDWARE. This is a vulnerability. Exporting system reporting using software like Crystal Reports, or PDF software allows for vulnerabilities with their constant updates.

24. As per the COTS hardware components that are fixed, and origin may be cloaked under proprietary information a major vulnerability exists since once again third-party support software is dynamic and requires FREQUENT updates. The hardware components of the computer components, and election machines that are COTS may have slight updates that can be overlooked as they may be like those designed that support the other third -party software. COTS origin is important and the US Intelligence Community report in 2018 verifies that.

25. The Trump Administration made it clear that there is an absence of a major U.S. alternative to foreign suppliers of networking equipment. This highlights the growing dominance of

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

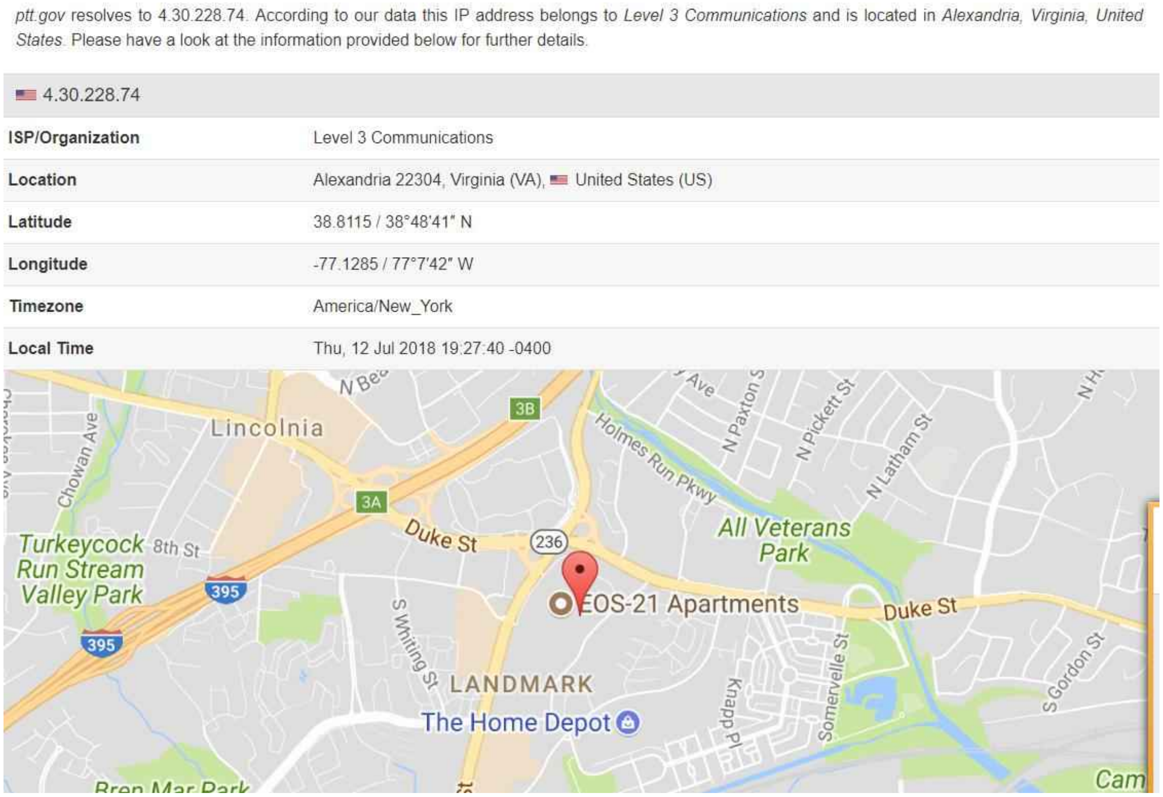
26. China, is not the only nation involved in COTS provided to election machines or the networking but so is Germany via a LAOS founded Chinese linked cloud service company that works with SCYTL named Akamai Technologies that have offices in China and are linked to the server that Dominion Software.



28 046 Madrid

Asian offices

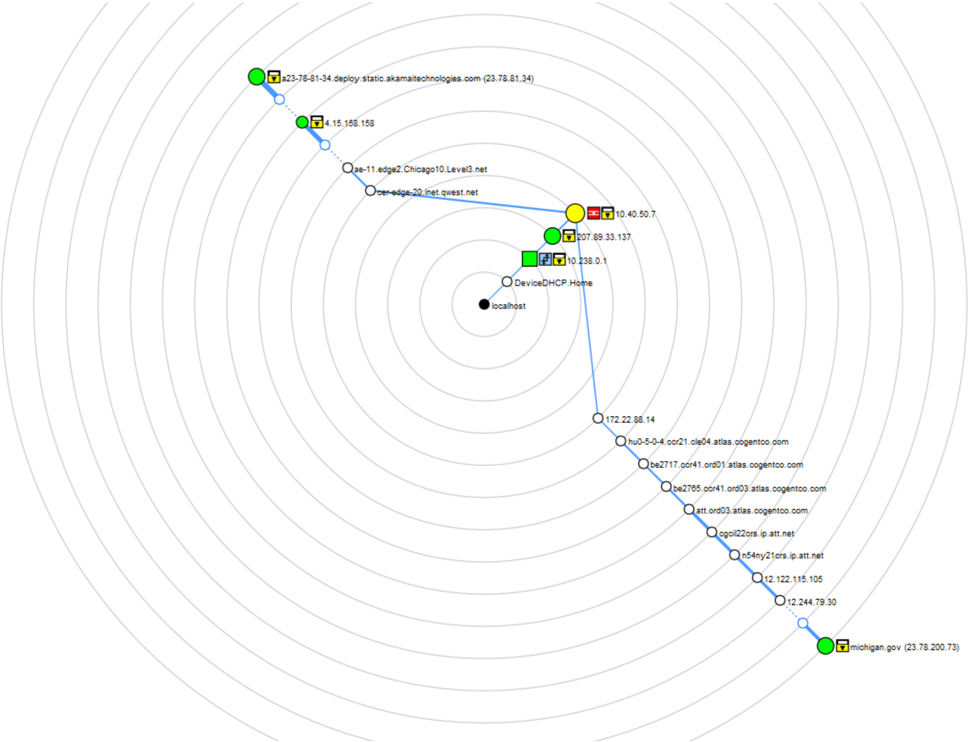
Akamai Technologies - India 111, Brigade Court Koramangala Industrial Area Bangalore 560 095, India	Telephone: Fax: Regional Manager:	91-80-575-99222 91-80-575-99209 Stuart Spiteri
Akamai Technologies - China Suite 1560, 15th Floor NCI Tower 12A Jianguomenwai Avenue Chaoyang District, Beijing 100022 China	Telephone: Fax: Regional Manager:	86-10-8523-3097 86-10-8523-3001 Stuart Spiteri
Akamai Japan K.K. The Executive Centre Japan K.K. 15F Tokyo Ginko Kyokai building 1-3-1 Marunouchi, Chiyoda-ku, Tokyo 100-0005	Telephone: Fax: Regional Manager:	81-3-3216-7200 (Centre) 81-3-3216-7300 (Akamai direct) 81-3-3216-7390 (Centre) Stuart Spiteri
Akamai Technologies - Singapore Akamai, Regus Centre, 36-01 UOB Plaza 1 80 Raffles Place Singapore 048624 ▶ Driving directions	Telephone: Fax: Regional Manager:	+65 6248 4614 +65 6248-4501 Stuart Spiteri
Akamai Technologies - Australia and New Zealand 201 Sussex St Tower 2, Level 20 Sydney, NSW 2000, Australia info@au.akamai.com	Telephone: Fax: Regional Manager:	61 2 9006 1325 61 2 9475 0343 Stuart Spiteri

27. 

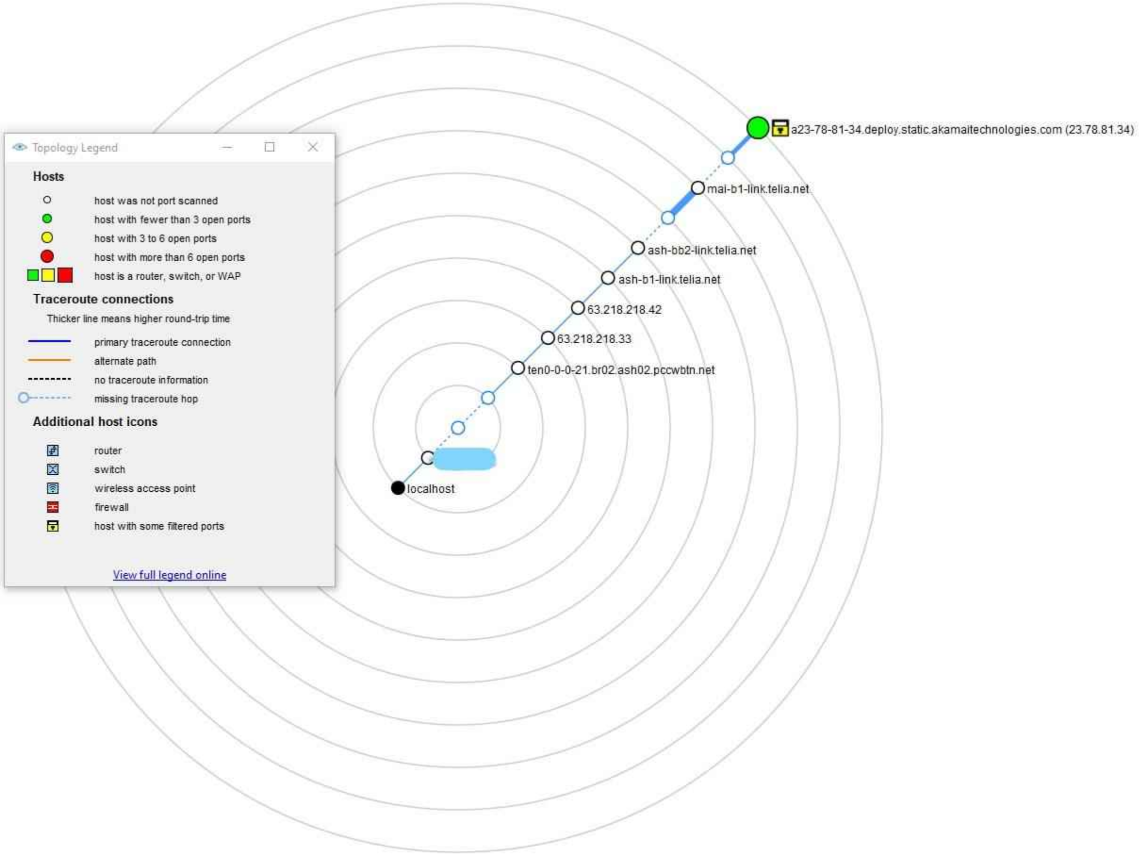
ptt.gov resolves to 4.30.228.74. According to our data this IP address belongs to *Level 3 Communications* and is located in *Alexandria, Virginia, United States*. Please have a look at the information provided below for further details.

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

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


a23-78-81-34.deploy.static.akamaitechnologies.com (23.78.81.34)
4.15.158.158
ae-11.edge2.Chicago10.Level3.net
cer-edge-20.inet.qwest.net
10.40.50.7
207.89.33.137
10.238.0.1
DeviceDHCP.Home
localhost
172.22.88.14
hu0-5-0-4.ccr21.cle04.atlas.cogentco.com
be2717.ccr41.ord01.atlas.cogentco.com
be2765.ccr41.ord03.atlas.cogentco.com
att.ord03.atlas.cogentco.com
cgcil22crs.ip.att.net
n54ny21crs.ip.att.net
12.122.115.105
12.244.79.30
michigan.gov (23.78.200.73)

29.

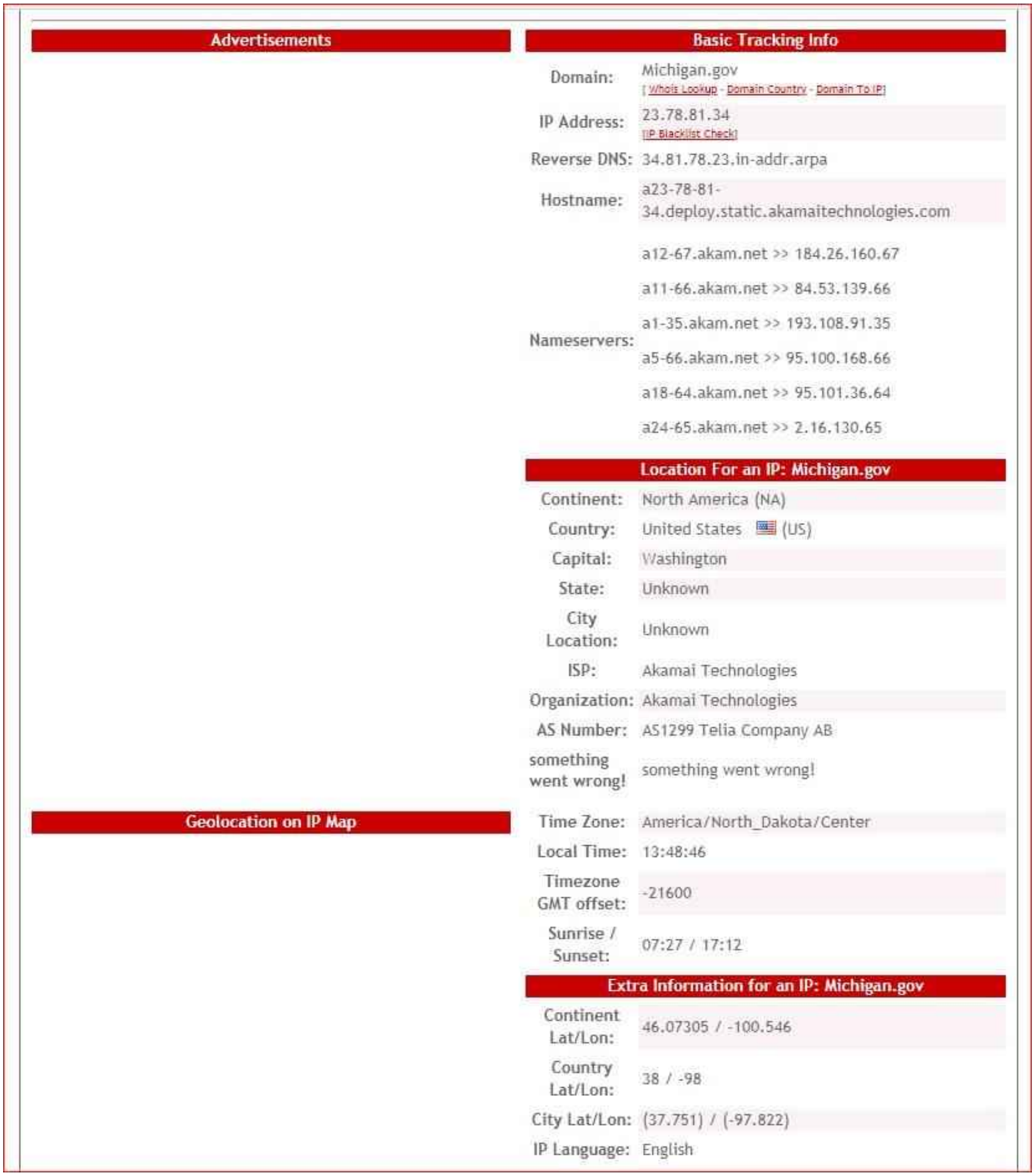

a23-78-81-34.deploy.static.akamaitechnologies.com (23.78.81.34)
mai-b1-link.telia.net
ash-bb2-link.telia.net
ash-b1-link.telia.net
63.218.218.42
63.218.218.33
ten0-0-0-21.br02.ash02.pccwbtn.net
localhost
Topology Legend
Hosts
○ host was not port scanned
● host with fewer than 3 open ports
● host with 3 to 6 open ports
● host with more than 6 open ports
🟩🟨🟥 host is a router, switch, or WAP
Traceroute connections
Thicker line means higher round-trip time
primary traceroute connection
alternate path
no traceroute information
missing traceroute hop
Additional host icons
router
switch
wireless access point
firewall
host with some filtered ports
View full legend online

30.

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

32. Michigan's government site is thumped off Akamai Technologies servers which are housed on **TELIA AB** a foreign server located in Germany.

33. Scytl, who is contracted with AP that receives the results tallied BY Scytl on behalf of Dominion – During the elections the AP reporting site had a disclaimer.
AP – powered by SCYTL.



Advertisements

Basic Tracking Info

Domain:	Michigan.gov [Whois Lookup - Domain Country - Domain To IP]
IP Address:	23.78.81.34 [IP Blacklist Check]
Reverse DNS:	34.81.78.23.in-addr.arpa
Hostname:	a23-78-81-34.deploy.static.akamaitechnologies.com
Nameservers:	a12-67.akam.net >> 184.26.160.67 a11-66.akam.net >> 84.53.139.66 a1-35.akam.net >> 193.108.91.35 a5-66.akam.net >> 95.100.168.66 a18-64.akam.net >> 95.101.36.64 a24-65.akam.net >> 2.16.130.65

Location For an IP: Michigan.gov

Continent:	North America (NA)
Country:	United States (US)
Capital:	Washington
State:	Unknown
City Location:	Unknown
ISP:	Akamai Technologies
Organization:	Akamai Technologies
AS Number:	AS1299 Telia Company AB
something went wrong!	something went wrong!

Geolocation on IP Map

Time Zone:	America/North_Dakota/Center
Local Time:	13:48:46
Timezone GMT offset:	-21600
Sunrise / Sunset:	07:27 / 17:12

Extra Information for an IP: Michigan.gov

Continent Lat/Lon:	46.07305 / -100.546
Country Lat/Lon:	38 / -98
City Lat/Lon:	(37.751) / (-97.822)
IP Language:	English

34. “Scytl was selected by the Federal Voting Assistance Program of the U.S. Department of Defense to provide a secure online ballot delivery and onscreen marking systems under a program to support overseas military and civilian voters for the 2010 election cycle and beyond. Scytl was awarded 9 of the 20 States that agreed to participate in the program (New York, Washington, Missouri, Nebraska, Kansas, New Mexico, South Carolina, Mississippi and Indiana), making it the provider with the highest number of participating States.” PDF

35. According to DOMINION : 1.4.1Software and Firmware The software and firmware employed by Dominion D-Suite 5.5-Aconsists of 2 types, custom and commercial off the shelf (COTS). COTS applications were verified to be pristine or were subjected to source code review for analysis of any modifications and verification of meeting the pertinent standards.

36. The concern is the HARDWARE and the NON – ACCREDITED VSTLs as by their own admittance use COTS.

37. The purpose of VSTL’s being accredited and their importance in ensuring that there is no foreign interference/ bad actors accessing the tally data via backdoors in equipment software. The core software used by ALL SCYTL related Election Machine/Software manufacturers ensures “anonymity” .

38. Algorithms within the area of this “shuffling” to maintain anonymity allows for setting values to achieve a desired goal under the guise of “encryption” in the trap-door.

39. The actual use of trapdoor commitments in Bayer-Groth proofs demonstrate the implications for the verifiability factor. This means that no one can SEE what is going on during the process of the “shuffling” therefore even if you deploy an algorithms or manual scripts to fractionalize or distribute pooled votes to achieve the outcome you wish – you cannot prove they are doing it! See STUDY : “The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system”

40. **Key Terms**

41. **UNIVERSAL VERIFIABILITY**: Votes cast are the votes counted and integrity of the vote is verifiable (the vote was tallied for the candidate selected) . **SCYTL FAILS UNIVERSAL VERIFIABILITY** because no mathematical proofs can determine if any votes have been manipulated.

42. **INDIVIDUAL VERIFIABILITY**: Voter cannot verify if their ballot got correctly counted. Like, if they cast a vote for ABC they want to verify it was ABC. That notion clearly discounts the need for anonymity in the first place.

43. To understand what I observed during the 2020 I will walk you through the process of one ballot cast by a voter.

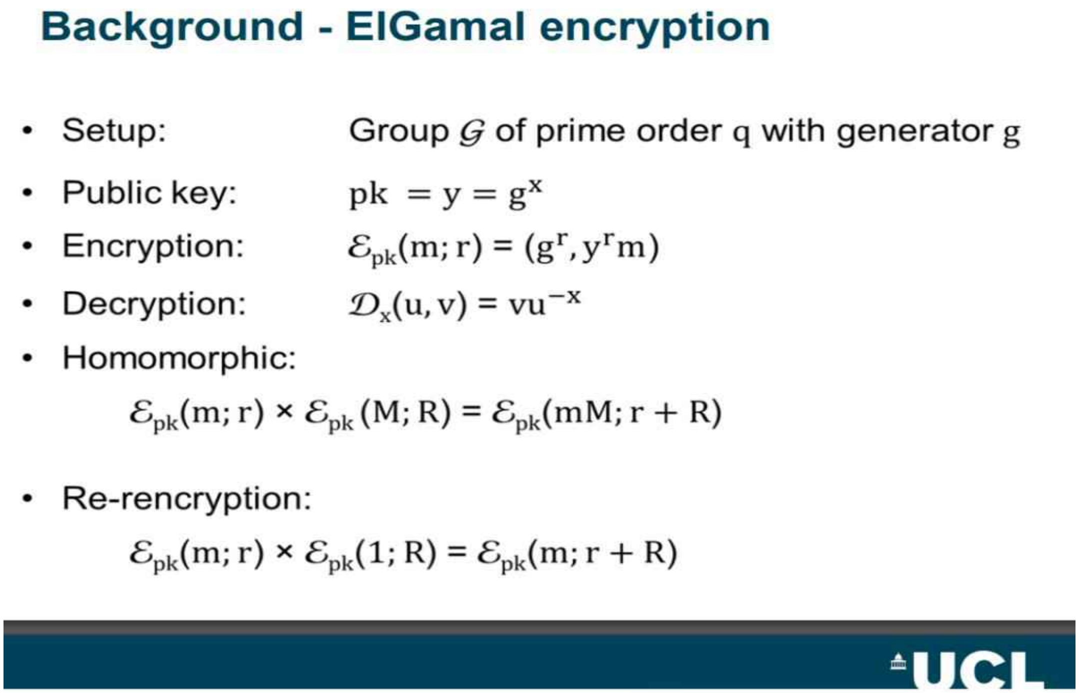
44. STEP 1 |Config Data | All non e-voting data is sent to Scytl (offshore) for configuration of data. All e-voting is sent to CONFIGURATION OF DATA then back to the e-voting machine and then to the next phase called CLEANSING. **CONCERNS**: Here we see an "OR PROOF" as coined by mathematicians – an "or proof" is that votes that have been pre-tallied parked in the system and the algorithm then goes back to set the outcome it is set for and seeks to make adjustments if there is a partial pivot present causing it to fail demanding manual changes such as block allocation and narrowing of parameters or self-adjusts to ensure the predetermined outcome is achieved.

45. STEP 2|CLEANSING | The Process is when all the votes come in from the software run by Dominion and get "cleansed" and put into 2 categories: invalid votes and valid votes.

46. STEP 3|Shuffling /Mixing | This step is the most nefarious and exactly where the issues arise and carry over into the decryption phase. Simply put, the software takes all the votes, literally mixes them a and then re-encrypts them. This is where if ONE had the commitment key- TRAPDOOR KEY – one would be able to see the parameters of the algorithm deployed as the votes go into this mixing phase, and how algorithm redistributes the votes.

47. This published PAPER FROM University College London depicts how this shuffle works. In essence, when this mixing/shuffling occurs, then one doesn't have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes when mixed.

48.



Background - ElGamal encryption

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

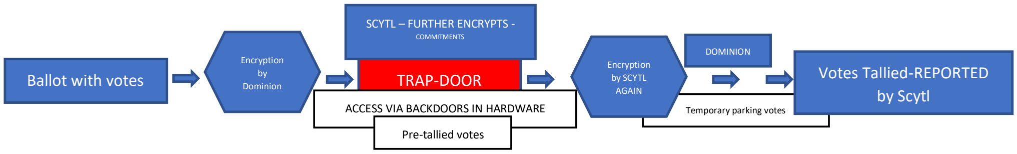
$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(M; R) = \mathcal{E}_{pk}(mM; r + R)$$

- Re-rencryption:

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

49. When this mixing/shuffling occurs, then one doesn't have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes.

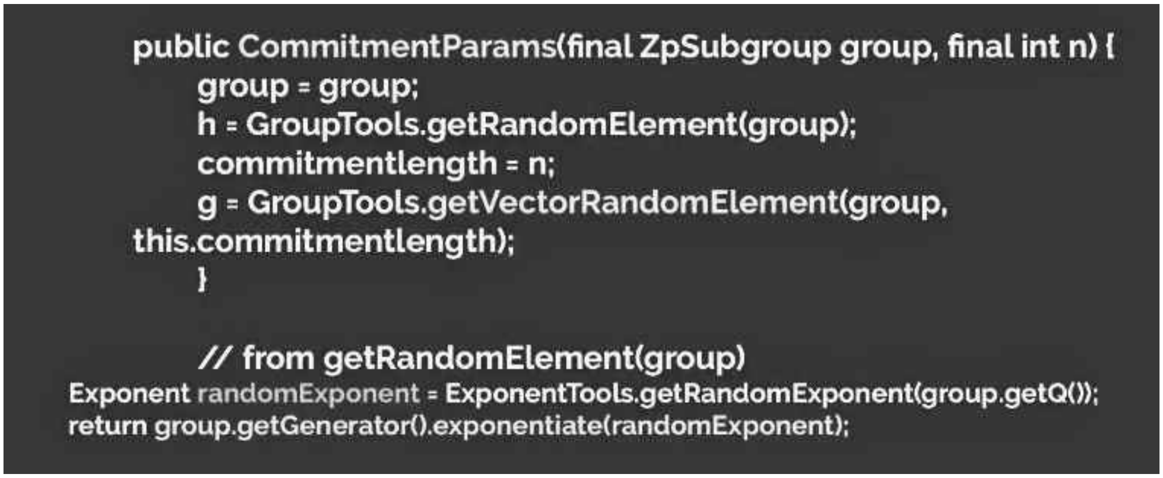
50. When the votes are sent to Scytl via Dominion Software EMS (Election Management System) the Trap Door is accessed by Scytl or TRAP DOOR keys (Commitment Parameters).

51. 
Ballot with votes
Encryption by Dominion
SCYTL – FURTHER ENCRYPTS - COMMITMENTS
TRAP-DOOR
ACCESS VIA BACKDOORS IN HARDWARE
Pre-tallied votes
Encryption by SCYTL AGAIN
DOMINION
Temporary parking votes
Votes Tallied-REPORTED by Scytl

52. The encrypted data is shifted into Scytl's platform in the form of ciphertexts – this means it is encrypted and a key based on commitments is needed to read the data. The ballot data can only be read if the person has a key that is set on commitments.

53. A false sense of security is provided to both parties that votes are not being "REPLACED" during the mixing phase. Basically, Scytl re-encrypts the ballot data that comes in from Dominion (or any other voting software company) as ciphertexts. Scytl is supposed to prove that votes A, B, C are indeed X, Y, Z under their new re-encryption when sending back the votes that are tallied coding them respectively. This is done by Scytl and the Election Software company that agrees to certain

“Generators” and therefore together build “commitments.”

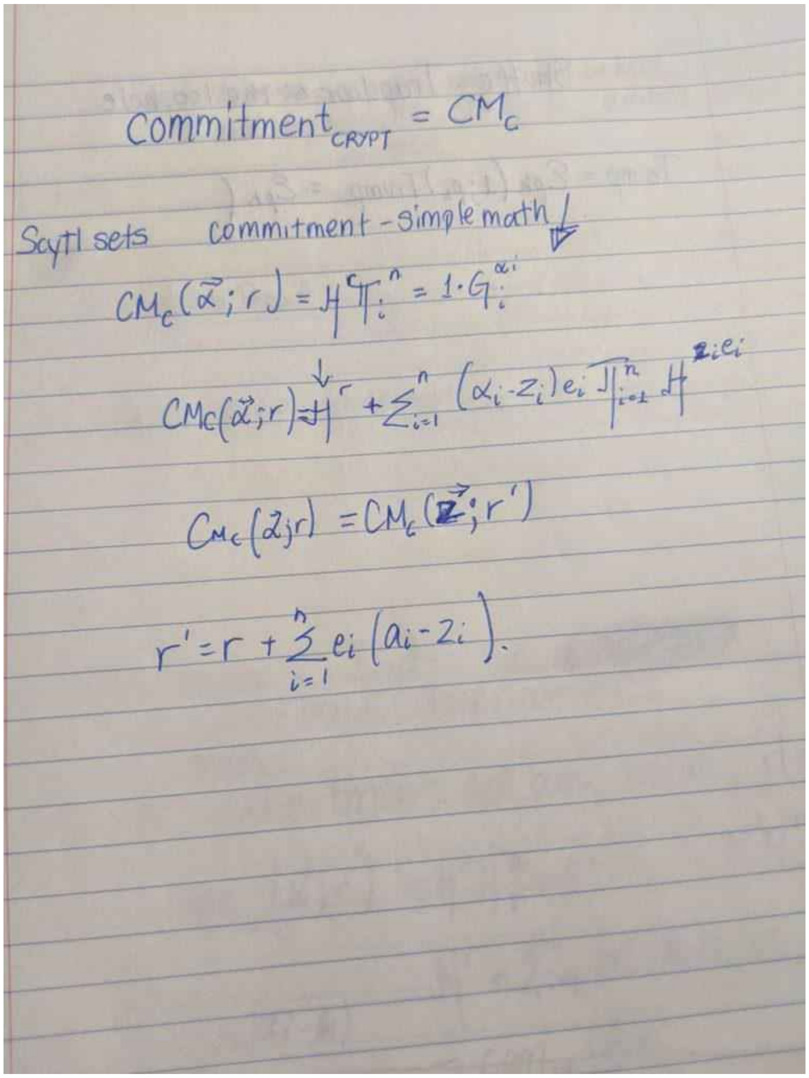


```
        public CommitmentParams(final ZpSubgroup group, final int n) {
            group = group;
            h = GroupTools.getRandomElement(group);
            commitmentlength = n;
            g = GroupTools.getVectorRandomElement(group,
        this.commitmentlength);
            }

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

54. Scytl and Dominion have an agreement – only the two would know the parameters. This means that access is able to occur through backdoors in hardware if the parameters of the commitments are known in order to alter the range of the algorithm deployed to satisfy the outcome sought in the case of algorithm failure.

55. Trapdoor is a cryptotech term that describes a state of a program that knows the commitment parameters and therefore is able change the value of the commitments however it likes. In other words, Scytl or anyone that knows the commitment parameters can take all the votes and give them to any one they want. If they have a total of 1000 votes an algorithm can distribute them among all races as it deems necessary to achieve the goals it wants. (Case Study: Estonia)

56. 

Commitment$_{CRYPT}$ $= CM_c$

Scytl sets commitment - simple math ↓

$$CM_c(\vec{\alpha}; r) = H^{c} \prod_i^{n} = 1 \cdot G_i^{\alpha_i}$$

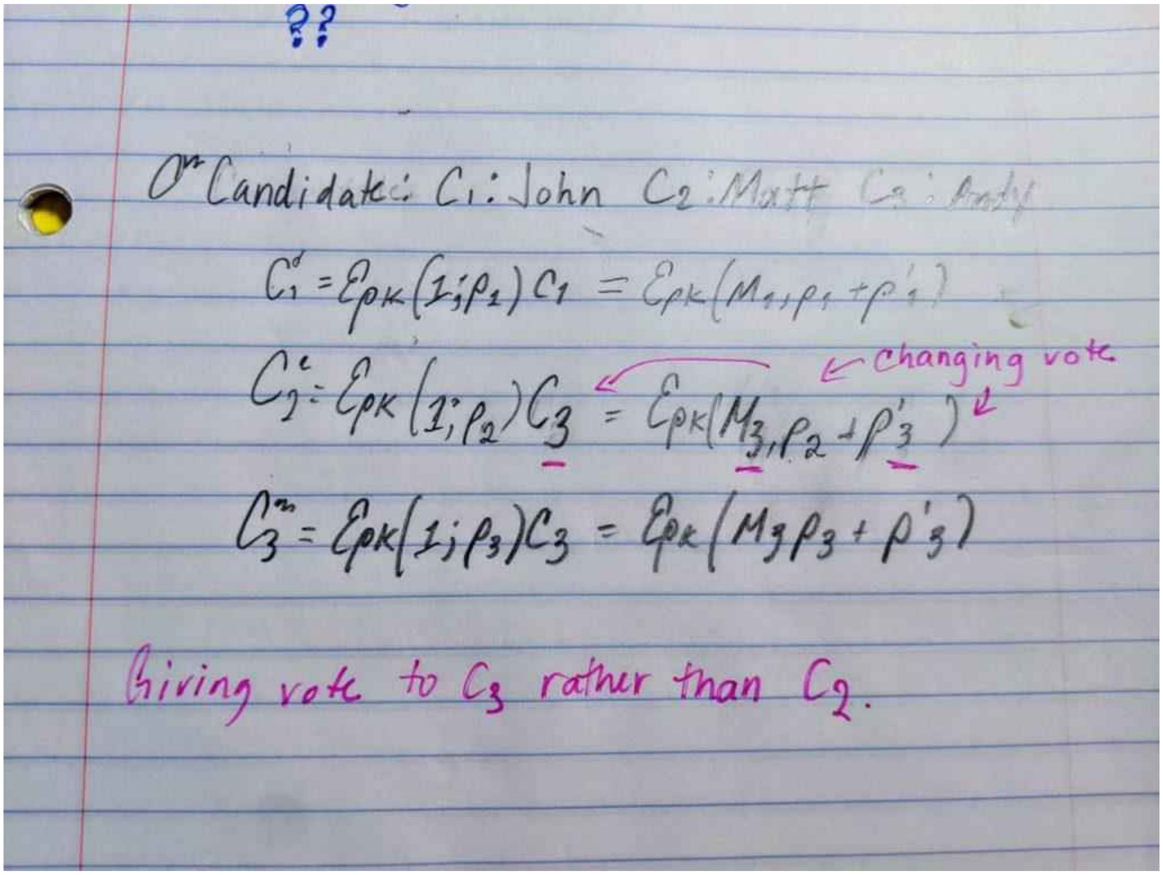
$$CM_c(\vec{\alpha}; r) = \overset{\downarrow}{H}^{r} + \sum_{i=1}^{n} (\alpha_i - z_i) e_i \prod_{i=1}^{n} H^{z_i e_i}$$

$$CM_c(\alpha; r) = CM_c(\vec{z}; r')$$

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

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

"reallocate" votes via an algorithm to achieve the goal set.



??

Or Candidate: C_1: John C_2: Matt C_3: Andy

$$C_1^d = \mathcal{E}_{pk}(1;\rho_1)\,C_1 = \mathcal{E}_{pk}(M_1,\rho_1+\rho'_1)$$

$$C_2^c = \mathcal{E}_{pk}(1;\rho_2)\,C_{\underline{3}} = \mathcal{E}_{pk}(M_{\underline{3}},\rho_2+\rho'_{\underline{3}})$$

← changing vote

$$C_3^m = \mathcal{E}_{pk}(1;\rho_3)\,C_3 = \mathcal{E}_{pk}(M_3\,\rho_3+\rho'_3)$$

Giving vote to C_3 rather than C_2.

58. STEP 4|Decryption would be the decryption phase and temporary parking of vote tallies before reporting. In this final phase before public release the tallies are released from encrypted format into plain text. As previously explained, those that know the trapdoor can easily change any votes that the randomness is applied and used to generate the tally vote ciphertext. Thus in this case, Scytl who is the mixer can collude with their vote company clients or an agency (-------) to change votes and get away with it. This is because the receiver doesn't have the decryption key so they rely solely on Scytl to be ***honest*** or free from any foreign actors within their backdoor or the Election Company (like Dominion) that can have access to the key.

59. In fact, a study from the University of Bristol made claim that interference can be seen when there is a GREAT DELAY in reporting and finalizing numbers University of Bristol : How not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios

60. "Zero-knowledge proofs of knowledge allow a prover to convince a verifier that she holds information satisfying some desirable properties without revealing anything else." David Bernhard, Olivier Pereira,and Bogdan Warinschi.

61. Hence, you can't prove anyone manipulated anything. The TRAP DOOR KEY HOLDERS can offer you enough to verify to you what you need to see without revealing anything and once again indicating the inability to detect manipulation. **ZERO PROOF of INTEGRITY OF THE VOTE.**

62. Therefore, if decryption is challenged, the administrator or software company that knows the trap door key can provide you proof that would be able to pass verification (blind). This was proven to be factually true in the case study by The University of Melbourne in March. White Hat Hackers purposely altered votes by knowing the parameters set in the commitments and there was no way to prove they did it – or any way to prove they didn't.

63. IT'S THE PERFECT THREE CARD MONTY. That's just how perfect it is. They fake a proof of ciphertexts with KNOWN "RANDOMNESS" .This rolls back to the integrity of the VOTE. The vote is not safe using these machines not only because of the method used for ballot "cleansing" to maintain anonymity but the EXPOSURE to foreign interference and possible domestic bad actors.

64. In many circumstances, manipulation of the algorithm is NOT possible in an undetectable fashion. This is because it is one point heavy. Observing the elections in 2020 confirm the deployment of an algorithm due to the BEHAVIOR which is indicative of an algorithm in play that had no pivoting parameters applied.

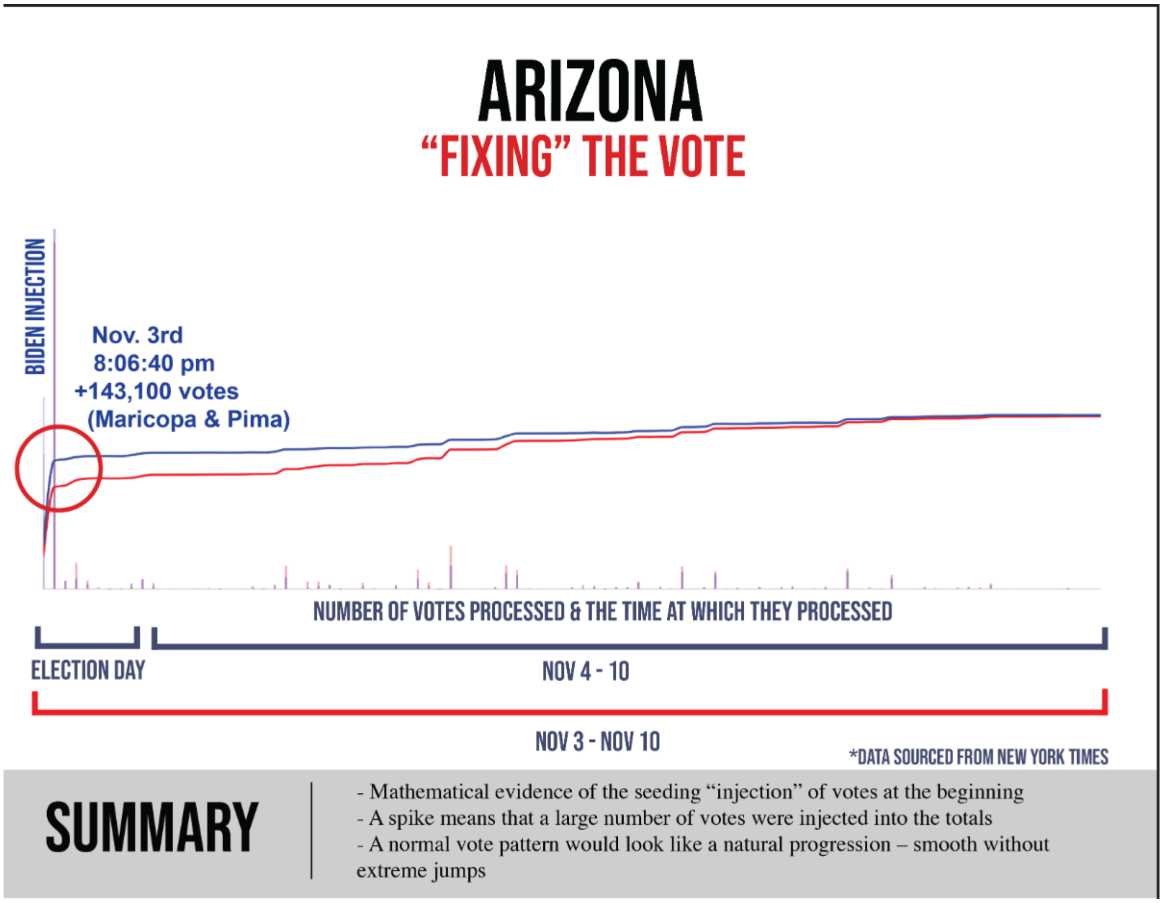
65. The behavior of the algorithm is that one point (B) is the greatest point within the allocated set. It is the greatest number within the A B points given. Point A would be the smallest. Any points outside the A B points are not necessarily factored in yet can still be applied.

66. The points outside the parameters can be utilized to a certain to degree such as in block allocation.

67. The algorithm geographically changed the parameters of the algorithm to force blue votes and ostracize red.

68. Post block allocation of votes the two points of the algorithm were narrowed ensuring a BIDEN win hence the observation of NO Trump Votes and some BIDEN votes for a period of time.

69.



ARIZONA

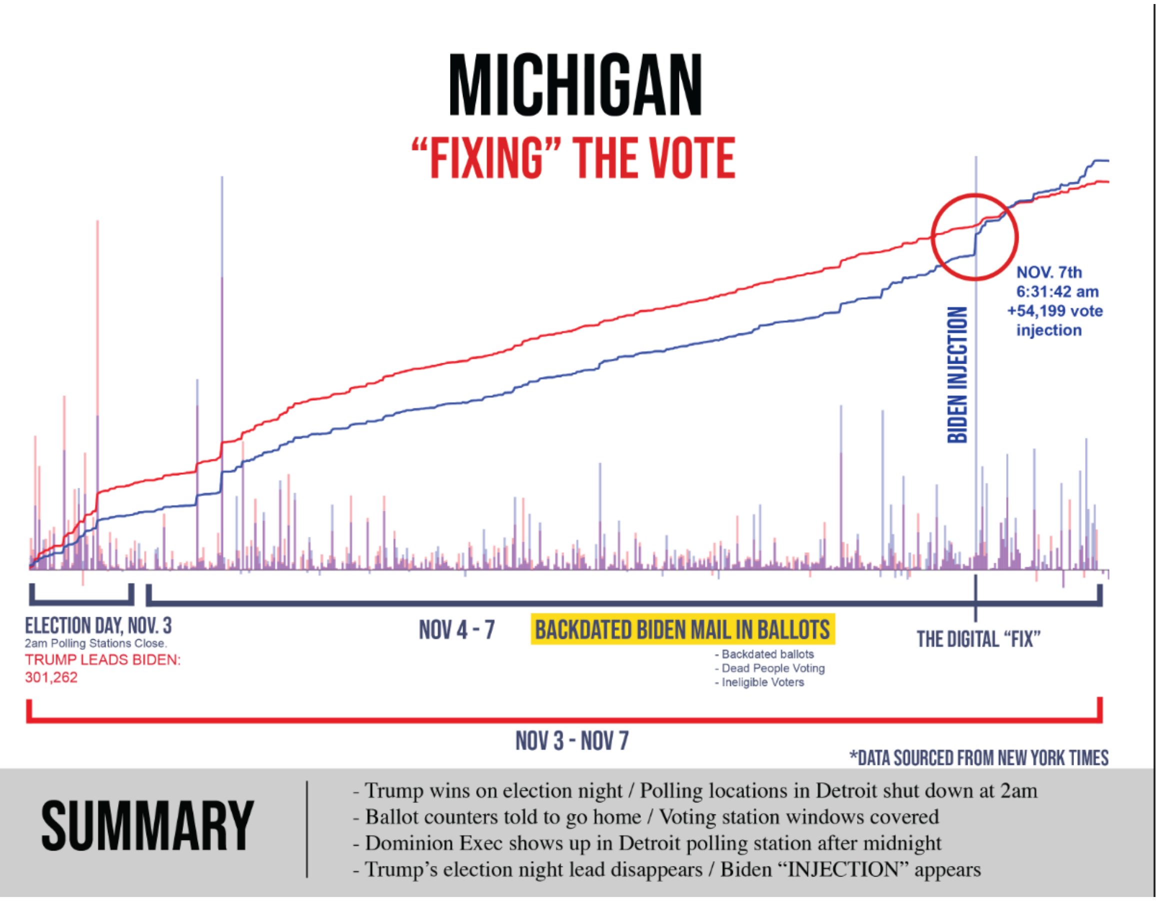
“FIXING” THE VOTE

*DATA SOURCED FROM NEW YORK TIMES

SUMMARY

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

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



MICHIGAN

“FIXING” THE VOTE

SUMMARY

- Trump wins on election night / Polling locations in Detroit shut down at 2am
- Ballot counters told to go home / Voting station windows covered
- Dominion Exec shows up in Detroit polling station after midnight
- Trump’s election night lead disappears / Biden “INJECTION” appears

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

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

72.

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

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

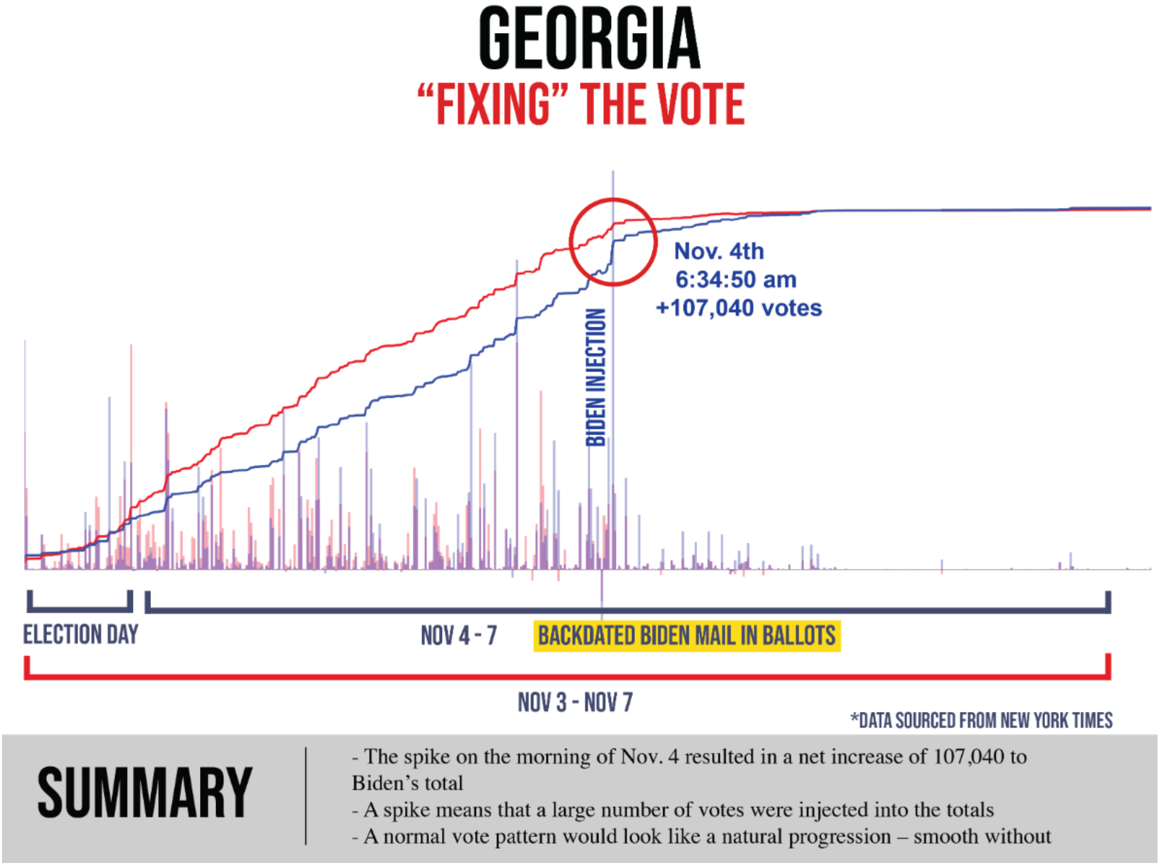
ballots being fed or THUMB DRIVES. The algorithm block adjusted itself and the PEOPLE were creating the evidence to BACK UP the block allocation.

75. I have witnessed the same behavior of the election software in countries outside of the United States and within the United States. In -------, the elections conducted behaved in the same manner by allocating BLOCK votes to the candidate "chosen" to win.

76. Observing the data of the contested states (and others) the algorithm deployed is identical to that which was deployed in 2012 providing Barack Hussein Obama a block allocation to win the 2012 Presidential Elections.

77. The algorithm looks to have been set to give Joe Biden a 52% win even with an initial 50K+ vote block allocation was provided initially as tallying began (as in case of Arizona too). In the am of November 4, 2020 the algorithm stopped working, therefore another "block allocation" to remedy the failure of the algorithm. This was done manually as ALL the SYSTEMS shut down NATIONWIDE to avoid detection.

78.

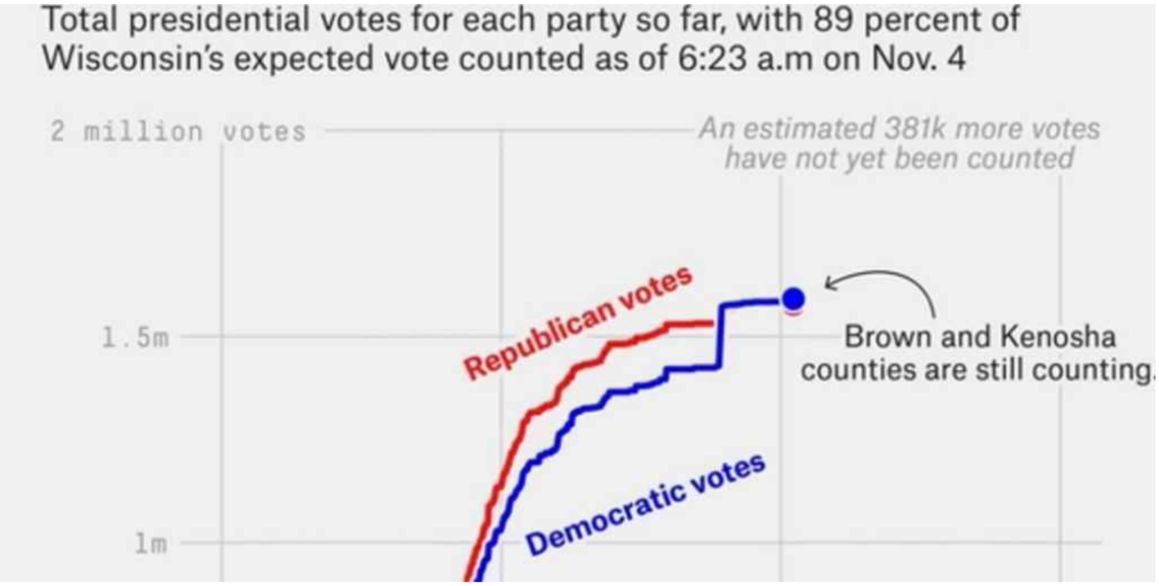


- The spike on the morning of Nov. 4 resulted in a net increase of 107,040 to Biden's total
- A spike means that a large number of votes were injected into the totals
- A normal vote pattern would look like a natural progression – smooth without

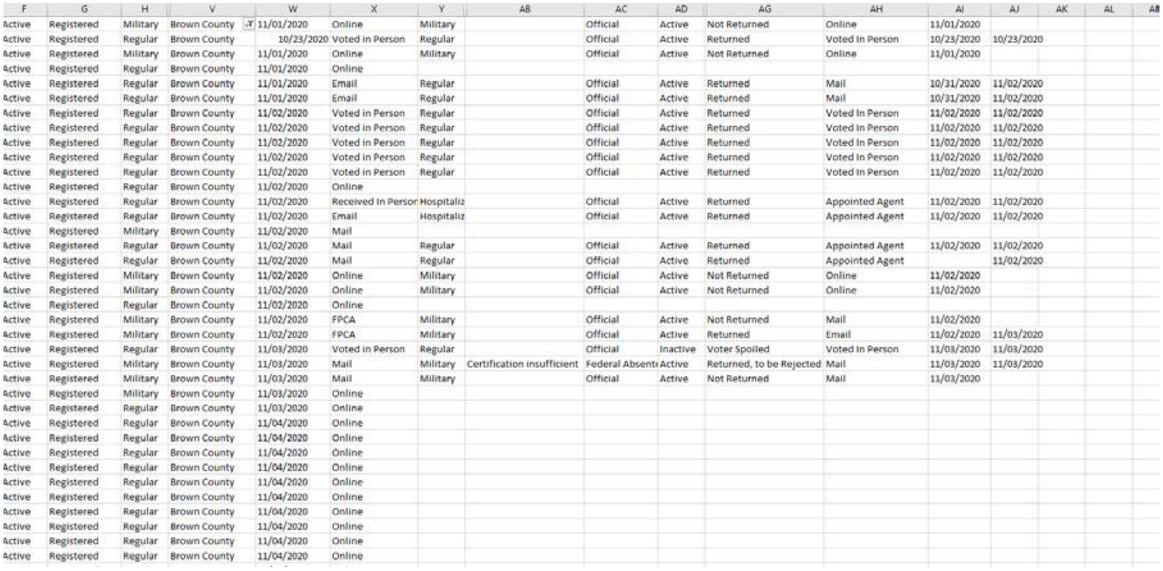
79. In Georgia during the 2016 Presidential Elections a failed attempt to deploy the scripts to block allocate votes from a centralized location where the "trap-door" key lay an attempt by someone using

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

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

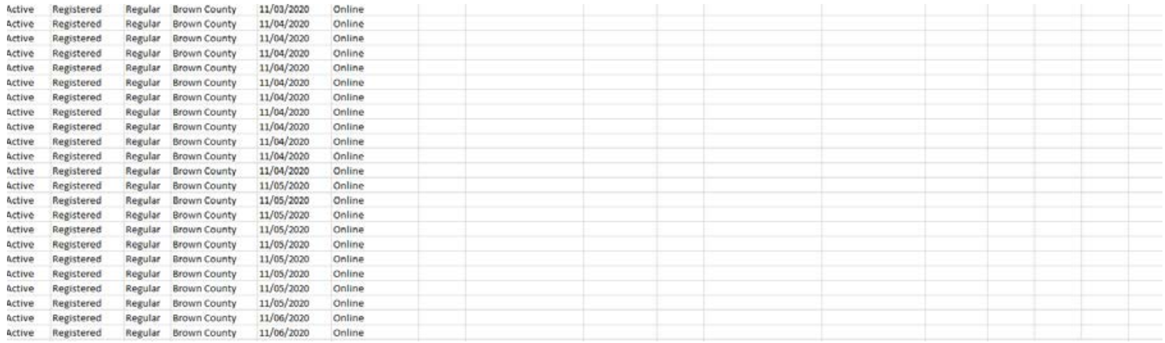
81. 

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

83. 

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

84.



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

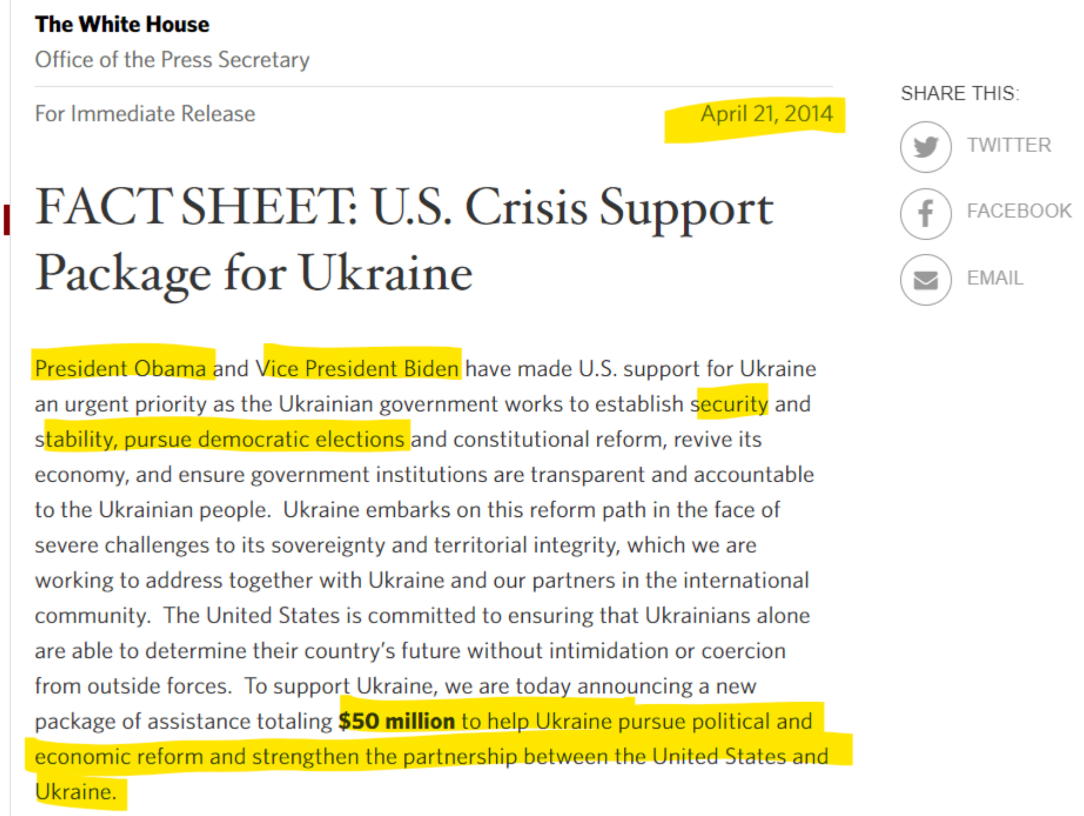
85. I can personally attest that in 2013 discussions by the Obama / Biden administration were being had with various agencies in the deployment of such election software to be deployed in ----- in 2013.

86. On or about April 2013 a one year plan was set to fund and usher elections in -----.

87. Joe Biden was designated by Barack Hussein Obama to ensure the ----- accepted assistance.

88. John Owen Brennan and James (Jim) Clapper were responsible for the ushering of the intelligence surrounding the elections in -----.

89. Under the guise of Crisis support the US Federal Tax Payers funded the deployment of the election software and machines in ------ signing on with Scytl.



The White House

Office of the Press Secretary

For Immediate Release April 21, 2014

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

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

90.

91. Right before the ----- elections it was alleged that CyberBerkut a pro-Russia group infiltrated --- central election computers and **deleted key files**. These actions supposedly rendered the vote-tallying system inoperable.

92. In fact, the KEY FILES were the Commitment keys to allow Scytl to tally the votes rather than the election machines. The group had disclosed emails and other documents proving that their election was rigged and that they tried to avoid a fixed election.

93. The elections were held on May 25, 2014 but in the early AM hours the election results were BLOCKED and the final tally was DELAYED flipping the election in favor of -----.

94. The claim was that there was a DDoS attack by Russians when in actual fact it was a mitigation of the algorithm to inject block votes as we observed was done for Joe Biden because the KEYS were unable to be deployed. In the case of -----, the trap-door key was "altered"/deleted/ rendered ineffective. In the case of the US elections, representatives of Dominion/ ES&S/ Smartmatic/ Hart Intercivic would have to manually deploy them since if the entry points into the systems seemed to have failed.

95. The vote tallying of all states NATIONWIDE stalled and hung for days – as in the case of Alaska that has about 300K registered voters but was stuck at 56% reporting for almost a week.

96. This "hanging" indicates a failed deployment of the scripts to block allocate remotely from one location as observed in ------ on May 26, 2014.

97. This would justify the presence of the election machine software representatives making physical appearances in the states where the election results are currently being contested.

98. A Dominion Executive appeared at the polling center in Detroit after midnight.

99. Considering that the hardware of the machines has NOT been examined in Michigan since 2017 by Pro V& V according to Michigan's own reporting. COTS are an avenue that hackers and bad actors seek to penetrate in order to control operations. Their software updates are the reason vulnerabilities to foreign interference in all operations exist.

100. The importance of VSTLs in underrated to protect up from foreign interference by way of open access via COTS software. Pro V& V who's EAC certification EXPIRED on 24 FEB 2017 was contracted with the state of WISCONSIN.

101. In the United States each state is tasked to conduct and IV& V (Independent Verification and Validation) to provide assurance of the integrity of the votes.

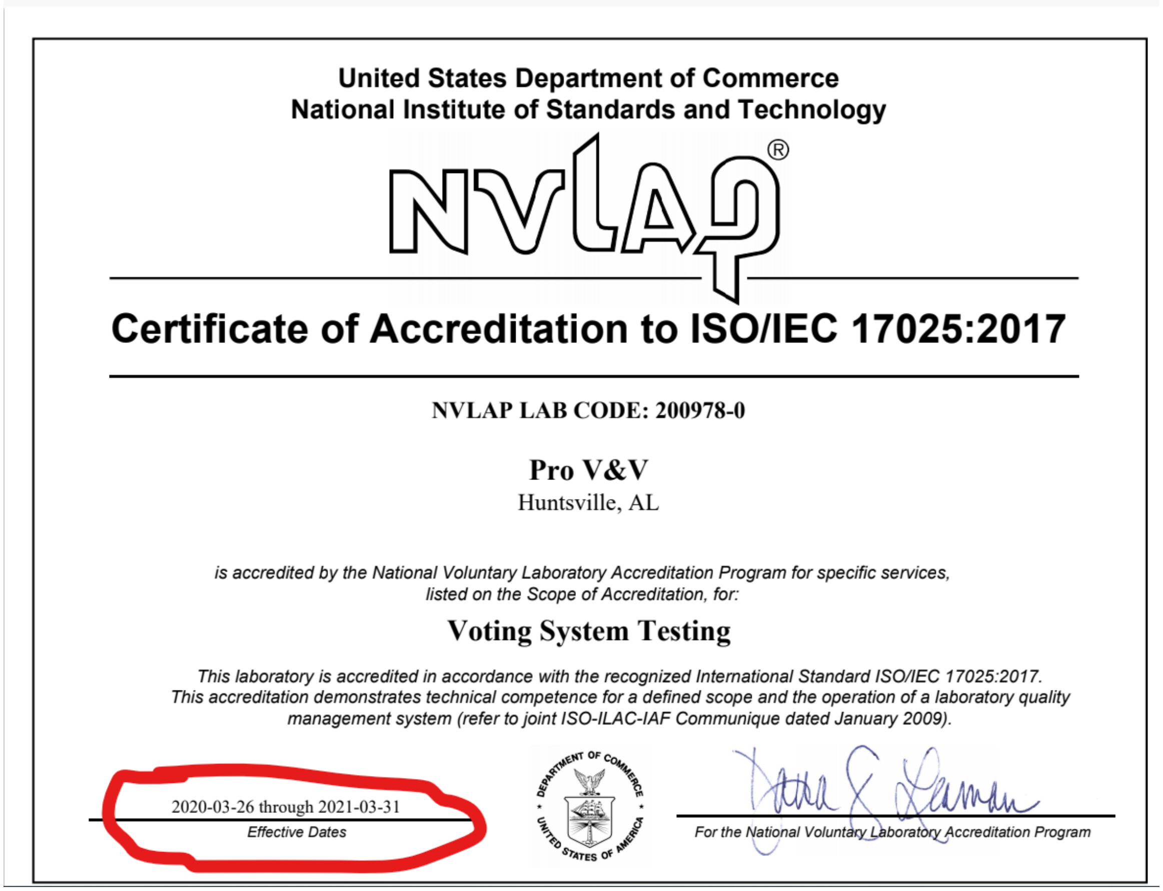
102. If the "accredited" non-federal entities have NOT received EAC accreditation this is a failure of the states to uphold their own states standards that are federally regulated.

103. In addition, if the entities had NIST certificates they are NOT sufficing according the HAVA ACT 2002 as the role of NIST is clear.

104. Curiously, both companies PRO V&V and SLI GAMING received NIST certifications OUTSIDE the 24 month scope.

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

106.



United States Department of Commerce
National Institute of Standards and Technology

NVLAP®

Certificate of Accreditation to ISO/IEC 17025:2017

NVLAP LAB CODE: 200978-0

Pro V&V
Huntsville, AL

is accredited by the National Voluntary Laboratory Accreditation Program for specific services, listed on the Scope of Accreditation, for:

Voting System Testing

This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2017. This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality management system (refer to joint ISO-ILAC-IAF Communique dated January 2009).

2020-03-26 through 2021-03-31
Effective Dates

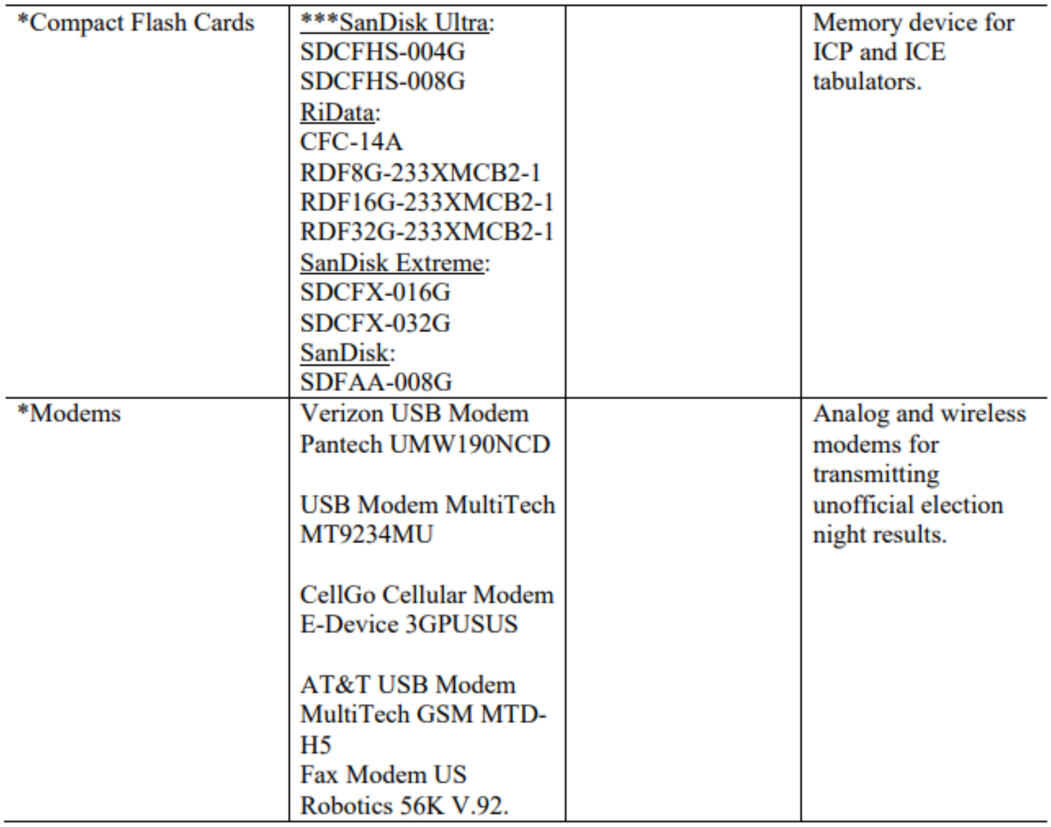
DEPARTMENT OF COMMERCE * UNITED STATES OF AMERICA

For the National Voluntary Laboratory Accreditation Program

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

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

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



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

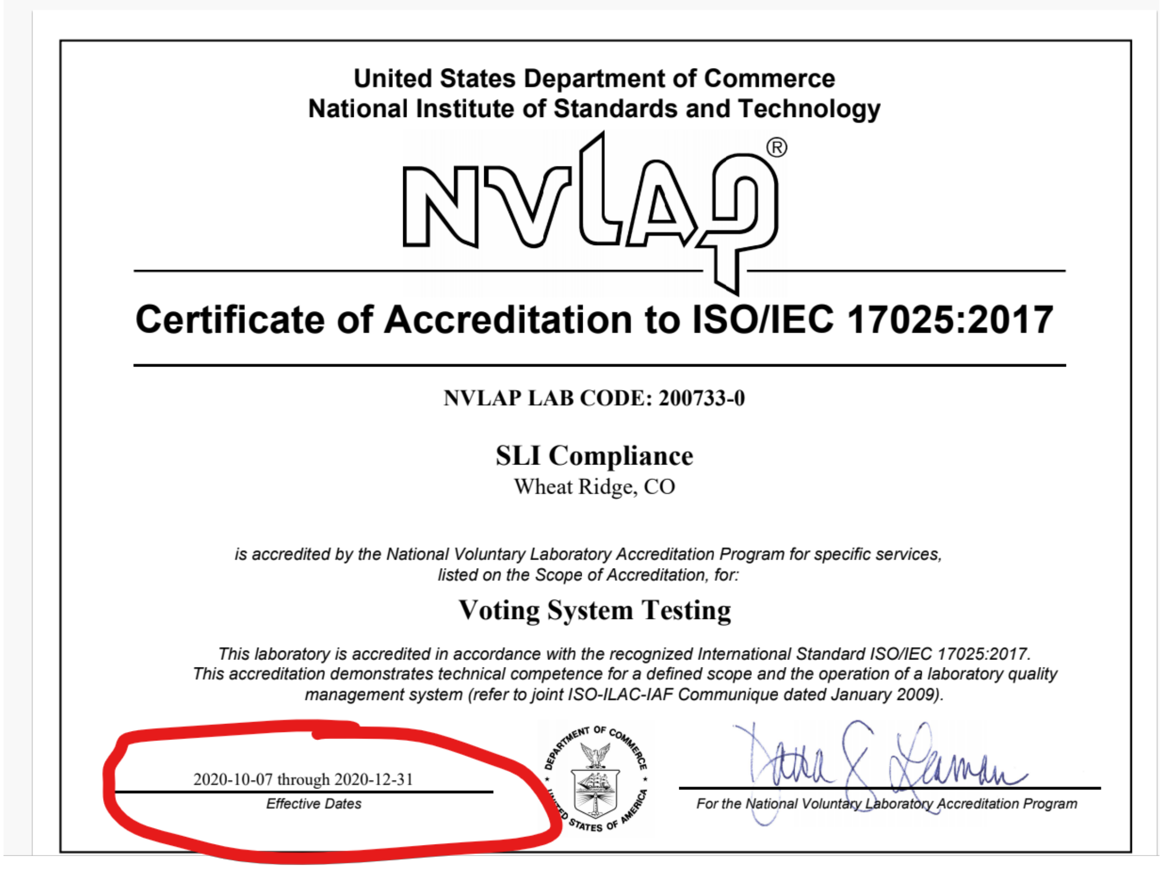
110.

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

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

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

114.



United States Department of Commerce
National Institute of Standards and Technology

NVLAP®

Certificate of Accreditation to ISO/IEC 17025:2017

NVLAP LAB CODE: 200733-0

SLI Compliance
Wheat Ridge, CO

is accredited by the National Voluntary Laboratory Accreditation Program for specific services, listed on the Scope of Accreditation, for:

Voting System Testing

This laboratory is accredited in accordance with the recognized International Standard ISO/IEC 17025:2017. This accreditation demonstrates technical competence for a defined scope and the operation of a laboratory quality management system (refer to joint ISO-ILAC-IAF Communique dated January 2009).

2020-10-07 through 2020-12-31
Effective Dates

DEPARTMENT OF COMMERCE · UNITED STATES OF AMERICA

Dana S Leaman
For the National Voluntary Laboratory Accreditation Program

115. In fact SLI was NIST ISO Certified for less than 90 days.

116. I can personally attest that high-level officials of the Obama/Biden administration and large private contracting firms met with a software company called GEMS which is ultimately the software ALL election machines run now running under the flag of DOMINION.

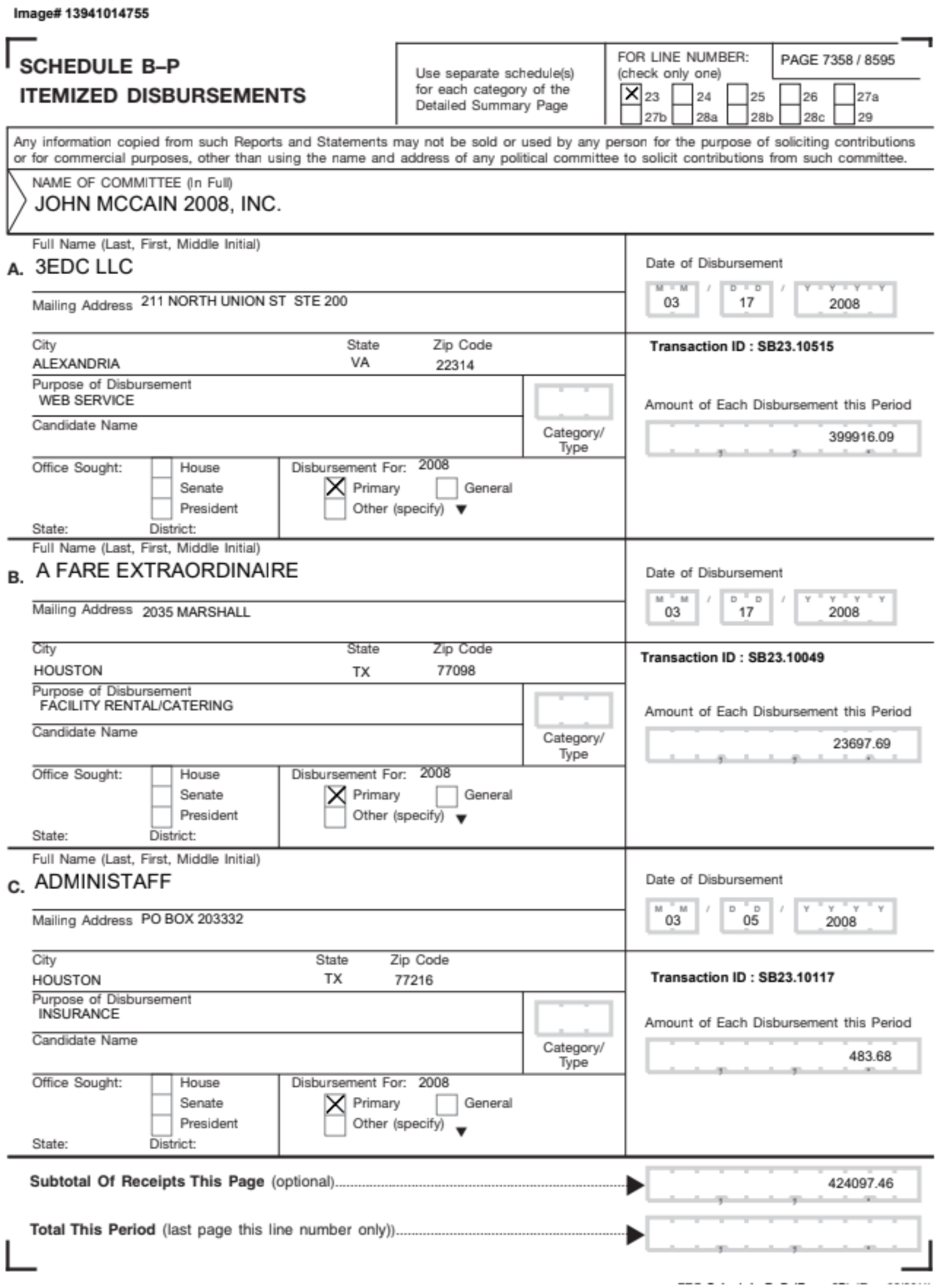
117. GEMS was manifested from SOE software purchased by SCYTL developers and US Federally Funded persons to develop it.

118. The only way GEMS can be deployed across ALL machines is IF all counties across the nation are housed under the same server networks.

119. GEMS was tasked in 2009 to a contractor in Tampa, Fl.

120. GEMS was also fine-tuned in Latvia, Belarus, Serbia and Spain to be localized for EU deployment as observed during the Swissport election debacle.

121. John McCain's campaign assisted in FUNDING the development of GEMS web monitoring via WEB Services with 3EDC and Dynology.



Image# 13941014755

SCHEDULE B-P
ITEMIZED DISBURSEMENTS

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

FOR LINE NUMBER: (check only one)
☒ 23 □ 24 □ 25 □ 26 □ 27a
□ 27b □ 28a □ 28b □ 28c □ 29

PAGE 7358 / 8595

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

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

A. Full Name (Last, First, Middle Initial): 3EDC LLC
Mailing Address: 211 NORTH UNION ST STE 200
City: ALEXANDRIA State: VA Zip Code: 22314
Purpose of Disbursement: WEB SERVICE
Candidate Name:
Category/Type:
Office Sought: □ House □ Senate □ President
State: District:
Disbursement For: 2008 ☒ Primary □ General □ Other (specify) ▼
Date of Disbursement: 03 / 17 / 2008
Transaction ID : SB23.10515
Amount of Each Disbursement this Period: 399916.09

B. Full Name (Last, First, Middle Initial): A FARE EXTRAORDINAIRE
Mailing Address: 2035 MARSHALL
City: HOUSTON State: TX Zip Code: 77098
Purpose of Disbursement: FACILITY RENTAL/CATERING
Candidate Name:
Category/Type:
Office Sought: □ House □ Senate □ President
State: District:
Disbursement For: 2008 ☒ Primary □ General □ Other (specify) ▼
Date of Disbursement: 03 / 17 / 2008
Transaction ID : SB23.10049
Amount of Each Disbursement this Period: 23697.69

C. Full Name (Last, First, Middle Initial): ADMINISTAFF
Mailing Address: PO BOX 203332
City: HOUSTON State: TX Zip Code: 77216
Purpose of Disbursement: INSURANCE
Candidate Name:
Category/Type:
Office Sought: □ House □ Senate □ President
State: District:
Disbursement For: 2008 ☒ Primary □ General □ Other (specify) ▼
Date of Disbursement: 03 / 05 / 2008
Transaction ID : SB23.10117
Amount of Each Disbursement this Period: 483.68

Subtotal Of Receipts This Page (optional) ▶ 424097.46

Total This Period (last page this line number only)) ▶

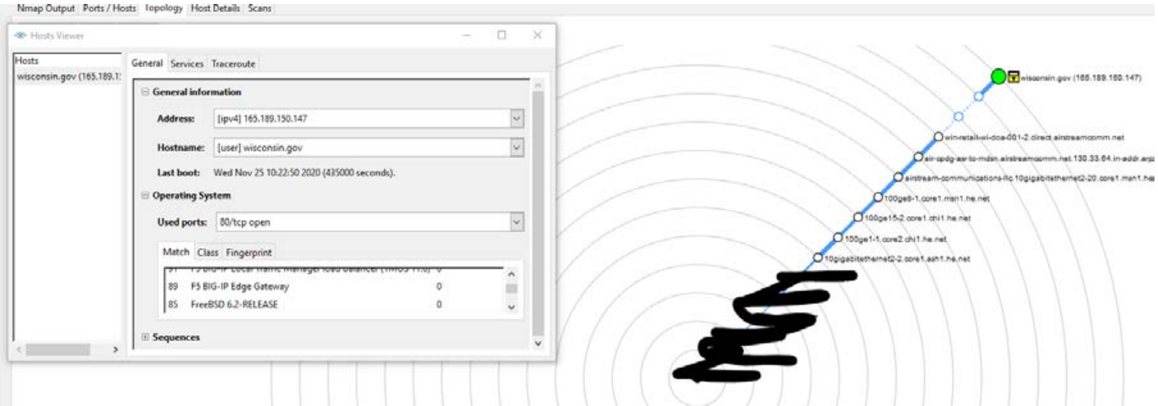
122.

123.

124. AKAMAI Technologies services SCYTL.

125. AKAMAI Technologies Houses ALL foreign government sites. (Please see White Paper by Akamai.)

126. AKAMAI Technologies houses ALL .gov state sites. (ref Item 123 Wisconsin.gov Example)


Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Hosts
wisconsin.gov (165.189.1:
General
Services
Traceroute
Match
Class
Fingerprint
wisconsin.gov (165.189.150.147)
win-retail-wi-doa-001-2.direct.airstreamcomm.net
air-cpdg-asr-to-mdsn.airstreamcomm.net.130.33.64.in-addr.arpa
airstream-communications-llc.10gigabitethernet2-20.core1.msn1.he
100ge8-1.core1.msn1.he.net
100ge15-2.core1.chi1.he.net
100ge1-1.core2.chi1.he.net
10gigabitethernet2-2.core1.ash1.he.net

General information

Address: [ipv4] 165.189.150.147

Hostname: [user] wisconsin.gov

Last boot: Wed Nov 25 10:22:50 2020 (435000 seconds).

Operating System

Used ports: 80/tcp open

```
89   F5 BIG-IP Edge Gateway   0
85   FreeBSD 6.2-RELEASE      0
```

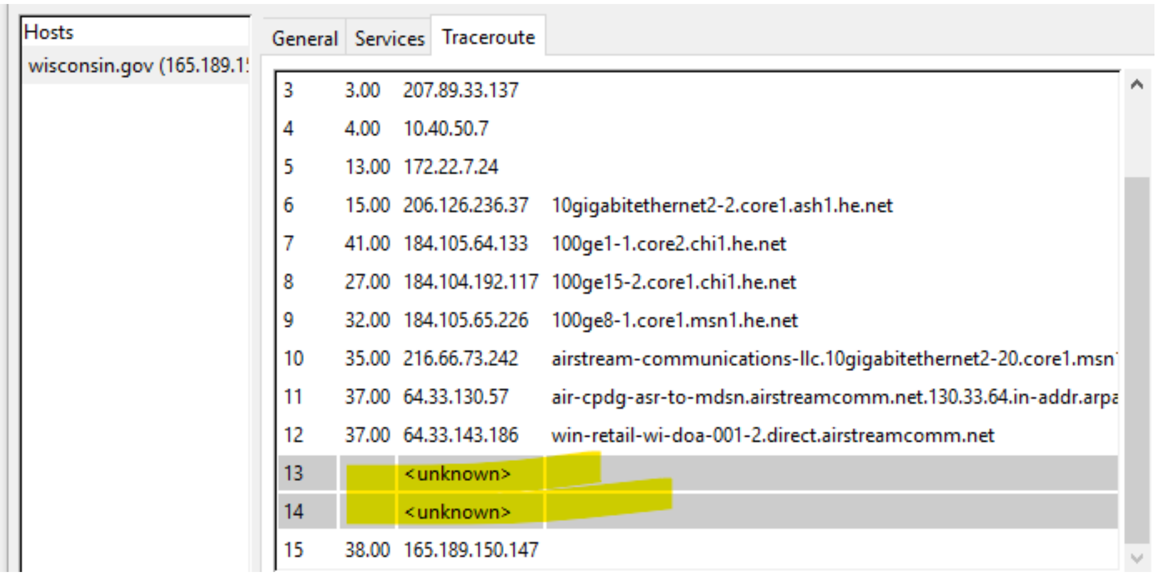
Sequences

[redacted]

127.

128. Wisconsin has EDGE GATEWAY port which is AKAMAI TECHNOLOGIES based out of GERMANY.

129. Using AKAMAI Technologies is allowing .gov sites to obfuscate and mask their systems by way of HURRICANE ELECTRIC (he.net) Kicking it to anonymous (AKAMAI Technologies) offshore servers.



```
3    3.00   207.89.33.137
4    4.00   10.40.50.7
5    13.00  172.22.7.24
6    15.00  206.126.236.37   10gigabitethernet2-2.core1.ash1.he.net
7    41.00  184.105.64.133   100ge1-1.core2.chi1.he.net
8    27.00  184.104.192.117  100ge15-2.core1.chi1.he.net
9    32.00  184.105.65.226   100ge8-1.core1.msn1.he.net
10   35.00  216.66.73.242    airstream-communications-llc.10gigabitethernet2-20.core1.msn
11   37.00  64.33.130.57     air-cpdg-asr-to-mdsn.airstreamcomm.net.130.33.64.in-addr.arpa
12   37.00  64.33.143.186    win-retail-wi-doa-001-2.direct.airstreamcomm.net
13          <unknown>
14          <unknown>
15   38.00  165.189.150.147
```

130.

131. AKAMAI Technologies has locations around the world.

132. AKAMAI Technologies has locations in China (ref item 22)

133. AKAMAI Technologies has locations in Iran as of 2019.

134. AKAMAI Technologies merged with UNICOM (CHINESE TELECOMM) in 2018.

135. AKAMAI Technologies house all state .gov information in GERMANY via TELIA AB.

136. In my professional opinion, this affidavit presents unambiguous evidence:

137. That there was Foreign interference, complicit behavior by the previous administrations from 1999 up until today to hinder the voice of the people and US persons knowingly and willingly colluding with foreign powers to steer our 2020 elections that can be named in a classified setting.

138. Foreign interference is present in the 2020 election in various means namely,

139. Foreign nationals assisted in the creation of GEMS (Dominion Software Foundation)

140. Akamai Technologies merged with a Chinese company that makes the COTS components of the election machines providing access to our electronic voting machines.

141. Foreign investments and interests in the creation of the GEMS software.

142. US persons holding an office and private individuals knowingly and willingly oversaw fail safes to secure our elections.

143. The EAC failed to abide by standards set in HAVA ACT 2002.

144. The IG of the EAC failed to address complaints since their appointment regarding vote integrity

145. Christy McCormick of the EAC failed to ensure that EAC conducted their duties as set forth by HAVA ACT 2002

146. Both Patricia Layfield (IG of EAC) and Christy McCormick (Chairwoman of EAC) were appointed by Barack Hussein Obama and have maintained their positions since then.

147. The EAC failed to have a quorum for over a calendar year leading to the inability to meet the standards of the EAC.

148. AKAMAI Technologies and Hurricane Electric raise serious concerns for NATSEC due to their ties with foreign hostile nations.

149. For all the reasons above a complete failure of duty to provide safe and just elections are observed.

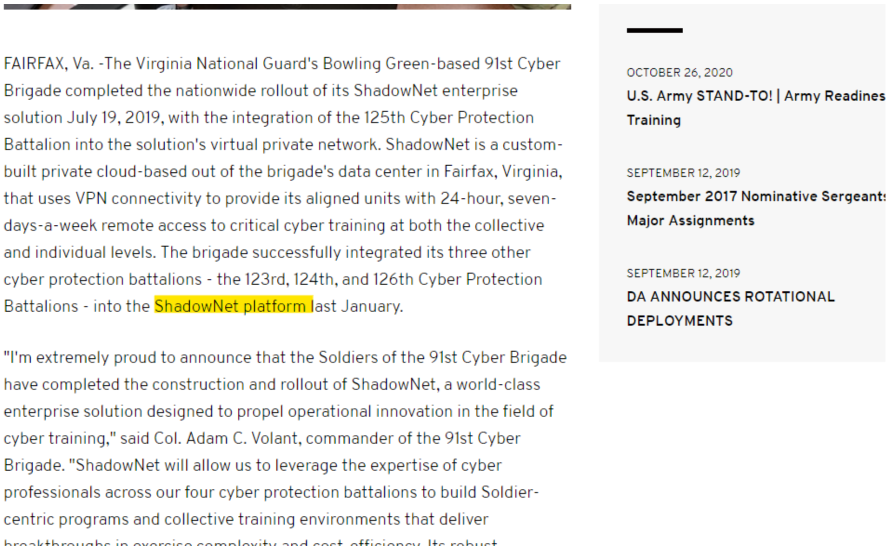
150. For the people of the United States to have confidence in their elections our cybersecurity standards should not be in the hands of foreign nations.

151. Those responsible within the Intelligence Community directly and indirectly by way of procurement of services should be held accountable for assisting in the development, implementation and promotion of GEMS.

152. GEMS ------- General Hayden.

153. In my opinion and from the data and events I have observed -------------------- with the assistance of SHADOWNET under the guise of L3-Communications which is MPRI. This is also confirmed by us.army.mil making the statement that shadownet has been deployed to 30 states which all

happen to be using Dominion Machines.



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

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

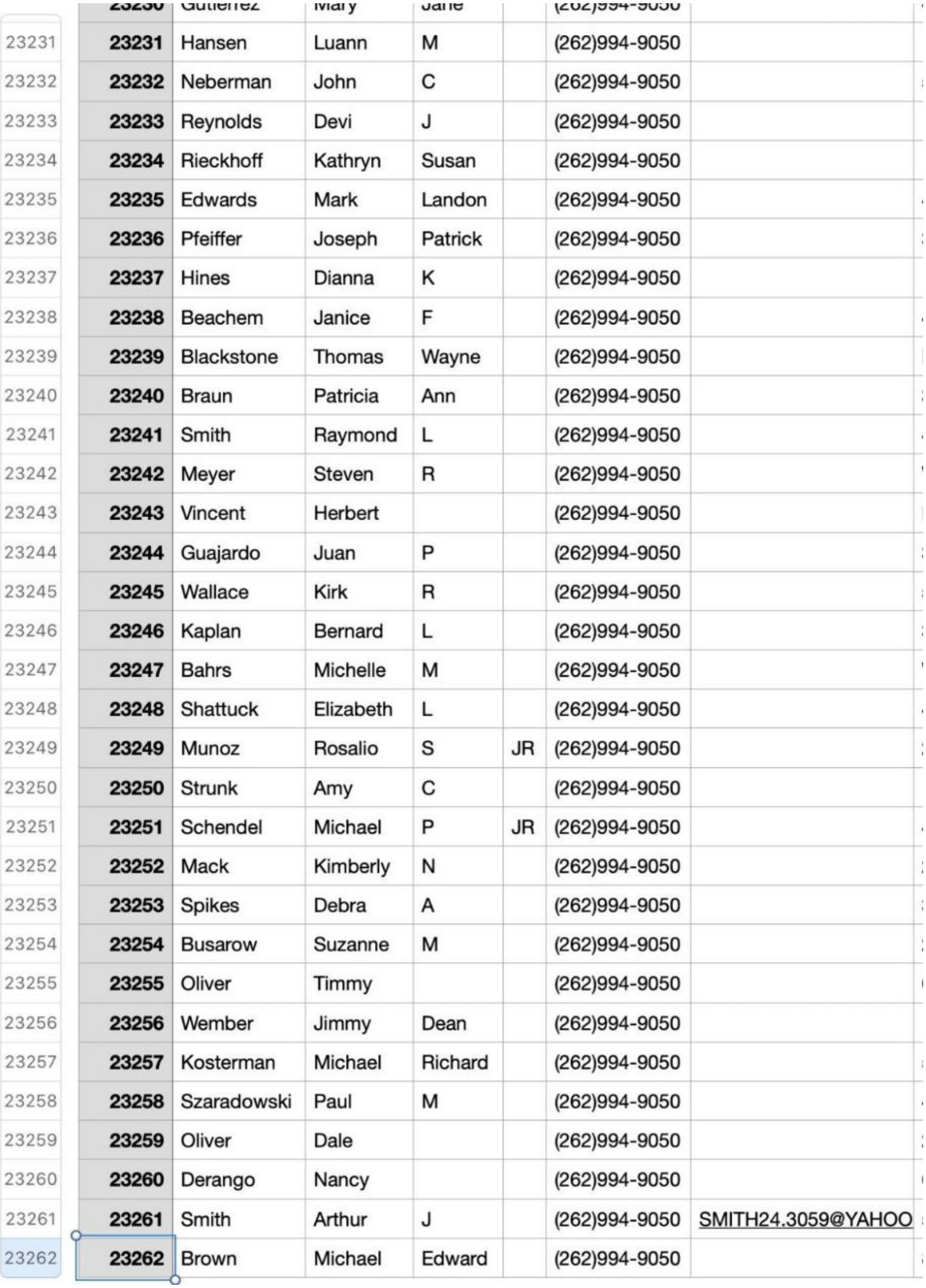
OCTOBER 26, 2020
U.S. Army STAND-TO! | Army Readines Training

SEPTEMBER 12, 2019
September 2017 Nominative Sergeant Major Assignments

SEPTEMBER 12, 2019
DA ANNOUNCES ROTATIONAL DEPLOYMENTS

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

155.



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

I declare under penalty of perjury that the forgoing is true and correct to the best of my knowledge.
Executed this November 29th, 2020.

Terpsehore P Maras

EXHIBIT X

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

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. I have reviewed the expert disclosures prepared by Dr. Juan Gilbert and Dr. Benjamin Adida for State Defendants. Neither Dr. Gilbert not Dr. Adida offers any rebuttal to the numerous, critical vulnerabilities in Georgia's BMDs that I described in my July 1, 2021 expert report. Dr. Adida did not respond to my report at all; State Defendants reissued prior declarations from him previously provided in this litigation. Neither of them disputes the presence of any of the serious

vulnerabilities I detail in my report or the steps I describe for exploiting those vulnerabilities to alter individual votes and election outcomes in Georgia. Nor does either of them claim to have examined any of the voting equipment used in Georgia to evaluate whether the vulnerabilities I identified—or others—have been exploited in any past election. Although each of them presumably could do this with the permission of State Defendants, who I understand engaged them as experts in this case, there is no indication either has undertaken any such inquiry or asked to do so. As a result, neither Dr. Gilbert nor Dr. Adida has anything to say about the reliability of the voting equipment used in Georgia elections. This is surprising, given that they have had at least the last year to examine Georgia's voting equipment.

3. State Defendants urgently need to engage with the findings in my report and address the vulnerabilities it describes before attackers exploit them. Nothing in Dr. Gilbert's or Dr. Adida's responses indicates that State Defendants understand the seriousness of these problems or have taken any measures to address them and their implications for the Plaintiffs' individual votes in future elections. Established practice in the security field would require State Defendants to promptly subject Georgia's voting system to rigorous testing in response to my report, to assess the extent and significance of each of the vulnerabilities I described, and to identify and *promptly implement* specific measures (where possible) to eliminate or mitigate each

of those vulnerabilities. Neither Dr. Gilbert nor Dr. Adida indicates any such efforts on their own part or on the part of State Defendants or anyone else. Again, Dr. Adida did not respond to my report.

4. In my report—a 25,000-word document that is the product of twelve weeks of intensive testing of the Dominion equipment provided by Fulton County—I find that Georgia's BMDs contains multiple severe security flaws. Attackers could exploit these flaws to install malicious software, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. I explain in detail how such malware, once installed, could alter voters' votes while subverting all the procedural protections practiced by the State, including acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk-limiting audits (RLAs). Finally, I describe working proof-of-concept malware that I am prepared to demonstrate in court.

5. My report concludes, *inter alia*, that Georgia's BMDs are not sufficiently secured against technical compromise to withstand vote-altering attacks by bad actors who are likely to target future elections in the state; that the BMDs' vulnerabilities compromise the auditability of Georgia's paper ballots; that the BMDs can be compromised to the same extent as or more easily than the DREs they replaced; and that using these vulnerable BMDs for all in-person voters, as Georgia

does, greatly magnifies the level of security risk compared to using hand-marked paper ballots and providing BMDs to voters who need or request them.

Reply to Declaration of Dr. Juan Gilbert

6. Rather than engage with the facts in my report, Dr. Gilbert responds largely with vague generalities. He gives no indication that he has ever used an ICX BMD, let alone tested its security. He begins by conceding that "any computer can be hacked," but he contends that "this general statement is largely irrelevant," because hand-marked paper ballot systems use computers too (to scan the ballots) (¶ 6). His position is inconsistent with accepted standards for election security and with the facts of the particular voting system used in Georgia.

7. My testing has shown that the BMDs used in Georgia suffer from specific, highly exploitable vulnerabilities that allow attackers to change votes despite the State's purported defenses. There is no evidence that Georgia's ballot scanners suffer from the same extraordinary degree of exploitability, nor does Dr. Gilbert contend they do. He ignores the relative ease with which Georgia's BMDs can be hacked, including by a voter in a voting booth in mere minutes. That extreme difference in security as compared to other voting technologies, particularly hand-marked paper ballots, is far from "irrelevant" as Dr. Gilbert implies.

8. Furthermore, even if the scanners were just as insecure as the BMDs, Georgia's practice of requiring essentially all in-person voters to use highly vulnerable BMDs would needlessly give attackers *double* the opportunity to change the personal votes of individual Georgia voters, since malware could strike either the BMDs or the scanners. Accepted standards in election security compel reducing points of attack for bad actors, not unnecessarily expanding them—a point Dr. Gilbert ignores.

9. Lastly, Dr. Gilbert also ignores that accepted election security protocols include an effective measure to protect against hacks of ballot scanners when the ballots are hand-marked rather than generated by BMDs—namely, reliable risk-limiting audits (RLAs), which would have a high probability of detecting any outcome-changing attack on the scanners. Not only do Georgia's BMDs defeat the efficacy of RLAs, but Dr. Gilbert continues to ignore the fact that Georgia requires an RLA of just one statewide contest every two years (and, to my knowledge, has not adopted specific, adequate procedures to ensure a reliable RLA for that one audit every other year).

10. Dr. Gilbert goes on to discuss issues related to voter verification of BMD ballots (which I respond to below). Yet he fails to address the potential for attackers to cheat by changing only the QR codes printed by Georgia's BMDs.

Voters cannot read the QR codes, but they are the only part of the ballots that the scanners count. My report details several routes by which malicious hardware or software can manipulate the QR codes and cause the recorded votes to differ from voters' selections. In principle, a rigorous risk-limiting audit would be likely to detect such an attack if the attacker changed enough votes to alter the outcome of the contest being audited, but again Georgia rules require such an audit in only a single statewide contest once every two years. As my report explains, this leaves the vast majority of elections and contests in Georgia vulnerable to QR code (and others) attacks, yet Dr. Gilbert says nothing about this threat.

11. Instead, Dr. Gilbert focuses exclusively on a different threat: attacks that change *both* the QR codes and the ballot text. In addition to the barcode-only attacks I just discussed, my report demonstrates that Georgia's BMDs can be manipulated so that both the barcodes and the printed text indicate the same fraudulent selections. No audit or recount can catch such fraud, because all records of the voter's intent would be wrong. The only reliable way to detect it would be if enough voters carefully reviewed their ballots, noticed that one or more selections differed from their intent, and reported the problems to election officials, *and* if Georgia officials then discerned from the pattern of voter reports that the BMDs were systematically misbehaving. Thus, Dr. Gilbert is mistaken when he contends that the distinction

between "voter-verifiable" and "voter-verified" paper ballots "only matters in principle" (¶ 7). All BMD ballots are potentially voter-verifiable, but unless enough BMD ballots are actually voter-*verified*, BMD-based attacks could alter election outcomes even in the rare instances where the State conducts a risk-limiting audit. And unless *every* BMD ballot is actually voter-*verified*, BMD-based attacks could alter individual voters' selections without detection..

12. A large body of recent scientific evidence has established that few voters are likely to catch errors caused by malicious BMDs. I have reviewed this evidence in previous declarations.[1] It comes from both field observations (which report how long real voters review their ballots during real elections) and laboratory tests (which report the fraction of errors that subjects detect when voting on hacked BMDs in simulated elections). These methodologies are complementary, and results to-date from all studies of both kinds point to a low rate of voter-verification.

13. Dr. Gilbert criticizes field observations because "[t]ime spent reviewing a ballot has little to do with whether it was actually verified" (¶ 9). This claim is inconsistent with accepted election security principles. Of course, they are not exactly the same question, but obviously the time spent reviewing a ballot can

[1] *Halderman decl.* (Dec. 16, 2019), Dkt. 682 at 23-33; *Halderman decl.* (Sept. 1, 2020) Dkt. 855-1 at 6-8, 55.

provide important insight into whether it was likely verified. For example, we can conclude that a voter who spends only a second or two reviewing a lengthy, complicated ballot is unlikely to have reliably verified each of their selections on the ballot. And of course, the same is true for a voter who spends no time at all reviewing their ballot. Review time is both practical to measure and clearly correlated with the error detection success, making it a valuable and relevant metric, as multiple studies confirm.

14. Dr. Gilbert seems to contend, without evidence, that a casual glance is sufficient to review Georgia-style ballots because selections are printed together with party affiliations (¶ 9). He cites no research (and I am unaware of any) that supports this conclusion, particularly when, as in Georgia, the party affiliations are printed in small type and in a different horizontal position for each contest. A real BMD ballot is reproduced on page 15 of my expert report. This is just one example of such a ballot; they can be longer and more confusing. Dr. Gilbert provides no basis for believing that voters would likely catch deliberate errors caused by compromised BMDs when voting such a ballot.

15. Dr. Gilbert references my award-winning peer-reviewed study about voter verification behavior, which found very poor rates of error detection and

reporting in a mock election using BMDs that my team hacked (¶ 10).[2] He contends that my study "ignores the reaction to such manipulation in an actual election, particularly one as heated in the public domain as the 2020 Election." (¶ 11). He does not explain how or why such circumstances would be expected to materially increase voter verification of their respective BMD ballots, nor does he cite any support for his claim to believe they would. And, just last week, the Atlanta Journal-Constitution obtained a study (under the Georgia Open Records Act) commissioned by the Secretary of State's Office in which researchers from the University of Georgia observed Georgia voters during the November 2020 election and reported how long they spent reviewing their BMD ballots.[3] Although it appears the Secretary of State had this study at the time of Dr. Gilbert's response to my report, he does not address or acknowledge it. The new study suggests that voters in the real world review their ballots *even less carefully* than voters in recent laboratory studies—despite the reminders election workers are supposed to give them to carefully review

[2] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" In *41st IEEE Symposium on Security and Privacy* (May 2020). Available at https://ieeexplore.ieee.org/document/9152705.

[3] Mark Niesse, "Under half of Georgia voters checked their paper ballots, study shows," *Atlanta Journal-Constitution* (July 27, 2021). Available at https://www.ajc.com/politics/under-half-of-georgia-voters-checked-their-paper-ballots-study-shows/6HSVHHFOBRBDPODRZXLIBTUS64/.

their ballots at the polling sites, which Dr. Gilbert emphasizes as a remedy for poor voter verification of BMD ballots.[4]

16. The University of Georgia researchers report that 20% of voters they observed did not check their ballots at all.[5] Only about 49% examined their ballots for at least one second, and only 19% did so for more than five seconds. This is significantly worse performance than observed in my study, which found that when voters were verbally prompted to review their ballots before casting them, as should occur in Georgia, 63% of voters reviewed their ballots for only *two* seconds or more, compared to 19-49% in the new study.

17. This suggests that laboratory studies like mine tend to *overestimate* the rate at which real Georgia voters would detect errors on their BMD ballots. Since real Georgia voters were observed to review their ballots even less carefully than the

[4] Secretary Raffensperger appears to disagree with Dr. Gilbert about the value of measuring voter review time for assessing voter verification performance. He told the Atlanta Journal-Constitution that the new study "shows voters do indeed review their ballots for accuracy before casting them" and offers "proof the votes that were counted were for the candidates the voters intended." (*Id.*). I agree that the new study provides valuable insights about voter behavior, but, contrary to the Secretary's pronouncements, the results indicate that real Georgia voters are even less likely to detect errors caused by compromised BMDs than previous studies have suggested.

[5] Audrey A. Haynes and M.V. Hood III, "Georgia Voter Verification Study" (January 22, 2021). Available at https://s3.documentcloud.org/documents/21017815/gvvs-report-11.pdf.

participants in my study, it is reasonable to infer that real voters would catch an even smaller fraction of errors. The participants in my study who were similarly prompted to review their ballots caught 14% of errors. Therefore, real voters in Georgia are likely to catch substantially less than 14% of errors.

18. How often would voters have to detect errors on their BMD ballots to effectively safeguard against attacks? The answer depends on the margin of victory, since an outcome-changing attack would need to change fewer votes in a close contest. The model from my study shows that, given the margin of victory from the 2020 Presidential contest in Georgia, voters would need to have detected 46% of errors for there to be even one error report per 1000 voters, under a hypothetical scenario where the election outcome had been changed by hacked BMDs.[6] The University of Georgia observations show that barely 49% of voters looked at their ballots for even a second, let alone studied them carefully enough to reliably spot errors.

[6] To reiterate, the November presidential race was the only state-wide contest subjected to a risk-limiting audit. In other contests, attackers could change the outcome by tampering with only the ballot QR codes, and voters would have no practical way to detect this manipulation regardless of how diligently they reviewed their ballots.

19. Dr. Gilbert performs a similar calculation using the baseline error detection rate measured in my study. He finds that an outcome changing attack on Georgia's Presidential contest would have resulted in only 832 voters noticing that their BMD ballots showed the wrong selection. Dr. Gilbert suggests that there have not been such complaints from any voters, and says he finds it implausible that so many voters would have "simply not said anything or otherwise simply corrected their ballot and thought nothing of it then or since" (¶ 12).

20. This is an oddly constructed hypothetical, since Curling Plaintiffs do not claim here that the Presidential outcome was altered by hacking the BMDs. And Dr. Gilbert does not indicate any effort to determine the total number of spoiled ballots in Georgia's Presidential contest, which he presumably could have explored with State Defendants. Neither does he provide any basis to believe there were only 832 or fewer spoiled ballots. But suppose for the sake of argument that the Presidential election outcome in Georgia had been altered by hacking the BMDs, and there *were* complaints from the 832 voters that Dr. Gilbert has calculated. What then? It seems all but certain that these complaints would have been dismissed or drowned out in the cacophonous aftermath of the election or simply disregarded by election workers at the polling sites as voter errors. Yet the official count, the risk-limiting audit, and the recount would all have found the wrong winner, and there would be no

way to recover any altered vote or correct the election outcome short of rerunning the election. With a mere 832 complaints among 5 million participating voters (amidst a sea of other complaints, real and imagined), it is unlikely that poll workers or election officials, including State Defendants, would realize or even suspected there was a systemic problem with the BMDs, and it is completely implausible that they would take the drastic but necessary step of asking Georgians to vote again. Georgia's election system is susceptible to this extraordinary risk as long as it remains vulnerable to the attacks I described in my report (and potentially others).

21. To get to the point of making a decision to rerun an election, State Defendants (among others, perhaps) would first need to know how many voters discovered a problem when verifying their ballots. As Dr. Gilbert points out, the number of spoiled BMD ballots provides an upper bound on the number of voters who discovered and corrected an error (¶ 12). He does not say how many spoiled ballots there actually were in November 2020. If State Defendants knew the number was less than 832, they likely would have shared this fact with Dr. Gilbert, and he would have stated it in his report. It is reasonable to infer that either there were more than 832 spoiled ballots (and the attack is plausible) or State Defendants *do not know* how many BMD ballots were spoiled during the election, eight months later, despite

what Dr. Gilbert acknowledges those ballots would suggest about the reliability of the election.

22. That State Defendants may not know this information is consistent with gaps in other important election data that Georgia counties report to the Secretary of State. State Defendants recently produced electronic data (election projects) that I understand were required to be returned to them by counties after the November 2020 and January 2021 elections. In both elections, a large fraction of counties failed to return any data, returned the wrong data, or omitted data necessary for assessing the security and integrity of the result, such as election databases or ballot images. More than six months after these elections, the Secretary of State has not been able to assemble these electronic records and has not indicated any effort or willingness to do so. Yet the only way that State Defendants could use the number of spoiled ballots as a defense against BMD-based cheating would be if the poll workers accurately tracked it, counties accurately aggregated it, and the Secretary's Office received such data from across the state before the election result was determined. Even then, it is unlikely that the Secretary would be prepared to react by *rerunning the election* if the number of spoiled ballots exceeded the number predicted in an outcome-changing attack.

23. Given the ineffectiveness of such defenses and the critical security problems in Georgia's BMDs, I (like Dr. Appel) recommend that BMDs be reserved for voters who need or request them, as is the case in most states. Dr. Gilbert responds by claiming, without evidence, that "[d]isabled voters are even less likely to identify an error on their printed ballot" (¶ 14). I am unaware of any study that supports this sweeping indictment of voters with disabilities, which encompasses a vast array of disabilities that would not impact the ability of the voter to identify an error on their printed ballot in any way. He also contends that blind voters cannot detect errors on their ballot at all, but this is not true. Many blind voters use assistive technology to read printed text and likely could do so to verify their ballots. Moreover, only some voters who need BMDs are blind. For instance, those with motor impairments that prevent them from marking a ballot by hand would not necessarily have any greater difficulty verifying the printed text than any other voter. In any case, if BMDs are used primarily by voters with disabilities (as in most jurisdictions that use BMDs), they will represent a *much* smaller target,[7] and an

[7] Although Dr. Gilbert cites a figure that would imply that 10% of Georgians who voted in 2020 were disabled, data from Maryland, where BMDs are available upon request, suggests that only about 1.8% of voters would request to use BMDs if they were offered a hand-marked ballot first. (*Halderman decl.*, Aug. 19, 2020, Dkt. 785-2 at 49.) Dr. Gilbert's citation to the number of all Georgia voters with disabilities is highly misleading since, again, very few of those voters would be

outcome-changing attack on any given election will be detectable with a much lower rate of voter error detection than when all in-person voters use BMDs as they do in Georgia today. This in turn creates a strong disincentive for bad actors to attempt hacking an election (the risk likely is not worth the reward when the outcome is highly unlikely to be changed), which means individual votes would be less likely to be altered by hacking.

24. In his only direct response to my expert report, Dr. Gilbert states that he is not aware that I have "provided equipment marred by 'undetectable' hacks to any other independent researcher" (¶ 15).[8] This is a curious and ironic criticism coming from Dr. Gilbert, since he evidently chose not to evaluate my findings through an examination of the voting equipment himself, which he does not explain. Moreover, Dr. Gilbert misreads my report. It does not claim that malicious software infecting a BMD would be undiscoverable by any possible means. If an individual BMD is

unable to vote on a hand-marked paper ballot, consistent with the number reported in Maryland.

[8] Dr. Gilbert ignores that, as I understand it, State Defendants have objected to my report and the underlying work being shared with third parties (except Dominion), including other independent researchers, with whom I am eager to share my work for review. I am confident in my findings and believe they should be shared promptly with appropriate election security researchers and officials in an effort to mitigate the critical vulnerabilities in Georgia's voting equipment that I describe. I invite Dr. Gilbert to join me in seeking State Defendants' consent to do that.

known to contain malware, there will likely be some level of detailed forensic scrutiny that can detect where the malware is, perhaps requiring months of expert analysis per machine at extraordinary expense. It would be completely infeasible to perform this level of analysis on every machine before every election, much less between an election and the deadline for certification of its results. (And after manipulating ballots, malware could remove all traces of its presence from a machine, defeating any possible post-election examination of the device.) What my report shows is that vote-stealing malware of the type I have constructed would not be detected by any of the defenses that State Defendants purport to practice. I describe in detail how such malware would defeat QR code authentication, logic and accuracy testing, on-screen hash validation, and external APK validation (as was used by Pro V&V after the November election). Dr. Gilbert offers no rebuttal to these findings. He does not dispute them or even address them.

25. Moreover, there is already an example of an "undetectable" attack entered into testimony: exploitation of the Drupal vulnerability discovered by Logan Lamb in the Center for Election Systems server. As Lamb attested, the developers of the primary tool for detecting this vulnerability stated that "[n]either [the defensive tool] nor an expert can guarantee a website has *not* been compromised. They can only

confirm with certainty a website *has* been compromised."[9] Furthermore, the Drupal developers state that any server running the vulnerable software after the initial disclosure of the vulnerability should be assumed to have been compromised unless it was patched within *hours* of disclosure. According to the timeline presented in Lamb's declaration, he found the KSU server to be in a vulnerable state on August 28, 2016, nearly two years after the initial announcement of the critical vulnerability (October 15, 2014).[10] The KSU server image also contains evidence that a second vulnerability, the so-called Shellshock flaw, was exploited on December 2, 2014.[11] This vulnerability was publicly disclosed more than two months earlier and widely publicized in the media as a critical vulnerability, yet the KSU server remained unpatched.

26. An attacker who compromised the KSU server could therefore have maintained undetected access to the compromised server. Since the server remained in a vulnerable state undetected for almost two years, it is highly likely that it was successfully attacked at some point in time. An attacker who did so would have been able to move laterally to other systems within the CES network and to other

[9] *Lamb decl.*, Dkt. 258-1 at 19.
[10] See "Drupal Core - Highly Critical - Public Service announcement" (Oct. 29, 2014), available at https://www.drupal.org/PSA-2014-003.
[11] *Halderman decl.* (Sept. 1, 2020) Dkt. 855-1 at 23.

components of Georgia's voting system. As I have previously pointed out, many election system components that could have been compromised in this way are still in use in Georgia today, where they provide a means by which attackers could spread vote-stealing malware to the BMDs.

27. Rather than address the many threats to Georgia's voting system, Dr. Gilbert persists in drawing illogical comparisons between BMDs and hand-marked paper ballots. For instance, he questions why Plaintiffs have presented no research "regarding voters' proclivity to review [hand-marked paper ballots] to ensure their ballots are marked and will count as intended" (¶ 8). Much like Dr. Gilbert's earlier testimony that "[i]n essence, a BMD is nothing more than an ink pen,"[12] one does not need expertise in election security to find fault with this reasoning. Preventing voters from making accidental mistakes is a completely different problem from preventing their selections from being deliberately and systematically changed by an attacker who has compromised the BMDs. There is abundant evidence that voters do sometimes make errors whether filling out a ballot by hand or by machine. Bad ballot design exacerbates this problem with both voting modalities, but following ballot design best practices can greatly reduce it. Both

[12] *Gilbert decl.*, Dkt. No. 658-3 at 60.

BMDs and scanners that count hand-marked ballots can also be configured to reject overvotes and to warn voters about undervotes, the most common kinds of voter errors. Moreover, unlike older technologies for counting hand-marked ballots, the scanners used in Georgia (when properly configured) can detect improperly or incompletely marked bubbles and present them to human operators to adjudicate whether the marks should count as votes. Election officials can use all of these options to help protect voters from their own mistakes, but none of them offers protection against a BMD that deliberately changes the selections printed on a voter's ballot (or those encoded in the ballot barcode). The central problem with Georgia's highly vulnerable BMD system—that attackers can change all records of the voter's intent without being detected by election officials—has no parallel in a hand-marked paper ballot system.

28. Dr. Gilbert concludes as he started, with vague and sweeping generalities. "Simply put, BMD elections systems are no more insecure than [hand-marked] systems" (¶ 16). It is unclear whether he is claiming that *all* BMD systems are at least as secure as all hand-marked systems or merely that some specific BMD system (such as the one he recently developed himself to address some of the reliability problems that exist with Georgia's BMDs) is at least as secure as some hand-marked system, but this is of little consequence. The only BMD system that is

relevant here is the Dominion ICX as used in Georgia. As my expert report details, Georgia's BMD system suffers from numerous, severe vulnerabilities. These vulnerabilities would have little potential to change election outcomes if use of BMDs were limited to voters who need or request them, as Curling Plaintiffs desire, and they would be far less likely to affect the personal votes of individual Georgia voters.

Reply to Declarations of Dr. Benjamin Adida

29. The declarations by Dr. Adida that State Defendants have submitted predate my expert report, so Dr. Adida's opinions are not informed by the critical vulnerabilities in Georgia's BMD equipment that my analysis has revealed or by anything else in my lengthy, detailed report. Nor are they informed by any events that occurred in the year since he first provided these declarations, such as any aspect of the November 2020 election in Georgia or the Secretary of State's study indicating that few voters verified their respective ballots in that election.

30. Nevertheless, Dr. Adida's first declaration is correct that "Running a risk-limiting audit is one of the most important advances states can take in improving election integrity—without an RLA, we are effectively trusting computerized scanners to count our paper ballots" (Dkt. 834-2 at ¶ 5). This is true, but, as my expert report shows, without a risk-limiting audit Georgia is also trusting its critically

vulnerable BMDs to generate ballots with QR codes that correctly reflect voters' selections. Obviously compromised BMDs and compromised scanners could change individual votes and election outcomes. But again, nothing suggests that Georgia's scanners suffer from such easily exploitable critical vulnerabilities as the BMDs do.

31. Dr. Adida and I also agree that RLAs are important for discovering whether compromised BMDs have manipulated enough ballot QR codes to change the outcome of an election (¶ 12). Although RLAs are, as Dr. Adida says, "of the utmost importance" (¶ 6), Georgia does not require an RLA in the vast majority of elections and the vast majority of contests, leaving both election outcomes and individual voters' votes susceptible to manipulation via BMD malware. Additionally, it is insufficient for states to merely (in Dr. Adida's words) "take meaningful steps to implement RLAs"; rather, states have to *actually conduct* reliable RLAs, which Georgia does not intend to do for the vast majority of its elections (or perhaps any of its elections, depending on the reliability of the audit procedures it implements).

32. In his second declaration, Dr. Adida refers to a "dispute amongst academics regarding whether voters verify their ballots using ballot-marking devices" (Dkt. 912-1 at ¶ 11). This statement reflects a misunderstanding of the state of research today. I am not aware of any scientific research that supports the proposition that Georgia voters would likely detect more than a small fraction of

errors caused by BMD malware. In contrast, the past two years have seen a wave of laboratory studies and multiple field observation studies addressing this question, all of which strongly indicate the opposite, that few voters carefully review their ballots and so the vast majority of errors caused by BMD malware would likely to go undiscovered and uncorrected. Although there once was uncertainty about whether most voters carefully verify their BMD ballots, there is no longer any serious scientific dispute that they do not. It is the hallmark of good science (and of good public policy) that it evolves based on new evidence, such as the University of Georgia study commissioned by the Secretary of State that I discussed above—which Dr. Adida has not addressed.

33. Georgia's election system needs to evolve as well. Due to the critical vulnerabilities in Georgia's BMDs that are described in my expert report, Georgia voters face an extreme risk that BMD-based attacks could manipulate their individual votes and alter election outcomes. Even in the rare contests for which the State requires a risk-limiting audit, the scientific evidence about voter verification shows that attackers who compromise the BMDs could likely change individual votes and even the winner of a close race without detection. Georgia can eliminate or greatly mitigate these risks by adopting the same approach to voting that is practiced in most of the country: using hand-marked paper ballots and reserving

BMDs for voters who need or request them. Absent security improvements such as this, it is my opinion that Georgia's voting system does not satisfy accepted security standards. Neither Dr. Gilbert nor Dr. Adida offers a contrary opinion in their respective declarations, instead ignoring the critical issue of whether the *voting system used in Georgia*—which neither claims to have examined—reliably protects the right to vote for individual Georgia voters.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 2nd day of August, 2021 in Rushland, Pennsylvania.

J. ALEX HALDERMAN

From:	Beth Biesel
To:	Secretary
Cc:	tanparkertexas@gmail.com
Subject:	Fwd: Request for Call with WV Secretary of State Mac Warner
Date:	Wednesday, June 21, 2023 3:11:02 PM

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear Secretary Nelson,

I am concerned that perhaps my email (below) from June 6th did not come through to you. Per Senator Parker’s request, I am resending my email to you. Thank you for taking the time to consider my request. I look forward to hearing from you.

Sincerely,
Beth Biesel
SD12

> Begin forwarded message:
>
> **From:** Beth Biesel <[redacted]
> **Subject: Request for Call with WV Secretary of State Mac Warner**
> **Date:** June 6, 2023 at 12:58:56 PM CDT
> **To:** Secretary@sos.texas.gov
> **Cc:** tanparkertexas@gmail.com
>
> Dear Secretary Nelson,
>
> Senator Tan Parker told me to send my request for you to speak with West Virginia Secretary Mac Warner directly to you at this email address. Thank you for your willingness to consider this request.
>
> I have been in a national election integrity coalition with Secretary Mac Warner over the past year. Secretary Warner would like to speak with you about his call for US Secretary of State Tony Blinken’s resignation. You may read about it in this article: https://www.einpresswire.com/article/632970423/warner-says-that-rebuilding-trust-and-confidence-in-american-elections-begins-with-the-immediate-resignation-of-u-s-secretary-of-state-antony-blinken.
>
> Secretary Warner would like to have the top Secretaries of State across the country join him in his call for Blinken’s resignation. I would be very grateful if you would take time to speak with Secretary Warner. He is a fine gentleman and a true statesman. He loves this country. I would be so proud to have the Texas Secretary of State lead the

way in this worthy endeavor.

I can provide Secretary Warner’s personal phone number when you are ready to call him.

Thank you!

Sincerely,
Beth Biesel
SD12

From: Beth Biesel [redacted] >
Sent: Wednesday, November 15, 2023 1:14 PM
To: Christina Adkins
Cc: Elizabeth Baron; Clint Curtis; Jody Curtis
Subject: Fwd: Wednesday, Oct. 25th Follow-up

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Hello Christina,

I know you have been swamped with election and post-election issues. When you have a moment, could you take a look at the email below that I sent on Oct. 30th summarizing the points we gleaned from our meeting on Oct. 25th? I want to make sure that we have a proper understanding of the explanations you gave us. We continue to get calls from people who want to hand count their ballots, so we want our responses to be in line with what you and your team said in our meeting.

Thank you so much!

Sincerely,
Beth Biesel
Dallas County

Begin forwarded message:

From: Beth Biesel [redacted] >
Subject: Wednesday, Oct. 25th Follow-up
Date: October 30, 2023 at 9:28:35 AM CDT
To: Christina Adkins <CAdkins@sos.texas.gov>
Cc: Elizabeth Baron [redacted] >, Clint Curtis [redacted] >, Jody Curtis [redacted] >

Dear Christina,

Thank you so much for meeting with Elizabeth, Clint, Jody, and me Wednesday, October 25, 2023, and for bringing your very talented staff to the meeting to help us sort through the many sections of the Texas Election Code. We appreciate your taking a serious look at our two alternatives to the Chapter 65 Hand Count Method. Your guidance and suggestions are extremely valuable.

To make sure that we are on the right track, I would like to summarize the things that we learned from the meeting. I look forward to your feedback. In no particular order:

- Cameras are allowed after the polls close, 7:00pm or later, in the counting area - or before 7:00pm if the counting is done 100ft away from the polling place.
- If using the calculator method, we should use the label "Batch Total Sheet" rather than "Batch Tally Sheet" since we are not using tally marks.
- If using the calculator method, we need a way of memorializing the tally count with a paper trail showing how we arrived at our totals for each candidate or proposition.
- Elizabeth Baron will follow up with you on what can be done with the number grid/bingo tally sheets. We want to know if they comply with the need to have a paper record showing how the total for a candidate or proposition was determined.
- Parallel counting is not allowed. Parallel counting would be an unauthorized count. The reason is to avoid disputes as to which count would be official.
- Ballot on Demand printers do not need to be certified.
- The hand count calculators do not need to be certified because they are not a voting system. They do not cast ballots and they do not tabulate ballots.
- Write-in candidates would be counted and adjudicated, if necessary, by the Presiding Judge when the hand count is done at the precinct location.
- Ballot Boxes 1-4 may have some flexibility. In Dallas County, we use a zippered canvas bag with a seal for our ballot box 4. Chuck or Heidi were going to clarify the absolute requirements for boxes, especially if the counting begins after the polls closed. Could we eliminate one of the boxes if we begin after 7:00pm?
- Ballots must be approved by the SOS before going to the printer.
- Chuck will investigate whether or not the process of counting one pair of candidates at a time across all ballots in a batch vs counting one ballot at a time is materially different from the process described in Chapter 65? Would it need a legislative change or would the law requirements be met because we are still counting by race, albeit, by pairs. (The calculator method of hand counting is done by counting the votes for a pair of candidates at a time, within a given race, going through all the ballots in a batch for each pair. After all the candidates within the race are counted, then the counters would go to the next race/next pair. The advantage of this method is that the throughput rate is much faster than Chapter 65 (fewer people, less time) and the two means of reconciling a) for each

count run and b) at the end of each race yield a higher degree of accuracy and confidence.

- The question of sorting the ballots by precinct/ballot style during Early Voting was discussed, but I am unclear on what the law requires. For Early Voting, could we sort the ballots at the countywide vote location as they are voted into ballot boxes labeled by precinct number/ballot style? Historical data will give us a high degree of accuracy of predetermining the majority of precincts that are represented at a particular vote location. The outliers could go in a miscellaneous box to be sorted at the end of the night or some other time.
- We know that counting of Eary Voting ballots may not occur until polls open on Election Day, but may EVBB convene before that time to sort ballots into precincts?

We are so deeply grateful for your incredible dedication to protecting our Texas elections! You have a great team! We look forward to working closely with you as we find new ways to increase trust in our elections through transparency, verifiability, and accuracy. This is not a slogan; it is the gold standard!

Sincerely,
Beth Biesel
and
Elizabeth Baron
Jody and Clint Curtis

From: Andrew Eller <[redacted]>
Sent: Monday, October 16, 2023 11:17 AM
To: Christina Adkins; Elections Internet
Subject: Issues with Poll Watcher Training on SOS Website

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Christina, As I always do just prior to an election to make sure I understand everything, I went to take the SOS standardized training for several areas, Poll Watcher, Central Count, Poll Worker, etc. When I went to take the Poll Watcher training on the SOS website today and found what I believe to be some back end issues with the system.

As I reached several of the Lesson Quizzes I quickly selected my answers that I knew were correct and then clicked "complete". But multiple times it came back as failing the quiz with 0% correct. I knew I had clicked the correct answers. So I would retry again, this time selecting a different answer and still get the same issue. So I then would go back and selected what I knew were the correct answers again, only this time more slowly. Then I would wait a minute or so before clicking the "complete". At that point it would accept my answers as being correct. So by the time I got to the end of the training, I was slowing down on the quizzes and that seem to fix the problem.

It appears there is an issue on the back end where the GUI isn't transferring the selected answers fast enough for some of us to the back end for the check if they are correct or not. Please have someone look into this and if possible let me know if they have been able to correct it. It is rather frustrating knowing you gave the correct answer and having the system tell you it wasn't (most likely because it didn't see the my selected answer). Then redoing it with the exact same answers and passing the quiz at 100%.

Thanks
Andy Eller
SREC Committeeman SD24
Bell County Central Count Station Presiding Judge

From: no-reply@efilingmail.tylertech.cloud
To: Secretary
Subject: Notification of Service for Case: , for filing Application, Envelope Number: 81786704
Date: Saturday, November 18, 2023 12:28:13 AM

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Notification of Service

Case Number:
Case Style:
Envelope Number: 81786704

This is a notification of service for the filing listed. Please click the link below to retrieve the submitted document. If the link does not work, please copy the link and paste into your browser. You can also obtain this document by following the steps on this article.

Filing Details	
Case Number	
Case Style	
Date/Time Submitted	11/18/2023 12:26 AM CST
Filing Type	Application
Filing Description	Affidavit of J. Alex Halderman - Security Flaws in Ballot Marking Devices
Filed By	Travis Eubanks
Service Contacts	Travis Wayne Eubanks: Travis Eubanks (travis.eubanks@gmail.com) Jane Nelson: Jane Nelson (secretary@sos.texas.gov) Amanda Marie Eubanks:

	Amanda Eubanks (amanda.eubanks710@gmail.com) Jarrett Woodward: Jarrett Woodward (jarrett@texashomesduo.com)

Document Details	
Served Document	Download Document
This link is active for 30 days.	

From: no-reply@efilingmail.tylertech.cloud
To: Secretary
Subject: Notification of Service for Case: , for filing Application, Envelope Number: 81786704
Date: Saturday, November 18, 2023 12:28:15 AM

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Notification of Service

Case Number:
Case Style:
Envelope Number: 81786704

This is a notification of service for the filing listed. Please click the link below to retrieve the submitted document. If the link does not work, please copy the link and paste into your browser. You can also obtain this document by following the steps on this article.

Filing Details	
Case Number	
Case Style	
Date/Time Submitted	11/18/2023 12:26 AM CST
Filing Type	Application
Filing Description	Affidavit of Terpsehore Maras - VSTLs and the EAC
Filed By	Travis Eubanks
Service Contacts	Travis Wayne Eubanks: Travis Eubanks (travis.eubanks@gmail.com) Jane Nelson: Jane Nelson (secretary@sos.texas.gov) Amanda Marie Eubanks:

	Amanda Eubanks (amanda.eubanks710@gmail.com) Jarrett Woodward: Jarrett Woodward (jarrett@texashomesduo.com)

Document Details	
Served Document	Download Document
This link is active for 30 days.	

From: no-reply@efilingmail.tylertech.cloud
To: Secretary
Subject: Notification of Service for Case: , for filing Petition, Envelope Number: 81786704
Date: Saturday, November 18, 2023 12:28:16 AM

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Notification of Service

Case Number:
Case Style:
Envelope Number: 81786704

This is a notification of service for the filing listed. Please click the link below to retrieve the submitted document. If the link does not work, please copy the link and paste into your browser. You can also obtain this document by following the steps on this article.

Filing Details	
Case Number	
Case Style	
Date/Time Submitted	11/18/2023 12:26 AM CST
Filing Type	Petition
Filing Description	Constitutional Amendment Election Contest Petition
Filed By	Travis Eubanks
	Travis Wayne Eubanks: Travis Eubanks (travis.eubanks@gmail.com) Jane Nelson: Jane Nelson (secretary@sos.texas.gov)

Service Contacts	Amanda Marie Eubanks: Amanda Eubanks (amanda.eubanks710@gmail.com) Jarrett Woodward: Jarrett Woodward (jarrett@texashomesduo.com)

Document Details	
Served Document	Download Document
This link is active for 30 days.	

From: no-reply@efilingmail.tylertech.cloud
To: Secretary
Subject: Notification of Service for Case: , for filing Petition, Envelope Number: 81791461
Date: Saturday, November 18, 2023 10:46:53 PM

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Notification of Service

Case Number:
Case Style:
Envelope Number: 81791461

This is a notification of service for the filing listed. Please click the link below to retrieve the submitted document. If the link does not work, please copy the link and paste into your browser. You can also obtain this document by following the steps on this article.

Filing Details	
Case Number	
Case Style	
Date/Time Submitted	11/18/2023 10:45 PM CST
Filing Type	Petition
Filing Description	Constitutional Amendment Election Contest Petition
Filed By	Travis Eubanks
Service Contacts	Travis Wayne Eubanks: Travis Eubanks (travis.eubanks@gmail.com) Jane Nelson: Jane Nelson (secretary@sos.texas.gov) Amanda Marie Eubanks:

	Amanda Eubanks (amanda.eubanks710@gmail.com) Jarrett Woodward: Jarrett Woodward (Digging4au@protonmail.com)

Document Details	
Served Document	Download Document
This link is active for 30 days.	

From: [redacted] >
Sent: Saturday, June 10, 2023 1:57 PM
To: Elections Internet
Subject: Public Comment RE: Certification of ES&S EVS 6.2.0.0

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear Secretary Nelson,

I, Jarrett Woodward, DO NOT CONSENT to the certification of ES&S EVS 6.2.0.0 for use in Texas elections. Examiner reports mention EAC Certification Number ESSEVS6200 as evidence of compliance with Texas Election Code 122.001(a)(3) and Texas Administration Code 81.60. Because the specific phrase **nationally accredited voting system test laboratory** appears multiple times in Tex Admin Code 81.60, you have a duty to verify the accreditation status of the laboratory in order to validate the reference to EAC Certification Number ESSEVS6200. Although issuance of this certificate by the EAC implies that the system was tested by an accredited voting system test laboratory, the Voting System Testing and Certification Program Manual version 3.0 section 1.6.2 states: “State officials have responsibility for testing voting systems to ensure the system will support the specific requirements of each individual state. States may use EAC-accredited VSTLs to perform testing of voting systems to unique state standards while the systems are being tested to the VVSG. However, the EAC does not certify voting systems to state standards.”

The VSTL used to test ES&S EVS 6.2.0.0 for EAC certification was Pro V&V. The testing took place at some point between February 12, 2021 and December 23, 2021. Upon reviewing the Certificate of Accreditation issued for Pro V&V during this time frame and comparing it to the requirements of what must be on the certificate as outlined in the Voting System Test Laboratory Program Manual version 3.0 section 3.6.1 (version 2.0 as well), you will notice that it does not contain the required signature of the Chair of the Commission. Commission is defined in Appendix A as the US Election Assistance Commission, as an agency. This makes the Certificate of Accreditation INVALID resulting in Pro V&V being an UNACCREDITED test laboratory at the time of testing.

Utilizing any reports or delivery of voting system components from Pro V&V for the certification process to approve ES&S EVS 6.2.0.0 for use in Texas does not satisfy the requirements of Texas Election Code or Texas Administrative Code. The VSTL Program Manual states in section 1.4 that it is to be read in conjunction with the Voting System Testing and Certification Manual making them both voting system standards adopted by the EAC falling under Tex Elec Code 122.001(a)(3).

Because ES&S EVS 6.2.0.0 does not satisfy the applicable requirements for approval, you are required to deny the application under Tex Elec Code 122.038(c). If you certify this system for use in Texas elections, you will be knowingly breaking the law and continuing the damage that has already been done to elections in our great state. This is your moment of truth on full display for all of Texas and the People are watching to see if you honor your oath.

Respectfully,

Jarrett Woodward
[redacted]
210-693-7457

Sent with Proton Mail secure email.

From: [redacted] >
Sent: Saturday, June 10, 2023 1:58 PM
To: Elections Internet
Subject: Public Comment RE: Certification of ES&S EVS 6.3.0.0

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear Secretary Nelson,

I, Jarrett Woodward, DO NOT CONSENT to the certification of ES&S EVS 6.3.0.0 for use in Texas elections. Examiner reports mention EAC Certification Number ESSEVS6300 as evidence of compliance with Texas Election Code 122.001(a)(3) and Texas Administration Code 81.60. Because the specific phrase **nationally accredited voting system test laboratory** appears multiple times in Tex Admin Code 81.60, you have a duty to verify the accreditation status of the laboratory in order to validate the reference to EAC Certification Number ESSEVS6300. Although issuance of this certificate by the EAC implies that the system was tested by an accredited voting system test laboratory, the Voting System Testing and Certification Program Manual version 3.0 section 1.6.2 states: “State officials have responsibility for testing voting systems to ensure the system will support the specific requirements of each individual state. States may use EAC-accredited VSTLs to perform testing of voting systems to unique state standards while the systems are being tested to the VVSG. However, the EAC does not certify voting systems to state standards.”

The VSTL used to test ES&S EVS 6.3.0.0 for EAC certification was Pro V&V. The testing took place at some point between April 7, 2022 and November 17, 2022. Upon reviewing the multiple Certificate of Accreditations issued for Pro V&V during this time frame and comparing it to the requirements of what must be on the certificate as outlined in the Voting System Test Laboratory Program Manual version 3.0 section 3.6.1 (version 2.0 as well), you will notice that it does not contain the required signature of the Chair of the Commission. Commission is defined in Appendix A as the US Election Assistance Commission, as an agency. This makes the Certificate of Accreditation INVALID resulting in Pro V&V being an UNACCREDITED test laboratory at the time of testing.

Utilizing any reports or delivery of voting system components from Pro V&V for the certification process to approve ES&S EVS 6.3.0.0 for use in Texas does not satisfy the requirements of Texas Election Code or Texas Administrative Code. The VSTL Program Manual states in section 1.4 that it is to be read in conjunction with the Voting System Testing and Certification Manual making them both voting system standards adopted by the EAC falling under Tex Elec Code 122.001(a)(3).

Because ES&S EVS 6.3.0.0 does not satisfy the applicable requirements for approval, you are required to deny the application under Tex Elec Code 122.038(c). If you certify this system for use in Texas elections, you will be knowingly breaking the law and continuing the damage that has already been done to elections in our great state. This is your moment of truth on full display for all of Texas and the People are watching to see if you honor your oath.

Respectfully,

Jarrett Woodward
[redacted]
210-693-7457

Sent with Proton Mail secure email.

From: Beth Biesel
To: Secretary
Cc: tanparkertexas@gmail.com
Subject: Request for Call with WV Secretary of State Mac Warner
Date: Tuesday, June 6, 2023 12:59:07 PM

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear Secretary Nelson,

Senator Tan Parker told me to send my request for you to speak with West Virginia Secretary Mac Warner directly to you at this email address. Thank you for your willingness to consider this request.

I have been in a national election integrity coalition with Secretary Mac Warner over the past year. Secretary Warner would like to speak with you about his call for US Secretary of State Tony Blinken's resignation. You may read about it in this article: https://www.einpresswire.com/article/632970423/warner-says-that-rebuilding-trust-and-confidence-in-american-elections-begins-with-the-immediate-resignation-of-u-s-secretary-of-state-antony-blinken.

Secretary Warner would like to have the top Secretaries of State across the country join him in his call for Blinken's resignation. I would be very grateful if you would take time to speak with Secretary Warner. He is a fine gentleman and a true statesman. He loves this country. I would be so proud to have the Texas Secretary of State lead the way in this worthy endeavor.

I can provide Secretary Warner's personal phone number when you are ready to call him.

Thank you!

Sincerely,
Beth Biesel
SD12

From: Beverly Foley [redacted]
Sent: Thursday, May 25, 2023 2:03 PM
To: Secretary
Subject: Request meeting with Secretary Nelson elections related meeting

Follow Up Flag: Follow up
Flag Status: Flagged

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Hi Kim,

I would like to request a meeting in the near future with Secretary Nelson. The meeting would be to discuss elections. I am part of a group – Texas First – it would be 3-4 people.

Secretary Nelson was my Senator from North Texas. (Trophy Club TX-Denton County). Our group works on various topics, voter rolls, election workers training, election code, auditing elections and mine - "records management".

I recently spent 6 weeks in Tarrant County elections auditing 2020 mail in ballots. I came away with a very big concern over records management that I addressed with the Ballot Board president in Tarrant for future elections record storage. Auditing voter records after an election needs to be very well organized for accessibility.

Please let me know when Secretary Nelson will have availability in the near future to discuss some of these topics about our elections.

Sincerely,
Beverly Foley
8 Oak Village Ct
Trophy Club TX 76262
Denton County

(prior Trophy Club Town Council member)

Sent from Mail for Windows

From: Beth Biesel [redacted]
Sent: Monday, October 30, 2023 9:29 AM
To: Christina Adkins
Cc: Elizabeth Baron; Clint Curtis; Jody Curtis
Subject: Wednesday, Oct. 25th Follow-up

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to Informationsecurity@sos.texas.gov.

Dear Christina,

Thank you so much for meeting with Elizabeth, Clint, Jody, and me Wednesday, October 25, 2023, and for bringing your very talented staff to the meeting to help us sort through the many sections of the Texas Election Code. We appreciate your taking a serious look at our two alternatives to the Chapter 65 Hand Count Method. Your guidance and suggestions are extremely valuable.

To make sure that we are on the right track, I would like to summarize the things that we learned from the meeting. I look forward to your feedback. In no particular order:

- Cameras are allowed after the polls close, 7:00pm or later, in the counting area - or before 7:00pm if the counting is done 100ft away from the polling place.
- If using the calculator method, we should use the label “Batch Total Sheet” rather than “Batch Tally Sheet” since we are not using tally marks.
- If using the calculator method, we need a way of memorializing the tally count with a paper trail showing how we arrived at our totals for each candidate or proposition.
- Elizabeth Baron will follow up with you on what can be done with the number grid/bingo tally sheets. We want to know if they comply with the need to have a paper record showing how the total for a candidate or proposition was determined.
- Parallel counting is not allowed. Parallel counting would be an unauthorized count. The reason is to avoid disputes as to which count would be official.
- Ballot on Demand printers do not need to be certified.
- The hand count calculators do not need to be certified because they are not a voting system. They do not cast ballots and they do not tabulate ballots.
- Write-in candidates would be counted and adjudicated, if necessary, by the Presiding Judge when the hand count is done at the precinct location.
- Ballot Boxes 1-4 may have some flexibility. In Dallas County, we use a zippered canvas bag with a seal for our ballot box 4. Chuck or Heidi were going to clarify the absolute

requirements for boxes, especially if the counting begins after the polls closed. Could we eliminate one of the boxes if we begin after 7:00pm?

- Ballots must be approved by the SOS before going to the printer.
- Chuck will investigate whether or not the process of counting one pair of candidates at a time across all ballots in a batch vs counting one ballot at a time is materially different from the process described in Chapter 65? Would it need a legislative change or would the law requirements be met because we are still counting by race, albeit, by pairs. (The calculator method of hand counting is done by counting the votes for a pair of candidates at a time, within a given race, going through all the ballots in a batch for each pair. After all the candidates within the race are counted, then the counters would go to the next race/next pair. The advantage of this method is that the throughput rate is much faster than Chapter 65 (fewer people, less time) and the two means of reconciling a) for each count run and b) at the end of each race yield a higher degree of accuracy and confidence.
- The question of sorting the ballots by precinct/ballot style during Early Voting was discussed, but I am unclear on what the law requires. For Early Voting, could we sort the ballots at the countywide vote location as they are voted into ballot boxes labeled by precinct number/ballot style? Historical data will give us a high degree of accuracy of predetermining the majority of precincts that are represented at a particular vote location. The outliers could go in a miscellaneous box to be sorted at the end of the night or some other time.
- We know that counting of Eary Voting ballots may not occur until polls open on Election Day, but may EVBB convene before that time to sort ballots into precincts?

We are so deeply grateful for your incredible dedication to protecting our Texas elections! You have a great team! We look forward to working closely with you as we find new ways to increase trust in our elections through transparency, verifiability, and accuracy. This is not a slogan; it is the gold standard!

Sincerely,
Beth Biesel
and
Elizabeth Baron
Jody and Clint Curtis