

**IN THE SUPERIOR COURT OF CHEROKEE COUNTY
STATE OF GEORGIA**

LORI PORTILLO
210 Carmichael Road
Woodstock, GA 30189
Petitioner, Pro Se

CIVIL ACTION
No. 22CVE1890

v.

BRAD RAFFENSPERGER in his
official capacity as the Georgia
Secretary of State

CHEROKEE COUNTY
BOARD OF ELECTIONS
Alan Shinall
Mike Byrd
Rachel Kinsey
Cindy Castello
Donald Sams
Respondents

**VERIFIED COMPLAINT FOR DECLARATORY JUDGMENT and
INJUNCTIVE RELIEF**

COMES NOW, Lori Portillo, ("Petitioner"), Pro Se, and file this, their
Complaint against Brad Raffensperger in his official capacity as the Georgia
Secretary of State ("SoS") and the Cherokee County Board of Elections ("BoE")
as listed above. In support of the claims set forth herein, Petitioner alleges and
avers as follows:

INTRODUCTION

1. This action seeks Declaratory Judgment and Emergency Injunctive Relief pursuant to O.C.G.A.: 50-13-10 *et seq.*; 9-4-2 *et seq.*; 9-11-65; and 21-2-32.

This action arises under O.C.G.A.: 21-2-300(a)(2) and (3); 21-2-321(a), (c) and (e); 21-2-365(8). First, Fourteenth and Twenty Sixth Amendment of the US Constitution. Article I, Section I, Paragraphs I, II, VII, and IX of the Georgia ("GA") Constitution. Help America Vote Act ("HAVA") 2002, 52 USC 10307(d), 52 USC 10308 *et seq.* Subject matter jurisdiction and venue are proper and are conveyed to this honorable Court pursuant to GA Code Title 50-13-10. The petitioner is a citizen and taxpayer of Georgia and Cherokee County and a registered voter of the same.

2. The Petitioner and People of Georgia ("GA") have been bringing to the attention of our county Boards of Elections ("BoE"), County Commissioners, State BoE and the GA SoS office proof of widespread fraud, the fact that the Ballot Marking Devices ("BMD") and ImageCast X voting system ("ICX") do not record and count actual votes cast but the ICX's interpretation of the QR Code or bar code printed on the ballot, and the fact that these BMD's including all peripheral equipment, hardware and software were not legally certified by the Elections Assistance Commission ("EAC") at the time they were purchased nor at the times they were used as is required by GA law. Any standard, practice or

procedure that results in the abridgment or denial of the right of any citizen to vote ((Footnote ("FN") 3)) is unconstitutional and illegal (FN 4).

3. The Petitioner nor the People of GA ever voted to move from hand marked paper ballots to electronic machine voting as is required by law.

4. The Petitioner nor the People of GA ever voted to increase the debt of their county's of residence for the move to electronic voting machines as is required by law.

5. The County BoE's that have attempted to move to hand marked paper ballots, as is authorized by law, were intimidated by the GA SoS office with threats of exorbitant fines if they followed through with this move.

6. The county BoE's that have attempted to do hand recounts of the original ballots cast were also intimidated by the GA SoS office or their own county attorneys. The only explanation for this is to cover up fraud, or to cover up the fact that the current BMD/ICX voting system is fraught with errors.

7. The Petitioner and the People of Georgia are being stonewalled by either their County BoE's or the GA SoS office for Open Records Requests, that are our right to access, as is stated by GA law. Again, the only explanation would be to cover up fraud or the proof that the current BMD/ICX voting system is fraught with errors.

8. The current voting system is too dependent on technology. This allows for multiple avenues of hostile incursions into our elections. This was testified to

by Brian Kemp in 2016 while participating in a Congressional hearing, following his report titled “Critical Infrastructure & DHS Hacking Attempts”. Brian Kemp correctly argued at that time, based on the Constitution protecting the right of States to conduct elections, that designating elections as ‘critical infrastructure’ would cause a lack of transparency for voters and would open the States up to vulnerabilities.

9. The ‘critical infrastructure’ designation is a usurpation of State’s rights as protected by the United States (“US”) Constitution. The ‘critical infrastructure’ designation is unconstitutional and has effectively federalized our elections. This designation was an overstep of authority by an unelected administrative agency of the Executive Branch. It is in violation of separation of powers, the Tenth Amendment, and Article 1, Section 4 of the Constitution. Only Congress can make law to alter election regulations.

10. The US EAC is the authority for accreditation of vendors responsible for ensuring the electronic voting systems are certified for use. The EAC has now, allegedly, been caught falsifying documents in an attempt to mislead the People into believing these vendors are accredited when they are not and have not been since 2017. This alleged fraud and forgery committed by a federal employee of a federal commission should suspend all actions of the EAC and the vendors they supposedly accredited until a full investigation of these alleged crimes has been completed.

11. The fact that the voting machine manufacturers are the ones that pay the third party Voting System Testing Labs ("VSTL") for certifying that their voting machines meet the standards required by the EAC is an egregious conflict of interest.

12. The recent advisory issued by the Cybersecurity and Infrastructure Security Agency ("CISA") (Ex. J) lists a multitude of vulnerabilities that cannot be addressed with any assurances. This list of vulnerabilities prove that not only is it quite simple to install malware with a variety of avenues, but that these voting systems indeed have illegal internet access capability.

STATEMENT OF FACTS

13. Brad Raffensperger, in his official capacity as the GA SoS, had a duty to ensure these Dominion voting systems were certified prior to purchase. The applicable GA code reads - *O.C.G.A. 21-2-300 (a)(3) - The state shall furnish a uniform system of electronic ballot markers and ballot scanners for use in each county as soon as possible. Such equipment shall be certified by the United States Election Assistance Commission prior to purchase, lease, or acquisition.* This was not done. Brad Raffensperger acquired the Dominion voting system in violation of O.C.G.A. 21-2-300(a)(3). Therefore, the current ICX system is illegal in the state of GA and the usage of this system should be immediately discontinued.

14. A cursory inspection of the US EAC website shows the accreditation for Pro V&V expired February 24, 2017 (Ex. A). No later documents showing accreditation exist on the EAC website until February 1, 2021 (Ex. A1). Even this document is not valid since these certificates require expiration dates per VSTL Program Manual Section 3.6.1.3 which states *'The effective date of the certification, which shall not exceed a period of two (2) years'*. This is a complete failure on the part of the SoS office.

15. The EAC attempted to gloss over their and Pro V&V's oversight by issuing a memo dated 1/27/2021 (Ex. A2) in which they blamed COVID-19. This is ludicrous since the Pro V&V renewal period for their accreditation expired over three years prior to COVID-19 appearing in the US. Pro V&V was required to submit application for renewal between December 24, 2016 and January 24, 2017, which is 30 to 60 days prior to expiration, as is required by law. The EAC again attempted to gloss over their and Pro V&V's failings by stating the EAC did not vote to revoke Pro V&V's accreditation. This, again, is ludicrous as the accreditation had expired as of February 24, 2017 which adheres to the guidelines set forth in the VSTL Program Manual. The EAC admits a grant of accreditation is valid for a period not to exceed two years and that the date of expiration is required to be annotated on the certificate in this 'memo'.

16. The failings of the EAC and Pro V&V do not mitigate the malfeasance, nonfeasance of office and official misconduct perpetrated by Brad

Raffensperger. It also does not abrogate his responsibilities and duty to the People and laws of GA. If accreditation seemed questionable, which it still does, Brad Raffensperger as the SoS of this state and the individual in charge of elections, should have been able to discern these glaring issues. This is an obvious violation of O.C.G.A. 45-11-4.

17. Brad Raffensperger continued to expound on Pro V&V being EAC accredited on multiple occasions. Multiple times in a court of law, in the *Donna Curling, et al. v. Brad Raffensperger, et al. CIVIL ACTION NO. 1:17-cv-2989-AT*, as well as on the SoS website, where it was stated, “Secretary of State Brad Raffensperger last week ordered Pro V&V, a *U.S. Election Assistance Commission certified testing laboratory*, to do an audit of a random sample of machines to confirm no hack or tamper.” (emphasis added) (Ex. B). These are just a few examples. There are many more. There is another issue with this statement as put forward by the GA SoS, Pro V&V nor any VSTL is qualified nor accredited through the EAC to perform any type of forensic audit of the voting systems. Though, the People of GA paid them, under the direction of Brad Raffensperger, for this service they are not accredited, nor perhaps qualified, to do. It is also an obvious conflict of interest to have the company that supposedly ‘certified’ the voting machines to also perform the audit.

18. Brad Raffensperger was aware of the fact that Pro V&V was not accredited through the EAC since at least September 11, 2019. Ryan Germany,

General Counsel for the GA SoS, received an email from an attorney, Robert McGuire, who was representing the Coalition for Good Governance in the pending *Curling v. Raffensperger* lawsuit. The pertinent portion of this email, dated September 11, 2019, reads, *“Finally, we understand that Pro V&V served as the testing agent for the EAC and also to provide some functional testing for the State’s certification of the BMD system. We have been unable to find a current EAC certificate of accreditation for Pro V&V. The certificates seem to have been removed from the EAC website, and the latest ones we can locate expired in 2017. Can you please advise whether Pro V&V is an accredited testing lab, certified by the EAC?”* (Ex. C pg 5).

19. On September 17, 2019, six days after this email was received by Ryan Germany, a ‘document’ mysteriously appears on the EAC website. This ‘document’ titled “Pro V&V Letter of Agreement.pdf” was neither signed nor dated as is required pursuant to EAC’s VSTL Program Manual Section 3.4.2. (<https://www.eac.gov/voting-equipment/manuals-and-forms>). This ‘Letter of Agreement’, seems to have been created by the EAC Testing and Certification Director, Jerome Lovato (Ex. C), and put out to the public via the EAC website as a document submitted by Jack Cobb of Pro V&V.

20. The many and varied, glaringly obvious, discrepancies included in this ‘Letter’: it is addressed to Mr. Brian Hancock who retired in February 2019; the file’s metadata shows the document was created by Jerome Lovato, not Jack

Cobb of Pro V&V; metadata revealed the document was created on September 17, 2019, six days after Brad Raffensperger's office received the email notifying them of Pro V&V not being certified; when the document was opened in PhotoShop, artifacts revealed the 'Pro V&V letterhead' was cut and pasted and not one image; the Pro V&V address was misspelled and there was no phone number or email address (these items are required per the VSTL Program Manual Section 3.4.1.6); the address used for the EAC on the 'Letter' changed in 2013, well before the supposed date of the 'Letter'.

21. Based on the metadata and PhotoShop artifacts, it appears Jerome Lovato of the EAC and not Jack Cobb of Pro V&V 'authored' this 'Pro V&V Letter of Agreement.pdf' on September 17, 2019. EAC officials have gone to great lengths to fraudulently represent documents and give a false account of laws, rules and regulations, in order to misrepresent Pro V&V's accreditation status. This is in clear violation of the Help America Vote Act ("HAVA") of 2002 (52 USC 20901 to 21145), it may also be a violation of 18 USC 1512 - *conduct intended to illegitimately affect the presentation of evidence in a Federal proceeding*, since this document seems to have been created due to the question posed by the Plaintiff's attorney during the *Curling v. Raffensperger* lawsuit. This presents another avenue that requires investigation.

22. The EAC continues in their attempt to propagate misleading interpretations of the laws, regulations and guidelines associated with VSTL

accreditation processes. Currently posted on the EAC website is this explanation as to Pro V&V's missing documentation and certifications required for February 24, 2017 to 2019 and February 24, 2019 to 2021, *"Pro V&V was accredited by the EAC on February 24, 2015. Federal law provides that EAC accreditation of a VSTL cannot be revoked unless the EAC Commissioners vote to revoke the accreditation."* . This regulation has nothing to do with the fact that the Pro V&V accreditation expired. VSTL Program Manual, Version 1, effective July 2008 and Version 2, effective May 2015 Section 3.8 reads – Expiration and Renewal of Accreditation. - *A grant of accreditation is valid for a period not to exceed two years. A VSTL's accreditation expires on the date annotated on the Certificate of Accreditation.* Therefore, the Pro V&V accreditation legally expired two years after issuance as is set forth by the EAC VSTL guidelines. There are no documents archived for Pro V&V between the dates of 02/24/2015 and 01/27/2021 as is shown on the EAC website (Ex. A3).

23. The VSTL Program Manual Section 3.6.2. reads - Post Information on Web Site. - *The Program Director shall make information pertaining to each accredited laboratory available to the public on EAC's Web site. This information shall include (but is not limited to): 3.6.2.1. NIST's Recommendation Letter; 3.6.2.2. The VSTL's Letter of Agreement; 3.6.2.3. The VSTL's Certification of Conditions and Practices; 3.6.2.4. The Commissioner's Decision on Accreditation; and 3.6.2.5. The Certificate of Accreditation. None of*

these documents are posted on the EAC website for Pro V&V between the dates of 02/24/2015 and 02/01/2021. Therefore, Pro V&V was not an accredited VSTL, nor could have legally certified the ICX systems, at the time Brad Raffensperger negotiated for, purchased or held elections on the Dominion ICX voting systems. The current certificate is also illegal based on VSTL Program Manual Guidelines.

24. Pro V&V does not seem an innocent victim in this alleged document contrivance perpetrated by the EAC. Pro V&V, knowing they had not sent their application package for re-accreditation within the time allowed by law, still led the People of GA and America to believe they were accredited. Jack Cobb, Laboratory Director of Pro V&V, characterized this company as accredited through the EAC, testified, and provided affidavits, during the *Curling v. Raffensperger* action stating, "*Georgia certified the Dominion Voting's Democracy Suite 5.5-A in August 2019. Pro V&V did not test this specific version of the voting system for the EAC, but had previously engaged in testing the baseline system (D-Suite 5.5),*" (Doc. 821-6 at 3-4.). This testimony is more evidence that Pro V&V did not certify the actual version being used in GA. Their actions of continuing to illegally certify voting systems, and self-promotion of being EAC accredited would seem to portray their complicity in this scheme.

25. The lack of EAC accreditation was brought to the attention of Jack Cobb (Ryan Jackson Cobb) by a letter sent to him on October 31, 2017 by US Senator

Ron Wyden (KS). This letter advised Cobb of the importance of being certified and pointed out to him the last EAC certificate issued to Pro V&V had expired on February 24, 2017. US Senate Majority Leader Mitch McConnell was also informed on or about October of 2017, via a sworn affidavit, that the elections of 2017 may be null and void due to the lack of EAC certifications (Ex. D).

26. During the *Curling v. Raffensperger* lawsuit Judge Totenberg stated, “*Mr. Cobb represented in his affidavits filed by Defendants that the Dominion system’s security was fortified by the encryption of the QR code and accompanying digital signature code as well as various other security measures such as use of a built in security feature that generates SHA-256 hash values.*” (Doc. 821-6 at 4.) Interesting that Mr. Cobb attested to, and supposedly tested the fact that the QR codes are fortified by encryption since Dominion has since admitted that the QR codes are *not* encrypted and that they had no plans to encrypt them. Judge Totenberg stated, “*The evidence plainly contradicts any contention that the QR codes or digital signatures are encrypted here, as ultimately conceded by Mr. Cobb and expressly acknowledged later by Dr. Coomer during his testimony.*” (Tr. Vol. II at 123, 146, 237, 243.) These outright lies, under oath, in a federal proceeding are not only chargeable offenses, but should have nullified any and all testimony provided by Cobb.

27. During the *Curling v. Raffensperger* action, Mr. Cobb's first affidavit discloses that Pro V&V did not itself conduct any form of penetration or security testing of the 5.5-A software version specifically to be used in Georgia but relied on another company's security testing of earlier versions of the Dominion Democracy Suite software (*Doc. 865-1 at 5; Tr. Vol. II, at 233.*) Eric Coomer, an officer of Dominion, testified that there is a difference between the 5.5 and 5.5-A Dominion Democracy Suite versions – a change to the ICX software that was not deemed de minimis (*Tr. Vol. II at 138.*). This adds to the overwhelming evidence that the current ICX voting system was not, in fact, certified prior to purchase and use and that Pro V&V, Dominion and Raffensperger all seemed aware of this fact.

28. Brad Raffensperger, being the state official in charge of elections, was responsible for ensuring Pro V&V was legally able to certify the ICX system prior to spending \$107 million taxpayer dollars. The contract for the ICX voting system should have been canceled by Brad Raffensperger no later than September 11, 2019. When his office was informed that Pro V&V may not be accredited by the opposition's attorney in a federal proceeding, Raffensperger should have done his duty and with due diligence confirmed the accreditation status of Pro V&V by this time. In fact, Raffensperger signed certifications and affixed the Great Seal of GA to them, testifying that the electronic voting systems used in GA had been inspected and certified for use since February of 2019 (Ex.

E), even though the Pro V&V accreditation had expired in February 2017. This is a complete failure of due diligence and alleges a glaring example of malfeasance of office and a violation of 52 USC 10307(d). The SoS should have been well aware of Pro V&V's lack of accreditation before affixing his signature and Seal to these documents.

29. Brad Raffensperger attested to the fact that he retained Pro V&V during the *Curling v. Raffensperger* action. Judge Totenberg stated, "*The Secretary of State retained Pro V&V to perform a review of its newly adopted BMD voting system, as required for EAC certification purposes, for submission to the EAC for approval. Pro V&V originally certified the Dominion Voting's Democracy Suite 5.5-A system in August 2019 and has certified a modified version since that time – once in November 26, 2019 and once on October 2, 2020.*" At no time during these supposed reviews was Pro V&V legally accredited to 'review' or certify the SoS's new voting system.

30. Perhaps SoS Raffensperger's most egregious failure of duty to his office, the People of GA, and his Oath was the lack of investigation into the fact that GEMS (Global Election Management System), was manifested from SOE (Standard Operating Environment) software that was purchased by SCYTL (provider of electronic voting systems located in Barcelona, Spain) developers that runs on ALL election machines that now operate. This software now runs under the name of DOMINION. Akamai Technologies services SCYTL. Akamai

Technologies houses all State government sites as well as all Foreign government sites. Akamai Technologies has locations throughout the world including China and Iran. The GEMS (now flagged DOMINION) system connects ALL Akamai locations together. Akamai Technologies merged with UNICOM (Chinese Telecom) in 2018. Akamai Technologies makes the COTS (Commercial off-the-shelf products) for the Dominion ICX voting system. This allows for access by foreign entities into our voting systems, via the Akamai servers, since all State and Foreign governments are on the same system. It utilizes servers that are owned and operated by China and allows for internet connectivity and foreign interference of our elections (Ex. D).

31. GA uses SCYTL during elections to mix/shuffle our votes for anonymity'. The Dominion Software Election Management System sends the votes to SCYTL where this occurs, then sends those totals back to the SoS and to the AP (Associated Press). When this mixing/shuffling occurs, there is no ability to know that the vote coming out on the other end is actually the vote that was cast. Therefore, this creates zero integrity of the votes. These procedures are explained in detail in a published paper from University College London (Ex. D section 47 – 63).

32. On September 12, 2022 an Official Complaint was filed with the State Board of Elections (Ex. C) detailing some of the above allegations. In addition to the previously stated facts, this Complaint not only details additional proof of

the lack of official certification of GA's electronic voting system by the EAC but also contains evidence of alleged document tampering by officials of the EAC.

33. The unreadable QR code that prints on the ballot as part of the Dominion ICX voting system was declared noncompliant with GA election law by Judge Totenberg in *Curling v. Raffensperger*, Case 1:17-cv-02989-AT, 493 F. Supp 3d 1264 (2020). The QR code is in violation of O.C.G.A. 21-2-300(a)(2) which reads - *...however, that such electronic ballot markers shall produce paper ballots which are marked with the elector's choices in a format readable by the elector*. The use of ballots with human unreadable QR codes are in violation of the laws of GA. SoS Raffensperger was told this in 2020 by Judge Totenberg. He, obviously, completely ignored this revelation and has no respect for the laws of GA. Therefore, the use of this ICX voting system should be immediately discontinued by the SoS and all county BoE's.

34. O.C.G.A. 21-2-365(8) - Requirements for use of optical scanning voting systems - *No optical scanning voting system shall be adopted or used unless it shall, at the time, satisfy the following requirements: It shall, when properly operated, record correctly and accurately every vote cast*. During the *Curling v. Raffensperger* action, testimony and declaration by J. Alex Halderman (Ex. F) disclosed that vote stealing malware would not be detectable by any of the defenses the SoS, Pro V&V or Dominion purports to practice. He describes how malware defeats the QR code authentication, logic and accuracy testing, on

screen hash validation, and external APK validation which was used after the November 2020 election. The SoS representatives did not dispute nor address this issue.

35. Further, a poll worker in Williamson county TN kept track of the number of ballots being fed into an ICX tabulator on a notepad. At the end of the evening her count was 187. The tabulator count was 39. This 'anomaly' occurred on 7 of 18 ICX tabulators in that precinct. The difference of the vote count issue was reported to the TN SoS who informed the EAC that an investigation was being initiated. The EAC also initiated a formal investigation into this 'anomaly'. The EAC stated in their report at the conclusion of their investigation that, "the root cause of the anomaly was not determined." Pro V&V and Dominion staff were involved in this investigation.

36. Audit log information showed the 'anomaly' manifested from a "QR code signature mismatch" and a warning message that read, "Ballot format or id is unrecognizable" indicating a QR code misread occurred. This caused the ballots to be rejected. In the EAC's conclusion of the formal investigation they admit that a direct cause of the 'anomaly' was inconclusive (Ex. G). The EAC determined the ImageCast Precinct ("ICP") scanner, "mistakenly interprets a bit in the code that marks the ballot as provisional". This is not in conformity with O.C.G.A. 21-2-365(8). The machine was operated properly yet it did not record correctly and accurately every vote cast.

37. The QR code misreads would not have been caught without the presence of mind of the poll worker that was keeping track of the ballots. The ICX tabulators do not notify the poll workers of rejected ballots. The cause of the 'anomaly' was never found though, the EAC, Pro V&V and Dominion say it was fixed. Reading the report issued by the EAC, it seems that the way this issue was 'fixed' was to do a software update that resets the 'provisional ballot flag' after each ballot. In other words, the QR code misread was not actually fixed, they just allow the ballots to be rejected one at a time versus in batches.

38. The aforementioned QR code issues defeat Eric Coomer's testimony, as a witness for the defense, during the *Curling v Ruffensperger* case. Coomer's testimony as a response to State Defendants' question regarding what would be necessary to generate a valid (but false) QR code accepted by the ICP scanner, *Dr. Coomer discussed how all physical and software defenses of the system would have to be defeated and source code accessed, which his testimony as a whole suggests he did not think likely (Tr. Vol. II. At 124.)*. This would indicate that all physical and software defenses of the ICX system were, in fact, defeated and the source code accessed. Proving, once again, that this system is not safe, nor does it accurately count every vote cast.

39. The Voluntary Voting Systems Guidelines ("VVSG") issued by the EAC states - ***External Network Connections*** - *VVSG 2.0 does not permit devices or components using external network connections to be part of the voting*

system. There are significant security concerns introduced when networked devices are then connected to the voting system. This connectivity provides an access path to the voting system through the Internet and thus an attack can be orchestrated from anywhere in the world (e.g., nation state attacks). The external network connection leaves the voting system vulnerable to attacks, regardless of whether the connection is only for a limited period or if it is continuously connected. GA Rule 590-8-1-.01. (d)(1) reads - **Certification of Voting Systems** - the Qualification tests shall comply with the specifications of the Voting Systems Standards published by the EAC. Therefore, these voting systems cannot be able to connect, or have external network connections.

40. Spekin Forensics LLC was retained by Fulton County PA to acquire forensic images of hard drives of the county's Dominion ICX voting system. This is essentially the same exact voting system used across GA. Spekin's final report, issued September 15, 2022 (Ex. H), is being used as evidence in *County of Fulton v. Dominion Voting Systems, Inc.* filed September 21, 2022, in the 39th Judicial District Court. Spekin's forensic audit of the Dominion hard drives revealed substantial changes to the drives. Spekin's saw the inclusion of over 900 .dll files and links created since the date of install. They stated, "This .dll additional pathway is a security breach because of the introduction of an unauthorized script."

41. Speckin's report disclosed, *"The Adjudication Workstation has a python script installed after the certification date of the system."*, and *"This python script can exploit and create any number of vulnerabilities including, external access to the system, data export of the tabulations, or introduction of other metrics not part of or allowed by the certification process."* Python is a high level programming language that does not run natively on a Windows platform. For this to be installed with the functionality listed in this audit, the framework to run Python had to be intentionally installed with the script itself. Speckin's determined, as expected, that each of the drives are interconnected in a system to one another. Therefore, unauthorized access on any one device, allows unauthorized access to any device connected to the network of devices. Since all election systems in the US are interconnected via the Akamai servers, Python allows for access to the entirety of US elections. This also proves, without a doubt, that this Dominion ICX system connects to the internet, making this system illegal both by the standards of the EAC and GA law.

42. Speckin's report disclosed, *"An external IP address that is associated with Canada is found on the Adjudication. This shows that at least one of the network devices has connected to an external device on an external network. This is the same device that the post certification python script is found."* This not only proves external internet connectivity but also indicates foreign interference in our elections.

43. The petitioner nor the People of Cherokee County ever voted, to move from paper ballots to machine voting, via referendum, as is required by GA law. O.C.G.A. 21-2-321 (a), (c) and (f) read - **a)** *The governing authority of any municipality which conducts elections by paper ballot may, upon its own motion, submit to the electors of the municipality, at any election, the question: "Shall voting machines be used in _____ ?"* **c)** *The governing authority **shall** cause such question to be printed upon the ballots to be used at the election in the form and manner provided by the laws governing general elections. (emphasis added)* **f)** *If a majority of the electors voting on such question or questions shall vote in the affirmative, the governing authority of such municipality shall purchase, lease, or rent voting machines, conforming to the requirements of this part, for recording and computing the vote at all elections held in such municipality.* Therefore, voting machines were installed illegally in Cherokee County.

44. The petitioner nor the People of Cherokee County ever voted to increase the indebtedness of the county, nor taxes, via referendum, as is required by GA law. O.C.G.A. 21-2-321(e) reads - *Whenever, under this Code section, the question of the adoption of voting machines is about to be submitted to the electors of any municipality, it shall be the duty of the governing authority of such municipality to ascertain whether current funds will be available to pay for such machines, if adopted and purchased, or whether it has power to*

increase the indebtedness of the municipality in an amount sufficient to pay for the machines without the consent of the electors; and, if such current funds will not be available and the power to increase the indebtedness of the municipality in a sufficient amount without the consent of the electors is lacking, it shall be the duty of the governing authority to submit to the electors of the municipality, in the manner provided by law, at the same election at which the adoption of voting machines is to be voted on, the question of whether the indebtedness of such municipality shall be increased, in an amount specified by them, sufficient to pay for such voting machines, if adopted. Therefore, any increase to the indebtedness of Cherokee County, due to moving from paper ballots, was done so illegally and unconstitutionally based on the GA constitution's Home Rule (Art. IX, Section V).

45. The opinion of the Attorney General as to O.C.G.A. 21-2-321 reads - *The question of whether to authorize the use of voting machines in a county and the question of whether the indebtedness of the county should be increased sufficiently to pay for voting machines should be separately placed on the ballot and may not be combined (1984 Op. Att'y Gen. No. 84-75.).* This clears up any questions regarding whether O.C.G.A. 21-2-321 applies to counties.

46. O.C.G.A. 21-2-290 reads - *The superintendent shall provide, for each precinct in which a primary or election is to be held, a sufficient number of ballots equal to the number of active registered electors.* Therefore, the move

from the illegal ICX voting system would not cause additional expense nor hardship to the county BoE and would save the taxpayers tens of thousands of dollars in each county.

47. O.C.G.A. 21-2-281 reads - *In any primary or election in which the use of voting equipment is impossible or impracticable, for the reasons set out in Code Section 21-2-334, the primary or election may be conducted by paper ballot in the manner provided in Code Section 21-2-334.* O.C.G.A. 21-2-334 reads - *If a method of nomination or election for any candidate or office, or of voting on any question is prescribed by law, in which the use of voting machines is not possible or practicable, or in case, at any primary or election, the number of candidates seeking nomination or nominated for any office renders the use of voting machines for such office at such primary or election impracticable, **or if, for any other reason, at any primary or election the use of voting machines wholly or in part is not practicable, the superintendent may arrange to have the voting for such candidates or offices or for such questions conducted by paper ballots.** In such cases, paper ballots shall be printed for such candidates, offices, or questions, and the primary or election shall be conducted by the poll officers, and the ballots shall be counted and return thereof made in the manner required by law for such nominations, offices, or questions, insofar as paper ballots are used (emphasis added).*

48. GA law is clear. BoE supervisors have the authority to change to paper ballots 'for any other reason'. O.C.G.A. 21-2-70(4) reads – To **select and equip** polling places for use in primaries and elections in accordance with this chapter (emphasis added). The threats and strong arm tactics being utilized by the GA SoS and various county attorneys are illegal. Also, in *Pearson v. Kemp*, No. 1:20-cv-4809-TCB, defendant's counsel argued, "*the Secretary of State has no lawful authority over county election officials*", citing *Jacobson v. Florida Secretary of State*, 974 F.3d 1236, 1256-58 (11th Cir. 2020). SoS Raffensperger was also a defendant in the *Pearson v. Kemp* action (Ex. I).

49. On May 27, 2022, Ryan Germany, General Counsel SoS office, sent a memo to County Election Officials and County Registrars (Ex. K). In this memo he threatened the aforementioned officials with felony charges. In the first paragraph of this memo Germany states, "Physical ballots are not subject to public disclosure and Georgia courts have held that such documents are by law prohibited from being open to inspection by the general public.". This is a lie. O.C.G.A. 50-18-71 reads – a) All public records shall be open for personal inspection and copying, except those which by order of a court of this state or by law are specifically exempted from disclosure. O.C.G.A. 50-18-72 provides this list and ballots are NOT exempt. The court case being referenced, *Smith v. DeKalb County*, 288 Ga. App. 574 (2007), DID NOT apply to ballots, it applied to a CD-ROM that contained proprietary information. Germany lied about this

as well and interjected his own commentary into this case law by including the phrase (such as ballots) in an attempt to intimidate election officials. This is another attempt at covering up the fraud or a voting system rife with errors.

CONCLUSION

50. The election laws, rules and regulations in GA are clear, O.C.G.A. 21-2-300(a)(2) and (3), 21-321(a), (c) and (e), 21-2-365(8), are all being violated by Cherokee County BoE and Brad Raffensperger. These violations render the acquisition and use of this Dominion ICX voting system illegal and therefore, the use of this voting system should be immediately discontinued.

51. The right to vote is fundamental, and is protected by both the due process and equal protection guarantees of the Fourteenth Amendment of the US Constitution and Article I, Section I, Paragraphs I, II, and VII of the GA Constitution (FN 4 & 6). The definition of voting includes all actions necessary to make a vote effective in any primary, special, or general election, including, casting a ballot, and having such ballot counted properly and included in the appropriate totals of votes cast with respect to candidates for public or party office and propositions for which votes are received in an election (FN 3). The petitioner and the People of Cherokee County have no idea if their votes are being recorded accurately. This was proved during the GA mid-terms.

52. DeKalb County Commissioner District 2 candidate Michelle Long Spears said that during the primary, May 24, some precincts were reporting she received zero votes – including her own precinct. Dekalb county agreed to a hand count of ballots and determined a “display error” is to blame for the discrepancies. DeKalb Commissioner Ted Terry stated he believed the voting process is to blame.

53. GA’s voting system allocated 3,317 votes to a Fulton County School Board District 7 candidate who was not even on the ballot. This was blamed on a candidate alignment mismatch in the ballot definitions between BMD’s and scanner/tabulators. This is an impossibility. There was over a 1,300 vote difference between the voting system total votes cast and the hand count audit votes cast. This total vote discrepancy has nothing to do with a ballot definition alignment. The current Dominion system simply failed to count those votes regardless of how the candidates are aligned (Ex. L). The QR code is supposed to develop based on a voter’s actual choices. Obviously, that is not what is happening.

54. An audit monitoring team during the Cobb County Vinings cityhood hand count audit proved the Dominion ICX voting system software magically attributed 15% more votes to SoS Raffensperger during the midterms. The team monitored a majority of those election day ballots in the Vinings 04 precinct that were being hand counted. The monitoring team decided to count the votes of

incumbent SoS Raffensperger while the cityhood count was in progress. The team found that Raffensperger received about 53% of the Republican election day votes for SoS in that precinct, though the Dominion voting system awarded Raffensperger 68.4% of those same votes. Therefore, the Dominion software attributed 15% more votes to Raffensperger's totals than the actual ballots seem to show when the monitors hand counted Raffensperger's votes.

55. Based on the foregoing allegations and information provided in this action, no one can guarantee the petitioner nor the People's of GA votes are being counted as cast. This is a violation of the Fourteenth and Twenty Sixth Amendment of the US Constitution, our right to vote (FN 3) is being denied, impaired and adversely affected (FN 4) due to this ICX voting system and the actions taken, or not taken, by Brad Raffensperger and the Cherokee County BoE.

56. Petitioner has standing in that they have proven the injuries suffered are of a legal and constitutionally protected interest. Petitioner's injuries were caused by the unconstitutional and illegal actions of the defendants in their continued use of a voting system that is non-compliant with GA law, an unconstitutional abridgment of voting rights, and in violation of Article IX of the GA Constitution. Petitioner's redress is declaratory judgment and injunctive relief for unconstitutional procedures, illegally imposed rules and regulations used by defendants, under color of law, which has caused gross harm and

injurious deprivation of the plaintiff's and the People's of Cherokee County rights. that are protected by the Constitution(s) and the laws of GA.

57. Brad Raffensperger, in his official capacity as the GA SoS, seems to have disregarded many state and federal laws. The many and varied allegations set forth in this action include: O.C.G.A.: 16-10-1 – *Violation of Oath of a Public Officer*; 16-10-8 – *False official certificates or writings by officers or employees of state and political subdivisions*; 16-9-53 – *Damaging, destroying, or secreting property to defraud another*; 16-10-20 – *False statements and writings, concealment of facts, and fraudulent documents in matters within jurisdiction of state or political subdivisions*; 16-10-20.1 – *Filing false documents*; 16-8-3 – *Theft by deception*; 16-2-20 – *Party to a crime*; 45-10-3(1), (8) – *Code of Ethics*; 45-11-1 – *Offenses involving public records*; 45-11-4 – *Malfeasance of Office*; 21-2-562 – *Fraudulent entries*; 21-2-596 – *Failure of public or political officer to perform duty*; 21-2-603 – *Conspiracy to commit election fraud*; 18 USC 1512 - *conduct intended to illegitimately affect the presentation of evidence in a Federal proceeding*; 52 USC 10307(d); 52 USC 10308(b) and (c).

PRAYER FOR RELIEF

WHEREFORE, petitioner requests the following relief,

I. That, this honorable court grant the utilization of the illegal Dominion ICX voting systems in Cherokee County and GA to be immediately discontinued.

II. That, this honorable court grant a referendum vote for electors of Cherokee County to decide on the use of voting machines, as is required by law, prior to any further machine voting. And that, this referendum vote needs to be done by hand marked, paper ballots as this would have been the process if the law would have been followed prior to their installation.

III. That, this honorable court grant a referendum vote for electors of Cherokee County to decide whether to increase the debt and/or taxes in Cherokee County, as is required by law, in order to pay for voting machines needs done prior to any further use. And that, this referendum vote needs to be done by hand marked, paper ballots as this would have been the process if the law would have been followed prior to their installation.

IV. That, this honorable court grant the use of any electronic voter registration verification devices be immediately discontinued since these devices allow for network-wide internet intrusions.

V. That, this honorable court grant the indefinite preservation of all 2020, 2021 and 2022 election documents, written or electronic, until a full investigation into the aforementioned allegations can be completed.

VI. That, based on the scanning errors discovered in the midterm election, and the lack of certification of the Dominion ICX voting system since 2017, this honorable court grant a complete hand recount of the actual paper ballots cast, not the machine created re-prints, to be done immediately without the use of

scanners/tabulators for all elections held on the Dominion ICX voting systems since 2020.

VII. That, this honorable Court, in the event the Dominion ICX voting system is used for any future election, require a hand recount of the actual ballots cast, not the machine created re-prints, prior to polls closing and certification of any election.

VIII. That, the petitioner respectfully requests this honorable court impanel a Grand Jury to investigate the numerous, felonious crimes that seem to have been perpetrated against the People of GA. *Decatur County v. Bainbridge Post Searchlight, Inc.*, 632 SE 2d 113, 117 (2006), *The grand jury presentment process, a judicial proceeding conducted under the supervision of the superior courts, authorizes the grand jury to conduct investigations of allegations of official misconduct and to issue reports which can lead to further criminal or civil proceedings where violations of the public trust are revealed.* The facts disclosed in this action warrant a Grand Jury investigation. The appearance of collusion, fraud, forgery, conspiracy to defraud, conspiracy to commit election fraud, conspiracy to overthrow government, and the additional charges these crimes generally lead to are painfully obvious. This entire procedure and the actions taken by the parties involved reveal violations of the public trust.

IX. That, this honorable Court, rule in favor of the relief of Injunction and Declaratory Judgment based on the merit of this case.

X. That, should this honorable Court decline ruling on the merit of the case, a trial by jury is requested.

XI. That, this honorable Court grant an award of attorney's fees and costs incurred as a result of this action.

Respectfully submitted this 17th day of October, 2022

A handwritten signature in cursive script, appearing to read "Lori Portillo", written over a horizontal line.

By:

Lori Portillo
210 Carmichael Road
Woodstock, GA 30189

RETRIEVED FROM DEMOCRACYDOCKET.COM

FOOTNOTES

1. 52 USC 10307(d) - Falsification or concealment of material facts or giving of false statements in matters within jurisdiction of examiners or hearing officers; penalties

Whoever, in any matter within the jurisdiction of an examiner or hearing officer knowingly and willfully falsifies or conceals a material fact, or makes any false, fictitious, or fraudulent statements or representations, or makes or uses any false writing or document knowing the same to contain any false, fictitious, or fraudulent statement or entry, shall be fined not more than \$10,000 or imprisoned not more than five years, or both.

2. 52 USC 10308(a), (b) and (c) – Civil and criminal sanctions – (a) Depriving or attempting to deprive persons of secured rights – Whoever shall deprive or attempt to deprive any person of any right secured by section 10301, 10302, 10303, 10304, or 10306 of this title or shall violate section 10307(a) of this title, shall be fined not more than \$5,000, or imprisoned not more than five years, or both.

(b) Destroying, defacing, mutilating, or altering ballots or official voting records--Whoever, within a year following an election in a political subdivision in which an observer has been assigned (1) destroys, defaces, mutilates, or otherwise alters the marking of a paper ballot which has been cast in such election, or (2) alters any official record of voting in such election tabulated from a voting machine or otherwise, shall be fined not more than \$5,000, or imprisoned not more than five years, or both.

(c) Conspiring to violate or interfere with secured rights--Whoever conspires to violate the provisions of subsection (a) or (b) of this section, or interferes with any right secured by section 10301, 10302, 10303, 10304, 10306, or 10307(a) of this title shall be fined not more than \$5,000, or imprisoned not more than five years, or both.

3. 52 USC 10310(c) – Definitions

(1) The terms "vote" or "voting" shall include all action necessary to make a vote effective in any primary, special, or general election, including, but not limited to, registration, listing pursuant to this chapter, or other action required by law prerequisite to voting, casting a ballot, and having such ballot counted properly and included in the appropriate totals of votes cast with respect to candidates for public or party office and propositions for which votes are received in an election.

4. The right to vote is clearly fundamental, and is protected by both the due process and equal protection guarantees of U.S. Const., amend. 14. In either case, any alleged infringement of the right to vote must be carefully and meticulously scrutinized, for a state has precious little leeway in making it difficult for citizens to vote. *Duncan v. Poythress*, 515 F. Supp. 327 (N.D. Ga.), *aff'd*, 657 F.2d 691 (5th Cir. 1981)

5. If the right to vote is denied altogether or abridged in a manner which renders the electoral process fundamentally unfair, a violation of due process may be found. *Duncan v. Poythress*, 515 F. Supp. 327 (N.D. Ga.), *aff'd*, 657 F.2d 691 (5th Cir. 1981)

6. The interests encompassed by the right to vote are among the liberties protected against state infringement by the due process guarantee. *Duncan v. Poythress*, 515 F. Supp. 327 (N.D. Ga.), *aff'd*, 657 F.2d 691 (5th Cir. 1981), *cert. dismissed*, 459 U.S. 1012, 103 S. Ct. 368, 74 L. Ed. 2d 504 (1982)

7. <https://www.eac.gov/voting-equipment/manuals-and-forms>

EXHIBIT A

Expired PRO V&V Accreditation Certificate,

RETRIEVED FROM DEMOCRACYDOCKET.COM



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

A handwritten signature in cursive script, likely belonging to the Acting Executive Director, is positioned above the date line.

Date: 2/24/15

Acting Executive Director, U.S. Election Assistance Commission

EAC Lab Code: **1501**

EXHIBIT A1

Current PRO V&V Accreditation Certificate,

RETRIEVED FROM DEMOCRACYDOCKET.COM



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

EXHIBIT A2

Jerome Lovato Memo,

RETRIEVED FROM DEMOCRACYDOCKET.COM



U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

FROM: Jerome Lovato, Voting System Testing and Certification Director

SUBJECT: Pro V&V EAC VSTL Accreditation

DATE: 1/27/2021

Pro V&V has completed all requirements to remain in good standing with the EAC's Testing and Certification program per section 3.8 of the Voting System Test Laboratory Manual, version 2.0:

Expiration and Renewal of Accreditation. A grant of accreditation is valid for a period not to exceed two years. A VSTL's accreditation expires on the date annotated on the Certificate of Accreditation. VSTLs in good standing shall renew their accreditation by submitting an application package to the Program Director, consistent with the procedures of Section 3.4 of this Chapter, no earlier than 60 days before the accreditation expiration date and no later than 30 days before that date. Laboratories that timely file the renewal application package shall retain their accreditation while the review and processing of their application is pending. VSTLs in good standing shall also retain their accreditation should circumstances leave the EAC without a quorum to conduct the vote required under Section 3.5.5.

Due to the outstanding circumstances posed by COVID-19, the renewal process for EAC laboratories has been delayed for an extended period. While this process continues, Pro V&V retains its EAC VSTL accreditation.

EXHIBIT A3

PRO V&V VSTL,

RETRIEVED FROM DEMOCRACYDOCKET.COM



U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

The Voting System Test Laboratory (VSTL) accreditation program is an essential component of the EAC's Voting System Testing and Certification Program. The EAC has made National Institute of Standards and Technology's (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) accreditation a requirement as part of its VSTL accreditation program. NVLAP accreditation is **the primary means by which the EAC ensures that each VSTL meets and continues to meet the technical requirements** of the EAC program. It sets the standards for each VSTL's technical, physical and personnel resources, as well as its testing, management, and quality assurance policies and protocols. NVLAP reviews VSTLs one year after their initial accreditation and biennially thereafter.

The EAC takes additional steps to ensure that laboratory policies are in place regarding compliance management and issues like conflict of interest, record maintenance, and financial stability. It also ensures that the VSTL is willing and capable to work with EAC in its Testing and Certification Program. This is performed by regularly working closely with the labs and performing audits biannually and generating certificates. ¹The VSTL accreditation does not get revoked unless the commission votes to revoke accreditation; and by that same token, EAC generated certificates or lack thereof do not determine the validity of a VSTL's accreditation status.

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.**

The Testing and Certification program has been fully staffed since May 2019, and we are confident that the integrity of the labs and our voting system certification program has remained strong throughout. The lack of generating a new certificate does not indicate that the labs were out of compliance. All certifications during this period remain valid as does the lab accreditation. The quality of our labs' work is closely monitored during certification campaigns. Both Pro V&V and SLI Compliance are NAVLAP accredited laboratories that are assessed against the management and technical requirements published in the International Standard, ISO/IEC 17025:2017.

¹ Pro V&V was accredited by the EAC on February 24, 2015, and SLI Compliance was accredited by the EAC on February 28, 2007. Federal law provides that EAC accreditation of a voting system test **laboratory cannot be revoked unless the EAC Commissioners vote to revoke the accreditation**: "The accreditation of a laboratory for purposes of this section may not be revoked unless the revocation is approved by a vote of the Commission." 52 U.S. Code § 20971(c)(2). The EAC has never voted to revoke the accreditation of Pro V&V. Pro V&V has undergone continuing accreditation assessments and had new accreditation certificate issued on February 1, 2021.

EXHIBIT B

Raffensperger Audit Memo,

RETRIEVED FROM DEMOCRACYDOCKET.COM



Georgia
Secretary of State
Brad Raffensperger



Sign of Foul Play

[Home](#) > [News & Announcements](#) > Secretary Raffensperger Announces Completion of Voting Machine Audit Using Forensic Techniques: No Sign Of Foul Play

November 17th, 2020

(Atlanta) - Secretary of State Brad Raffensperger last week ordered Pro V&V, a U.S. Election Assistance Commission certified testing laboratory, to do an audit of a random sample of machines to confirm no hack or tamper: "Pro V&V found no evidence of the machines being tampered."

"We are glad but not surprised that the audit of the state's voting machines was an unqualified success," said Secretary Raffensperger. "Election security has been a top priority since day one of my administration. We have partnered with the Department of Homeland Security, the Georgia Cyber Center, Georgia Tech security experts, and wide range of other election security experts around the state and country so Georgia voters can be confident that their vote is safe and secure."

Pro V&V, based in Huntsville, Alabama is a U.S. Election Assistance Commission-certified Voting System Test Laboratory (VSTL), meaning the lab is

"qualified to test voting systems to Federal standards."

VSTL certification

is provided for under the Help America Votes Act of 2002. Pro V&V's accreditation by the USEAC was also recommended by the National Institute of Standards and Technology (NIST), the U.S. government's physical science



Georgia
Secretary of State
Brad Raffensperger



for the U.S. and the world.

Pro V&V conducted an audit of a random sample of Dominion Voting Systems voting machines throughout the state using forensic techniques, including equipment from Cobb, Douglas, Floyd, Morgan, Paulding, and Spalding Counties. ICP (precinct ballot scanners), ICX (ballot marking devices), and ICC (central absentee ballot scanners) components were all subject to the audit. In conducting the audit, Pro V&V extracted the software or firmware from the components to check that the only software or firmware on the components was certified for use by the Secretary of State's office. The testing was conducted on a Pro V&V laptop independent of the system.

According to the Pro V&V audit, all of the software and firmware on the sampled machines was verified to be the software and firmware certified for use by the Office of the Secretary of State. Coupled with the risk-limiting audit of all paper ballots relying solely on the printed text of the ballots, these steps confirm the

assessment

of the Cybersecurity and Infrastructure Security Agency that there are no signs of cyber attacks or election hacking.

Georgia is recognized as a national leader in elections. It was the first state in the country to implement the trifecta of automatic voter registration, at least 16 days of early voting (which has been called the "gold standard"), and no-excuse absentee voting. Georgia continues to set records for voter turnout and election participation, seeing the largest increase in average turnout of any other state in the 2018 midterm election and record overall, early, in-person, and absentee-by-mail turnout during the November 2020 elections.

###

EXHIBIT C

Formal Complaint to State of Georgia BoE,

RETRIEVED FROM DEMOCRACYDOCKET.COM

Kevin M. Moncla
824 Lake Grove Drive
Little Elm, TX 75068
469-588-7778
KMoncla@gmail.com

David Cross
4805 Spring Park Circle
Suwanee, GA 30024
678-925-6983
DCross108@protonmail.com

September 12, 2022

Georgia State Election Board
2 MLK Jr. Drive
Suite 802 Floyd West Tower
Atlanta, Georgia 30334

Mr. Matt Mashburn
mmashburn@georgia-elections.com

Dr. Jan Johnston
JJohnstonMD.seb@gmail.com

Mrs. Sara Tindall Ghazal
SaraGhazal.seb@gmail.com

Mr. Edward Lindsey
Edwardlindsey.seb@gmail.com

Ex officio:
Mr. Brad Raffensperger
Secretary of State
214 State Capitol
Atlanta, Georgia 30334

RE: OFFICIAL COMPLAINT

Board Members:

We are submitting this official complaint regarding the circumstances surrounding the official certification of Georgia's electronic voting system by the Elections Assistance Commission (hereinafter "EAC"). Our investigation has uncovered evidence which calls in to question, not only the validity of Georgia's voting system certification, but the accreditation of the Voting System Testing Laboratory, and the credibility of the EAC itself.

While the actions and deficiencies of the EAC are beyond the purview of this board, Georgia law required the purchase of an EAC certified electronic voting system.¹

When the Georgia State legislature passed such a requirement, they did so with the implicit expectation that such an EAC certified voting system would meet standards in accordance with federal law.

Unfortunately, that certification is but an empty shell as the EAC's outdated voting system guidelines, requirements, rules, and methods of measuring compliance as promulgated by federal law have been effectively ignored, circumvented, and dismissed. The EAC has failed to maintain oversight and accreditation of the Voting System Testing Labs as required by the Help America Vote Act (HAVA).² Efforts to conceal this fact have only magnified the damage, perpetuated a fraud upon the American people, and prevented correction or

¹ Ga. Code § 21-2-300 ("(3) The state shall furnish a uniform system of electronic ballot markers and ballot scanners for use in each county as soon as possible. Such equipment shall be certified by the United States Election Assistance Commission prior to purchase, lease, or acquisition.")

² [Help America Vote Act | U.S. Election Assistance Commission](#)

remedy. Specifically:

1. Pro V&V's EAC Voting System Testing Lab Accreditation expired in 2017.
2. EAC officials have falsely misrepresented the accreditation status of Pro V&V and have gone to extraordinary lengths to conceal the fact that Pro V&V's accreditation was expired for an extended period of time.
 - A. Records and analysis strongly suggest that the EAC fabricated documents on behalf of Pro V&V then posted those documents on the EAC website. Seemingly this was done in an effort to make it appear as though the required documents had been timely submitted.
 - B. Following the 2020 General Election, the EAC falsely claimed that the reason Pro V&V's accreditation certificate(s) had not been issued was because of:
 1. Delays caused by COVID-19
 2. Administrative Error
 3. Accreditation wasn't Revoked
3. Georgia's current voting system was not certified in accordance with the Help America Vote Act. The voting system Georgia purchased was not tested by an EAC accredited Voting System Testing Lab as required thereby rendering the EAC certification invalid based upon the established requirements.

BACKGROUND

The issues presented in this complaint are governed by the rules and regulations of the Election Assistance Commission (EAC). The EAC's authority is derived from the Help America Vote Act (HAVA) which was passed by the U.S. Congress in 2002.³ HAVA 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.⁴ The EAC is also charged with establishing those Federal Standards.⁵

³ HAVA is codified at 52 U.S.C. 20901 to 21145

⁴ 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.

⁵ Section 311 of the Help America Vote Act of 2002 (HAVA) requires the U.S. Election Assistance Commission (EAC) to periodically adopt standards for voting systems in the form of Voluntary Voting System Guidelines

From the EAC's website:

HAVA creates new mandatory minimum standards for states to follow in several key areas of election administration. The law provides funding to help states meet these new standards, replace voting systems and improve election administration. HAVA also established the Election Assistance Commission (EAC) to assist the states regarding HAVA compliance and to distribute HAVA funds to the states. EAC is also charged with creating voting system guidelines and operating the federal government's first voting system certification program.

The EAC is responsible for creating voting system testing guidelines which are standards and rules that voting machines must comply with to be certified. The EAC accredits third-party companies to test whether voting systems meet the requirements of the voting system guidelines. These companies are called Voting System Testing Labs (VSTLs). Although this complaint centers on the accreditation of one VSTL, it's important to understand the following facts:

1. **Every** voting machine certified by the EAC used in the United States today has not been tested beyond a 2005 standard (PrePhone).⁶
2. Voting system certification does not include testing for penetration, intrusion or system manipulation (doesn't test if the machines can be used to cheat).⁷
3. The Voting System Testing Labs (VSTLs) responsible for testing the voting systems for the EAC are not paid by the EAC but by the voting system manufacturers (Dominion, ES&S, Hart); therefore, an inherent conflict of interest exists.⁸
4. The VSTLs are not qualified nor are they accredited by the EAC to perform any type of forensic audits of the voting systems like those they were paid to perform in many locales following the 2020 general election (Maricopa, Georgia, Michigan, etc.).⁹
5. There are only 2 VSTLs currently recognized by the EAC; Pro V&V and SLI Compliance.¹⁰

1. PRO V&V'S ACCREDITATION EXPIRED IN 2017

⁶ Certified Voting Systems | U.S. Election Assistance Commission (eac.gov)

⁷ Voluntary Voting System Guidelines | U.S. Election Assistance Commission (eac.gov)

⁸ Frequently Asked Questions | U.S. Election Assistance Commission (eac.gov)

⁹ Chain of Custody Best Practices (eac.gov)

¹⁰ Voting System Test Laboratories (VSTL) | U.S. Election Assistance Commission (eac.gov)

The VSTL Program Manual¹¹ explicitly states:

3.8. Expiration and Renewal of Accreditation. A grant of accreditation is valid for a period not to exceed two years. A VSTL's accreditation expires on the date annotated on the Certificate of Accreditation. VSTLs in good standing shall renew their accreditation by submitting an application package to the Program Director, consistent with the procedures of Section 3.4 of this Chapter, no earlier than 60 days before the accreditation expiration date and no later than 30 days before that date. Laboratories that timely file the renewal application package shall retain their accreditation while the review and processing of their application is pending.

The fact is that Pro V&V was not in good standing. The first Certificate of Accreditation issued to Pro V&V is below:



The Certificate of Accreditation clearly delineates the beginning date of February 24, 2015 and is “Effective Through” February 24, 2017. There are simply no submissions by Pro V&V as required to renew their accreditation (save those filed in 2015) until after the 2020 general election. The fact is that Pro V&V’s accreditation expired on February 24, 2017. Even so, Pro V&V continued as though they remained accredited. It was during this time when Pro V&V tested Dominion’s Democracy Suite 5.5A(G), which was subsequently and erroneously certified by the EAC.

2. EAC FALSELY MISREPRESENTED PRO V&V’S ACCREDITATION

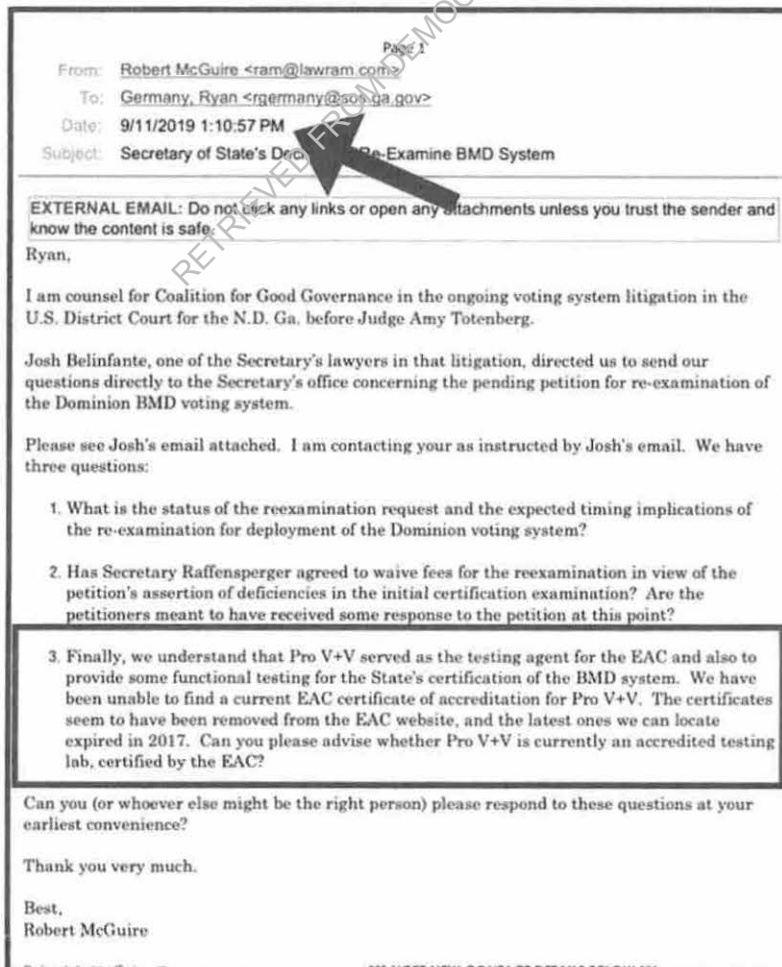
¹¹ VSTL Program Manual, Version 1, effective July 2008, and Version 2, effective May 2015, approved by vote of the EAC Commission

Through a series of fraudulent acts and extraordinary statements, the EAC has engaged in a practice of subterfuge and deceit to conceal the fact that Pro V&V was not an accredited laboratory for an extended period of time.

A. FABRICATION OF DOCUMENTS

On September 11, 2019, an attorney representing the Coalition for Good Governance in a pending federal lawsuit (Curling v. Raffensperger) sent an email to Ryan Germany, General Counsel for the Georgia Secretary of State. The email inquired about the accreditation status of Pro V&V who had tested Georgia's Dominion Democracy Suite 5.5A(G) voting system that the EAC had subsequently certified. Specifically, the email states in part:

"3. Finally, we understand that Pro V+V served as the testing agent for the EAC and also to provide some functional testing for the State's certification of the BMD system. We have been unable to find a current EAC certificate of accreditation for Pro V+V. The certificates seem to have been removed from the EAC website, and the latest ones we can locate expired in 2017. Can you please advise whether Pro V+V is an accredited testing lab, certified by the EAC?"



As Mr. McGuire states in the email above, the EAC website showed only one certificate of accreditation for Pro V&V which was issued in February of 2015 and expired in February of 2017.

A review of Pro V&V's records posted on the EAC's website revealed a document which was not posted until *after* the inquiry noted above. Complainants downloaded the document with the filename "Pro V&V Letter of Agreement.pdf" which is posted below (An electronic copy is also attached for your independent review):

PRO V&V 	<i>Pro V&V, Inc. 700 Boulevards South, Suite 102 Huntsville, AL 35803</i>
---	---

U.S Election Assistance Commission
1201 New York Avenue, N.W.
Suite 300
Washington DC 20005

Attention: Mr. Brian J. Hancock, Director Voting System Certification

Subject: Letter of Agreement for Voting System Test Laboratory Accreditation

Dear Mr. Hancock:

The undersigned representative of Pro V&V, Inc. (hereinafter "Laboratory"), being lawfully authorized to bind Laboratory and having read the EAC Voting System Test Laboratory Program Manual, accepts and agrees on behalf of Laboratory to follow the program requirements as laid out in Chapter 2 of the Manual. Laboratory shall meet all program requirements as they relate to NVLAP accreditation; conflict of interest and prohibited practices; personnel policies; notification of changes; resources; site visits, notice of law suits; testing, technical practices and reporting; laboratory independence; authority to do business in the United States; VSTL communications; financial stability; and recordkeeping. Laboratory further recognizes that meeting these program requirements is a continuing responsibility. Failure to meet each of the requirements may result in the denial of an application for accreditation, a suspension of accreditation or a revocation of accreditation.

Sincerely,

Pro V&V, Inc.

Jack Cobb
Laboratory Director

Pro V&V's "Letter of Agreement" was addressed to Mr. Brian J. Hancock, the former Director of Voting System Certification for the EAC. Interestingly, there is no date nor signature which the rules adopted by the EAC specifically require:

Submission of Documents. Any documents submitted pursuant to the requirements of this Manual shall be submitted:

with a proper signature when required by this Manual. Documents that require an authorized signature may be signed with an electronic representation or image of the signature of an authorized management representative.

3.4.2. Letter of Agreement. The applicant laboratory must submit a signed letter of agreement as part of its application. To that end, applicant laboratories are required to submit a Letter of Application requesting accreditation. The letter shall be addressed to the Testing and Certification Program Director and attach (in either hard copy or on CD/DVD) (1) all required information and documentation; (2) a signed letter of agreement; and (3) a signed certification of conditions and practices.

Due to the suspect circumstances surrounding the document, we decided to view the file's metadata. This shows the document posted on the EAC's website was created six (6) days after the email seeking the status of Pro V&V's accreditation.



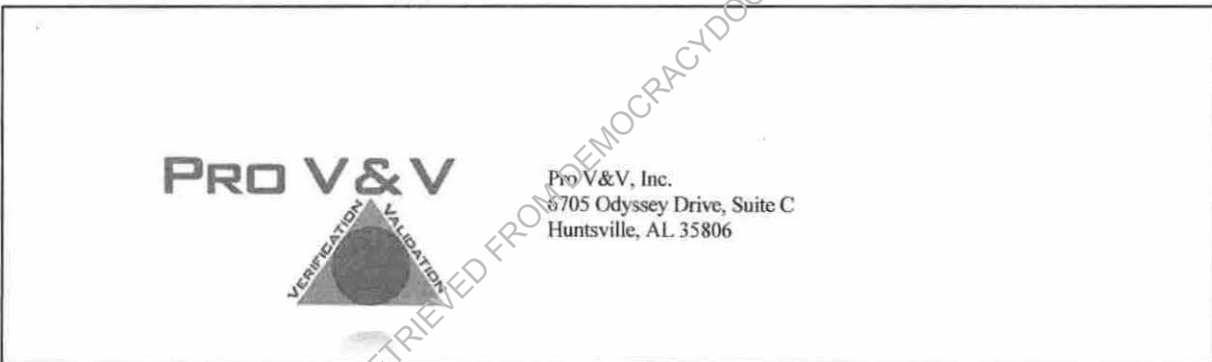
What's more, the Letter of Agreement that Mr. Lovato seemingly created on September 17, 2019, was addressed to Mr. Brian J. Hancock. The problem is that Mr. Hancock had retired in February of 2019, or nearly seven months before the letter was created.

Additionally, the file's metadata shows that the document was not authored by Jack Cobb of Pro V&V, but by the EAC's own Testing and Certification Director, Jerome Lovato. Perhaps there's a good explanation, or at least a plausible one; however, there are other problems. When the document was opened in Photoshop, it revealed that the letterhead was not one image as one would expect, but images that had been cut and pasted:

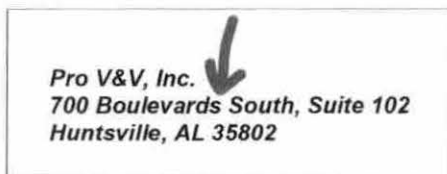
Document Header from the Letter of Agreement added by Jerome Lovato as shown in Adobe Photoshop:



Document Header from the 2020 Letter of Agreement as shown in Adobe Photoshop using the same process:



If the Letter of Agreement was in-fact created by Pro V&V, they didn't include their phone number, email, and misspelled their own address on their "letterhead":



Also, the EAC's address changed from that of the letter (1201 New York Ave, DC) to 1335 East West Highway, MD on October 22, 2013, or before the date to which the letter was attributed.

No matter the provenance of the Letter of Agreement, without a date or signature it fails to meet any acceptable standard. The same is acknowledged by the fact that the document was not publicly posted as required until 6 days after the email cited above inquiring about Pro V&V's accreditation status. Lastly, the EAC never issued a Certificate of Accreditation for 2017 when Pro V&V's 2015 accreditation expired.

B. EAC MISREPRESENTED STATUS OF PRO V&V

After the 2020 General election the EAC went so far as to surreptitiously cover-up the fact that Pro V&V was not accredited and had not been for years. Pro V&V was granted EAC accreditation as a Voting Systems Testing Laboratory (VSTL) on February 24, 2015 and was effective through February 24, 2017. From the Voting System Test Laboratory Program Manual, Version 2.0

3.8 Expiration and Renewal of Accreditation. A grant of accreditation is valid for a period not to exceed two years. A VSTL's accreditation expires on the date annotated on the Certificate of Accreditation. VSTLs in good standing shall renew their accreditation by submitting an application package to the Program Director, consistent with the procedures of Section 3.4 of this Chapter, no earlier than 60 days before the accreditation expiration date and no later than 30 days before that date. Laboratories that timely file the renewal application package shall retain their accreditation while the review and processing of their application is pending. VSTLs in good standing shall also retain their accreditation should circumstances leave the EAC without a quorum to conduct the vote required under Section 3.5.5.

There is no record whatsoever of Pro V&V renewing their accreditation in 2017, despite the requirement that all associated documents *shall* be posted on the EAC's website:

3.6.2. Post Information on Web Site. The Program Director shall make information pertaining to each accredited laboratory available to the public on EAC's Web site. This information shall include (but is not limited to):

- 3.6.2.1. NIST's Recommendation Letter;*
- 3.6.2.2. The VSTL's Letter of Agreement;*
- 3.6.2.3. The VSTL's Certification of Conditions and Practices;*
- 3.6.2.4. The Commissioner's Decision on Accreditation; and 3.6.2.5. The Certificate of Accreditation.*

There is also no record of Pro V&V renewing their accreditation in 2019. It isn't until after the 2020 general election that Pro V&V's accreditation is renewed.

1. PANDEMIC EXCUSE

On January 27, 2021, Jerome Lovato of the EAC issued the following memo attempting to use the pandemic somehow as cause for Pro V&V's "questionable" accreditation status:



U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

FROM: Jerome Lovato, Voting System Testing and Certification Director
SUBJECT: Pro V&V EAC VSTL Accreditation
DATE: 1/27/2021

Pro V&V has completed all requirements to remain in good standing with the EAC's Testing and Certification program per section 3.8 of the Voting System Test Laboratory Manual, version 2.0:

Expiration and Renewal of Accreditation. A grant of accreditation is valid for a period not to exceed two years. A VSTL's accreditation expires on the date annotated on the Certificate of Accreditation. VSTLs in good standing shall renew their accreditation by submitting an application package to the Program Director, consistent with the procedures of Section 3.4 of this Chapter, no earlier than 60 days before the accreditation expiration date and no later than 30 days before that date. Laboratories that timely file the renewal application package shall retain their accreditation while the review and processing of their application is pending. VSTLs in good standing shall also retain their accreditation should circumstances leave the EAC without a quorum to conduct the vote required under Section 3.5.5.

Due to the outstanding circumstances posed by COVID-19, the renewal process for EAC laboratories has been delayed for an extended period. While this process continues, Pro V&V retains its EAC VSTL accreditation.

Lovato states:

Pro V&V has completed all requirements to remain in good standing with the EAC's Testing and Certification program per section 3.8 of the Voting System Test Laboratory Manual, version 2.0:

The statement above is false by any metric. Lovato would have us believe that Pro V&V's accreditation was somehow current despite the required submissions and Certificates of Accreditation missing from the EAC's website (The EAC is required to post the documents). Then Lovato claims that the pandemic is the cause of any accreditation deficiency:

Due to the outstanding circumstances posed by COVID-19, the renewal process for EAC laboratories has been delayed for an extended period. While this process continues, Pro V&V retains its EAC VSTL accreditation.

Interestingly, Lovato specifically names Pro V&V and doesn't mention the other VSTL, SLI

Compliance. Furthermore, the EAC's pandemic excuse is refuted simply by referencing a calendar. Pro V&V's accreditation expired in February of 2017, three years before the pandemic. Even if we were to accept the cryptic, undated and unsigned Letter of Agreement of questionable origin and attribute it to 2017, the accreditation would have expired in 2019, a year before COVID-19 was deemed a national emergency.

2. CLERICAL ERROR EXCUSE

The pandemic excuse is not retroactive to a time before the pandemic, a fact which was evidently brought to the attention of the EAC and what precipitated the release of the next memo (attached hereto as "Exhibit C") which states:

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.

Again, even if we were to accept the highly suspect Letter of Agreement and attribute it to 2017, along with the EAC's explanation of administrative error in failing to issue a Certificate of Accreditation in 2017, the accreditation would have expired in February of 2019 without exception (3.8. *Expiration and Renewal of Accreditation. A grant of accreditation is valid for a period not to exceed two years*). The EAC conveniently ignores the irrefutable fact that Pro V&V is lacking *two* Certificates for Accreditation- one for 2017 and another for 2019. Also missing from the record and the EAC's website are Pro V&V's filings for accreditation renewal for both 2017 and 2019.

3. REVOCATION EXCUSE

In the same memo cited above, Mr. Lovato disingenuously attempts to address the concerns of *expiration* with the prospect of *revocation*. From the memo:

The VSTL accreditation does not get revoked unless the commission votes to revoke accreditation; and by that same token, EAC generated certificates or lack thereof do not determine the validity of a VSTL's accreditation status.

Pro V&V was accredited by the EAC on February 24, 2015, and SLI Compliance was accredited by the EAC on February 28, 2007. Federal law provides that EAC accreditation of a voting system test laboratory cannot be revoked unless the EAC Commissioners vote to revoke the accreditation: "The accreditation of a laboratory for purposes of this section may not be revoked unless the revocation is approved by a vote of the Commission." 52 U.S. Code § 20971(c)(2). The EAC has never voted to revoke the accreditation of Pro V&V. Pro V&V has undergone continuing accreditation assessments and had new accreditation certificate issued on February 1, 2021.

The EAC raises the matter of revocation and that such action requires a "vote of the Commission". It goes on to say "*The EAC has never voted to revoke the accreditation of Pro V&V*". The EAC is conflating the matters of *revocation* with that of *expiration*. Suggesting that simply because the Commission has never voted to revoke Pro V&V's accreditation, then it remains active by default. The prospect defies logic. The term "Expired" is defined as:

Expired- *cease to be valid after a fixed period of time.*

The term "Revocation" is defined as:

Revoked- *put an end to the validity or operation of.*

Expiration is automatic, as in when the term is up. Revocation requires an affirmative act to end something. Like a driver's license can be expired or revoked, the two are different and have different causes and meanings. A driver's license can be expired and therefore invalid without being revoked. Mr. Lovato's assertion is analogous to claiming that your expired driver's license is valid simply because it's not revoked. This rationale is ludicrous. Furthermore, to accept such a prospect would require ignoring the clearly defined prescription of time "...not to exceed two years."

The bright lines of the rules regarding accreditation renewal and expiration are clear; therefore, this is an effort of either deception or ignorance. Considering that Mr. Lovato cites the plain language detailing expiration in his January 21, 2021 memo (above), the possibility of ignorance is removed.

Also removed is a page from the EAC's website with the heading, "Labs with Expired Accreditation" that can be found archived here:

[Voting System Test Laboratories \(VSTL\) - Voting Equipment | US Election Assistance Commission \(archive.org\)](#)

The fact that the category, “Labs with Expired Accreditation” existed on the EAC’s website is damning to Lovato’s assertion as it establishes the EAC’s own acknowledgement that VSTL accreditations do expire *without* revocation. The removal of the page suggests that the EAC realized the same and acted to conceal that which would lift the thin veil of plausible deniability.

What’s more, we know from the email to the Georgia Secretary of State’s general counsel that the Secretary of State and the EAC were both made aware of Pro V&V’s long-expired accreditation over a year before the 2020 general election. Instead of properly addressing the deficiency at the time, the EAC presumably elected to create a fraudulent record on behalf of Pro V&V. Regardless, they knowingly chose to fraudulently misrepresent Pro V&V’s accreditation status and attempted to cover-up the facts with a litany of excuses that just don’t hold water.

3. GEORGIA’S VOTING SYSTEM WAS NEVER PROPERLY CERTIFIED

Pro V&V performed the testing on Georgia’s Dominion Democracy Suite 5.5A(G) system and submitted the final report to the EAC on August 7, 2019. Because Pro V&V’s VSTL accreditation expired in February of 2017 (or February of 2019 if we accept the EAC’s flawed excuses) and system certification requires testing by an EAC accredited VSTL, the EAC certification of Georgia’s voting system is not valid.

SUMMARY

As we mark the EAC’s 20th year, we must acknowledge that the EAC has failed to develop and maintain voting system testing guidelines, failed to oversee the accreditation of testing labs, and failed to test our country’s voting systems to a remotely reasonable standard. The fact is that EAC has miserably failed to perform not only its core mission, but all missions for its entire existence.

The actions of the EAC as detailed herein extend far beyond mere *failure*. The EAC has fabricated a fraudulent record for Pro V&V and has repeatedly, knowingly, and intentionally misrepresented the expired accreditation status of a Voting Systems Testing Laboratory to the American people. The EAC’s deceptive practices have fostered a false sense of security and materially violated their responsibilities under the HAVA in both letter and spirit of the law.

The inherit standard of any established institution or industry does not exist with voting systems in the United States. There is no benchmark, no independent method of testing, no oversight, and therefore there is no alternative but for the States to perform their own due

diligence in testing our voting systems.

Wherefore, the Georgia State Election Board must immediately suspend use of the Dominion voting systems until a thorough, review by a panel of independent experts can be performed.

RETRIEVED FROM DEMOCRACYDOCKET.COM

RETRIEVED FROM DEMOCRACYDOCKET.COM

RETRIEVED FROM DEMOCRACYDOCKET.COM

EXHIBIT D

Tore Maras Affidavit,

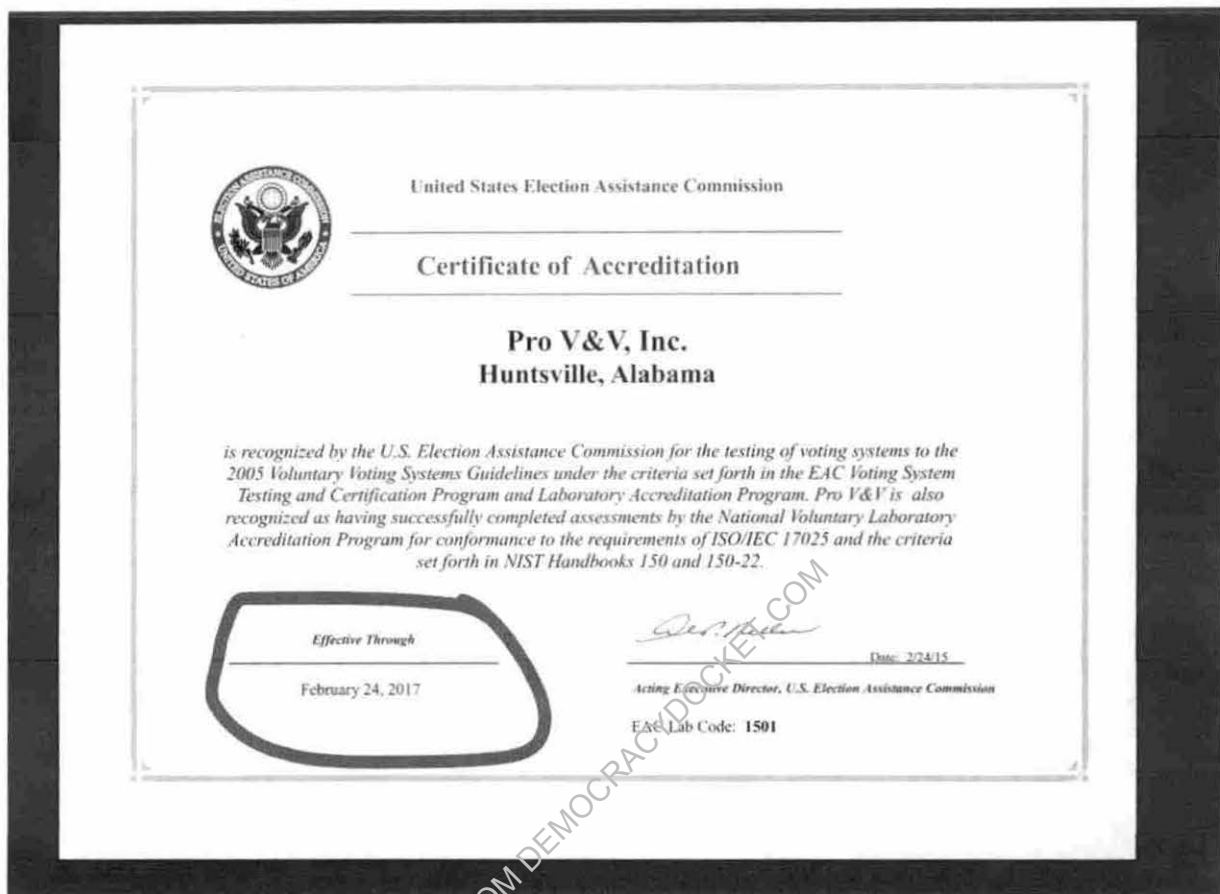
RETRIEVED FROM DEMOCRACYDOCKET.COM

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.



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.

United States Department of Commerce
National Institute of Standards and Technology



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 Communiqué dated January 2009).*

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



[Signature]
For the National Voluntary Laboratory Accreditation Program

10.

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



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



WISCONSIN

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



GEORGIA

<i>State Participation:</i>	Requires Federal Certification. GA requires that its voting systems are tested to EAC standards by EAC accredited labs and certified by the EAC.
<i>Applicable Statute(s):</i>	"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." <u>GA CODE ANN. § 21-2-324</u> (2008).
<i>Applicable Regulation(s):</i>	"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 <i>Voting Systems Standards</i> published by the EAC." <u>GA. COMP. R. & RES. 590-8-1-.01</u> (2009).
<i>State Certification Process:</i>	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. <u>GA. COMP. R. & RES. 590-8-1-.01</u> (2009).
<i>Fielded Voting Systems:</i>	[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)]. http://www.sos.georgia.gov/Elections/



PENNSYLVANIA

<i>State Participation:</i>	Requires Testing by a Federally Accredited Laboratory. PA requires that its voting systems are approved by a federally recognized independent testing laboratory as meeting federal voting system standards.
<i>Applicable Statute(s):</i>	"Any person or corporation owning, manufacturing or selling, or being interested in the manufacture or sale of, any electronic voting system, may request the Secretary of the Commonwealth to examine such system if the voting system has been examined and approved by a federally recognized independent testing authority and if it meets any voting system performance and test standards established by the Federal Government." <u>25 PA. CONS. STAT. ANN. Code § 3031.5</u> (West 2008).
<i>Applicable Regulation(s):</i>	PA does not have a regulation regarding the federal certification process.
<i>State Certification Process:</i>	The Secretary of State examines voting systems, upon request, once the voting systems have received approval by a federally recognized independent testing authority. The person(s) requesting the examination of the voting system are responsible for the cost of the examination. After the examination, the Secretary of State issues a report stating whether or not the voting systems are safe and compliant with state and federal requirements. If the voting systems are deemed safe and compliant by the Secretary of State then the systems may be adopted and approved for use in elections by each county through a majority vote of its qualified electors. <u>25 PA. CONS. STAT. ANN. Code §§ 3031.5, 3031.2</u> (West 2008).
<i>Fielded Voting Systems:</i>	[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



ARIZONA

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

17.

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

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

→ <https://eac-legacy.ei-admin.com/voting-equipment/voting-system-test-laboratories-vsl/>

SEARCH CLEAR

Accredited Labs

2 results found
Page 1 of 1

Pro V&V

700 Broadway South
Suite 102
Huntsville, AL 35892

Status: Accredited

Program Manager: Jack Cobb, President

Phone: 256-713-1111

[Learn More >](#)

SLI Compliance, a Division of Gaming Laboratories International, LLC

4730 Independence Street
Wheat Ridge, CO 80033

Status: Accredited

Program Manager: Tracy Mises, Director of Operations

Phone: 303-421-1500

[Learn More >](#)

Frequently Asked Questions

Manuals and Forms

Test and Certification Blogs

DO YOU HAVE QUESTIONS?

Send your questions to: info@provv.com or call 256-713-1111 to contact us.

[Contact Us](#)
(Link opens in new tab)

REGISTER TO VOTE!

Use the National Mail-In Voter Registration to vote legally and register your vote online with a valid ID.

From if you wish to vote in person you are a political resident a member of family member or a citizen living outside the U.S., contact the National Voting Assistance Program to register to vote.

[Register Today](#)

RETRIEVED FROM DEMOCRACYDOCKET.COM

Not secure | www.provv.com/contact/

Your Name (required)

Your Email (required)

Subject

Your Message

[Send](#)

Pro V&V

6705 Odyssey Drive NW
Suite C
Huntsville, AL 35896

Office: 256-713-1111
Fax: 256-713-1112

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

Close to Testimonial

5:53 PM 11/26/2020

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

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

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

28 046 Madrid

Asian offices

Akamai Technologies - India

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

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

Akamai Technologies - China

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

Telephone: 86-10-8523-3067
Fax: 86-10-8523-3061
Regional Manager: Stuart Spiteri

Akamai Japan K.K.

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

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

Akamai Technologies - Singapore

Akamai - Regus Centre, 36-01 UOB Plaza 1
80 Raffles Place
Singapore 048624
☐ Direct Dial 24/7

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

Akamai Technologies - Australia and New Zealand

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

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

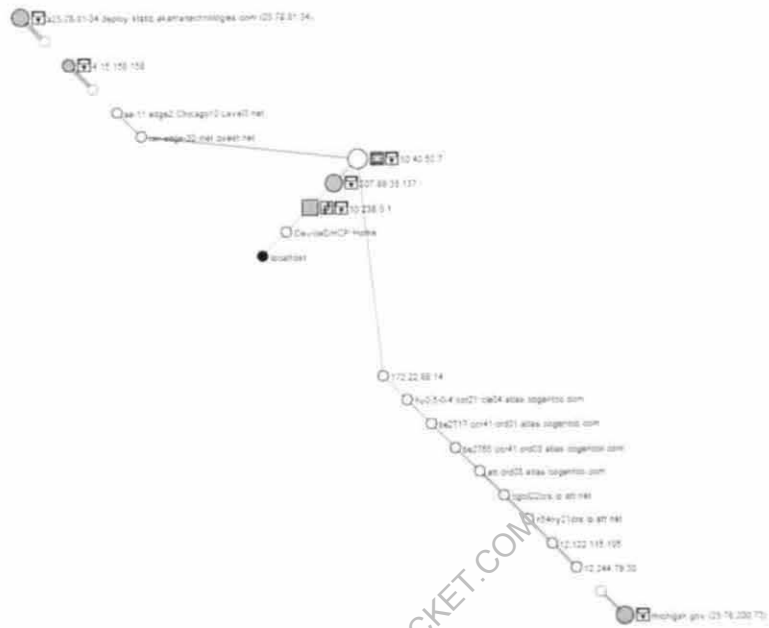
ptf.gov resolves to 4.30.228.74. According to our data this IP address belongs to Level 3 Communications and is located in Alexandria, Virginia, United States. Please have a look at the information provided below for further details

4.30.228.74

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



27. *Brann Mar Park*
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.






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. ScytI, who is contracted with AP that receives the results tallied BY ScytI 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 <small>(Whois Lookup Domain Country Domain To IP)</small> IP Address: 23.78.81.34 <small>(IP Blacklist Check)</small> Reverse DNS: 34.81.78.23.in-addr.arpa Hostname: a23-78-81-34.deploy.static.akamaitechnologies.com a12-67.akam.net >> 184.26.160.67 a11-66.akam.net >> 84.53.139.66 a1-65.akam.net >> 193.108.91.35 Nameservers: a5-66.akam.net >> 95.100.168.66 a18-64.akam.net >> 95.101.36.64 a24-65.akam.net >> 2.16.130.65
	Location For an IP: Michigan.gov
	Continent: North America (NA) Country: United States  (US) Capital: Washington State: Unknown City: Unknown 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: -21600 GMT offset: 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 : 1.4.1 Software and Firmware The software and firmware employed by Dominion D-Suite 5.5-A consists of 2 types, custom and commercial off the shelf (COTS). COTS applications were verified to be pristine or were subjected to source code review for analysis of any modifications and verification of meeting the pertinent standards.
36. The concern is the HARDWARE and the NON – ACCREDITED VSTLs as by their own admittance use COTS.
37. The purpose of VSTL's being accredited and their importance in ensuring that there is no foreign interference/ bad actors accessing the tally data via backdoors in equipment software. The core software used by ALL SCYTL related Election Machine/Software manufacturers ensures "anonymity" .
38. Algorithms within the area of this "shuffling" to maintain anonymity allows for setting values to achieve a desired goal under the guise of "encryption" in the trap-door.
39. The actual use of trapdoor commitments in Bayer-Groth proofs demonstrate the implications for the verifiability factor. This means that no one can SEE what is going on during the process of the "shuffling" therefore even if you deploy an algorithms or manual scripts to fractionalize or distribute pooled votes to achieve the outcome you wish – you cannot prove they are doing it! See STUDY : "[The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system](#)"
40. **Key Terms**
41. **UNIVERSAL VERIFIABILITY:** Votes cast are the votes counted and integrity of the vote is verifiable (the vote was tallied for the candidate selected) . **SCYTL FAILS UNIVERSAL VERIFIABILITY** because no mathematical proofs can determine if any votes have been manipulated.
42. **INDIVIDUAL VERIFIABILITY:** Voter cannot verify if their ballot got correctly counted. Like, if they cast a vote for ABC they want to verify it was ABC. That notion clearly discounts the need for anonymity in the first place.

43. To understand what I observed during the 2020 I will walk you through the process of one ballot cast by a voter.
44. STEP 1 |Config Data | All non e-voting data is sent to ScytI (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.

RETRIEVED FROM DEMOCRACYDOCKET.COM

48.

Background - ElGamal encryption

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

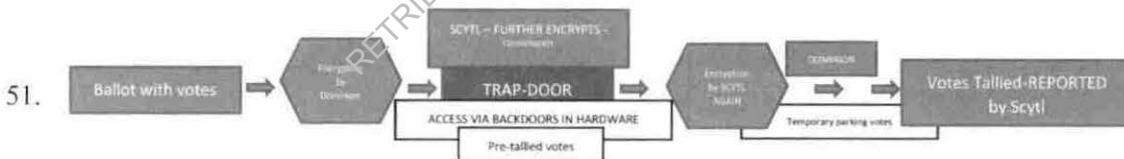
$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(M; R) = \mathcal{E}_{pk}(mM; r + R)$$

- Re-encryption:

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



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



52. The encrypted data is shifted into Scytal'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, Scytal re-encrypts the ballot data that comes in from Dominion (or any other voting software company) as ciphertexts. Scytal 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 Scytal 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)

$$\text{Commitment}_{\text{CRYPT}} = \text{CM}_c$$

Scytl sets commitment - simple math ↓

$$\text{CM}_c(\vec{a}; r) = H \prod_{i=1}^n G_i^{a_i} = 1 \cdot G_i^{a_i}$$

$$\text{CM}_c(\vec{a}; r) = H^r + \sum_{i=1}^n (a_i - z_i) e_i \prod_{j=1}^n H^{z_j e_j}$$

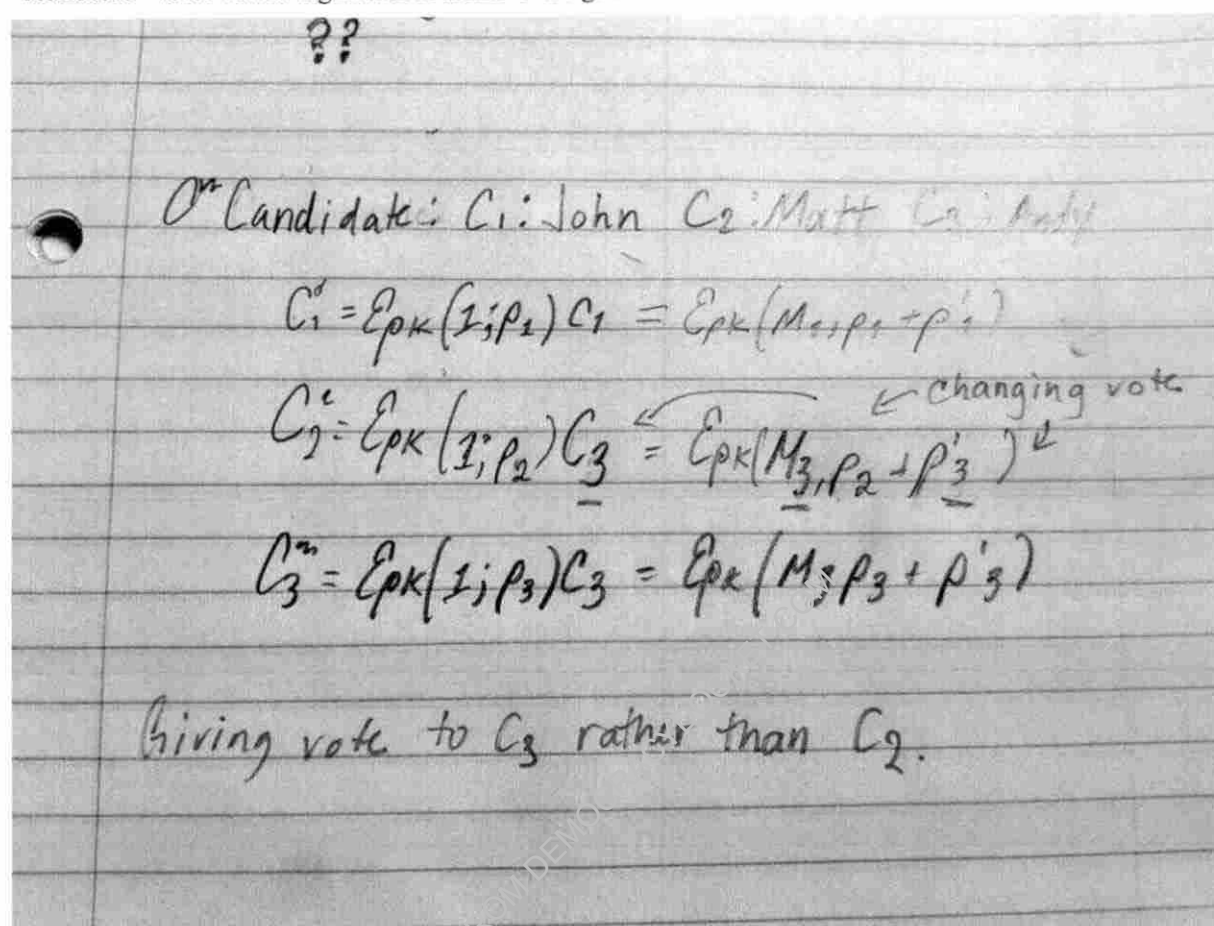
$$\text{CM}_c(\vec{a}; r) = \text{CM}_c(\vec{z}; r')$$

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

56.

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

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

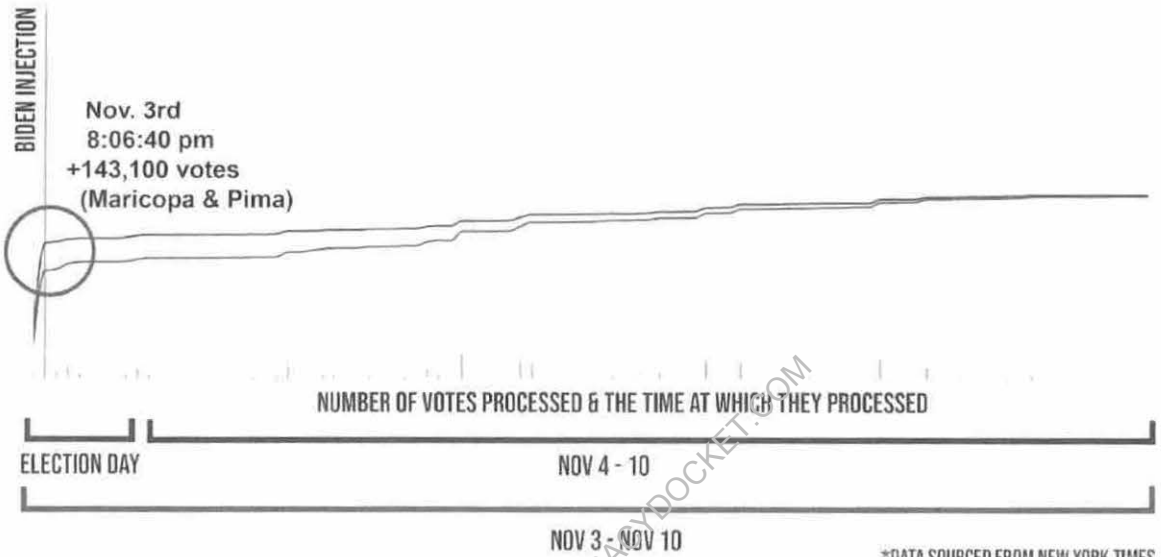


58. STEP 4|Decryption would be the decryption phase and temporary parking of vote tallies before reporting. In this final phase before public release the tallies are released from encrypted format into plain text. As previously explained, those that know the trapdoor can easily change any votes that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

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

ARIZONA

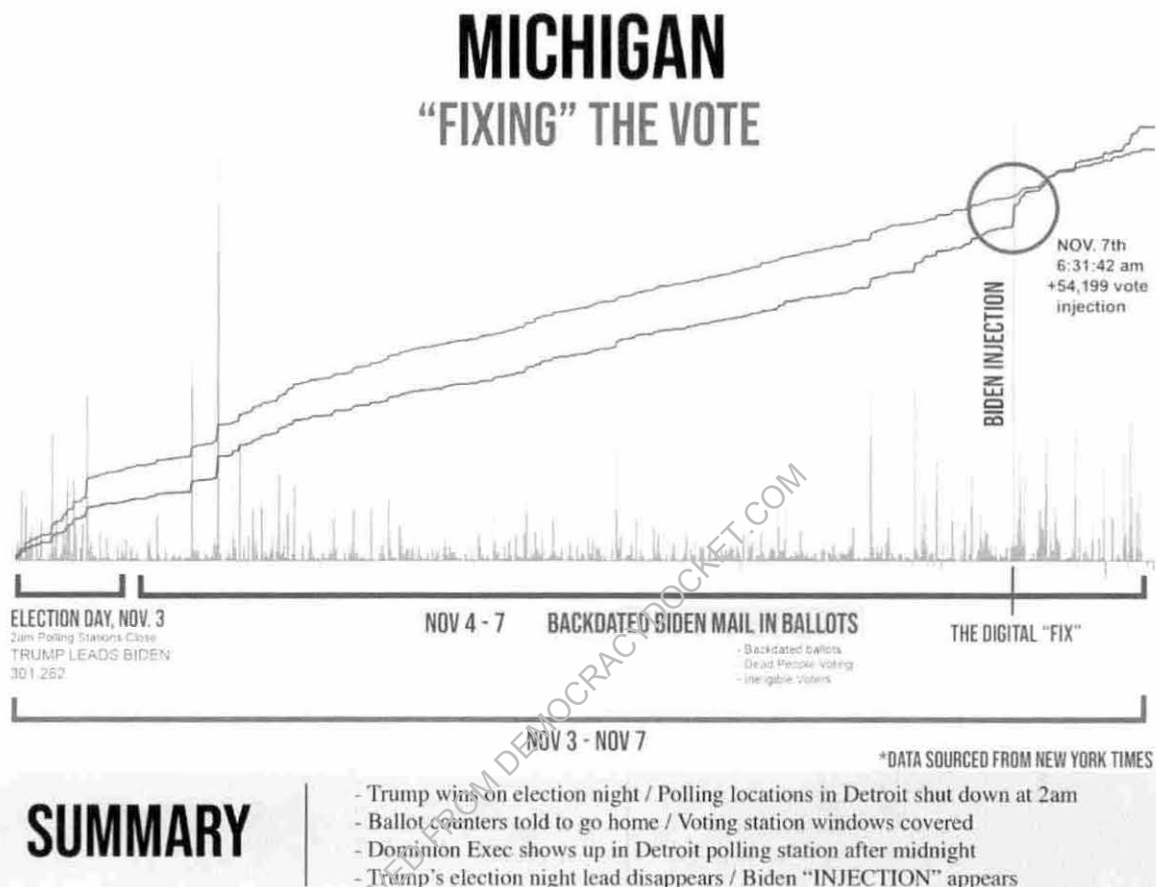
"FIXING" THE VOTE



SUMMARY

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

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



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

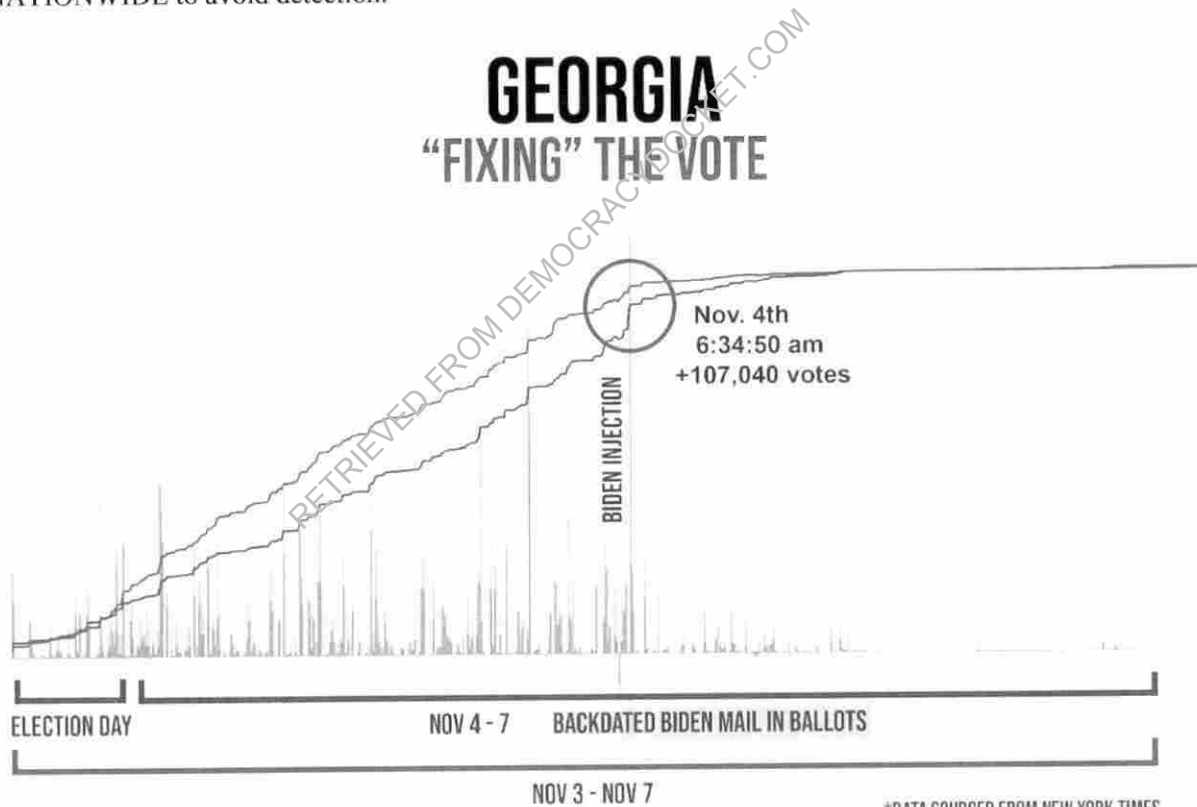
$$\frac{\|U\|_{\infty}}{\|A\|_{\infty}} \leq n^{\frac{1}{2} \log(n)}$$

72.

73. Such a conjecture allows the growth factor the ability to be upper bound by values closer to n . Therefore, complete pivoting can't be observed because there would be too many floating points. Nor can partial as the partial pivoting would overwhelm after the "injection" of votes. Therefore, external factors were used which is evident from the "DIGITAL FIX"
74. Observing the elections, after a review of Michigan's data a spike of 54,199 votes to Biden. Because it is pushing and pulling and keeping a short distance between the 2 candidates; but then a spike, which is how an algorithm presents; - and this spike means there was a pause and an insert was made, where they insert an algorithm. Block spikes in votes for JOE BIDEN were NOT paper

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

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



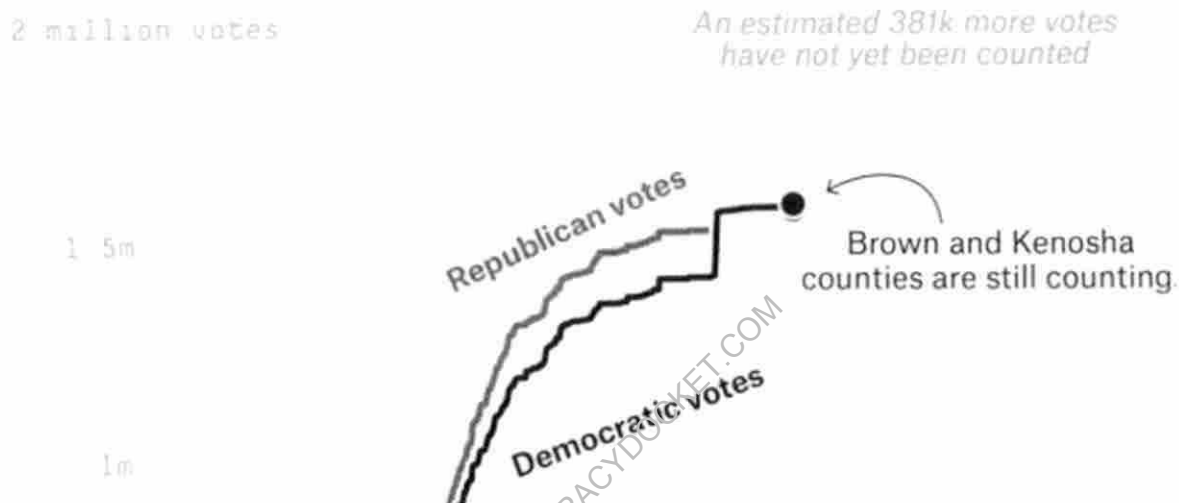
SUMMARY

- 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

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

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.

Total presidential votes for each party so far, with 89 percent of Wisconsin's expected vote counted as of 6:23 a.m. on Nov. 4



81.

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

[illegible]

83.

84.

April 21, 2014

SHARE THIS



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

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

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

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



- 106.
107. The last PRO V& V EAC accreditation certificate (Item 8) of this declaration expired in February 2017 which means that the IV & V conducted by Michigan claiming that they were accredited is false.
108. The significance of VSTLs being accredited and examining the HARDWARE is key. COTS software updates are the avenues of entry.
109. As per DOMINION'S own petition, the modems they use are COTS therefore failure to have an accredited VSTL examine the hardware for points of entry by their software is key.

*Compact Flash Cards	<u>***SanDisk Ultra:</u> SDCFHS-004G SDCFHS-008G <u>RiData:</u> CFC-14A RDF8G-233XMCB2-1 RDF16G-233XMCB2-1 RDF32G-233XMCB2-1 <u>SanDisk Extreme:</u> SDCFX-016G SDCFX-032G <u>SanDisk:</u> 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.

United States Department of Commerce
National Institute of Standards and Technology



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 Communiqué dated January 2009).*

2020-10-07 through 2020-12-31

Effective Dates



[Signature]
For the National Voluntary Laboratory Accreditation Program

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

SCHEDULE B-P **ITEMIZED DISBURSEMENTS**

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

FOR LINE NUMBER:
(check only one)

PAGE 7358 / 8595

☒ 23 ☐ 24 ☐ 25 ☐ 26 ☐ 27a
☐ 27b ☐ 28a ☐ 28b ☐ 28c ☐ 29

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

NAME OF COMMITTEE (In Full)

JOHN MCCAIN 2008, INC.

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

Subtotal Of Receipts This Page (optional)

424097.46

Total This Period (last page this line number only)

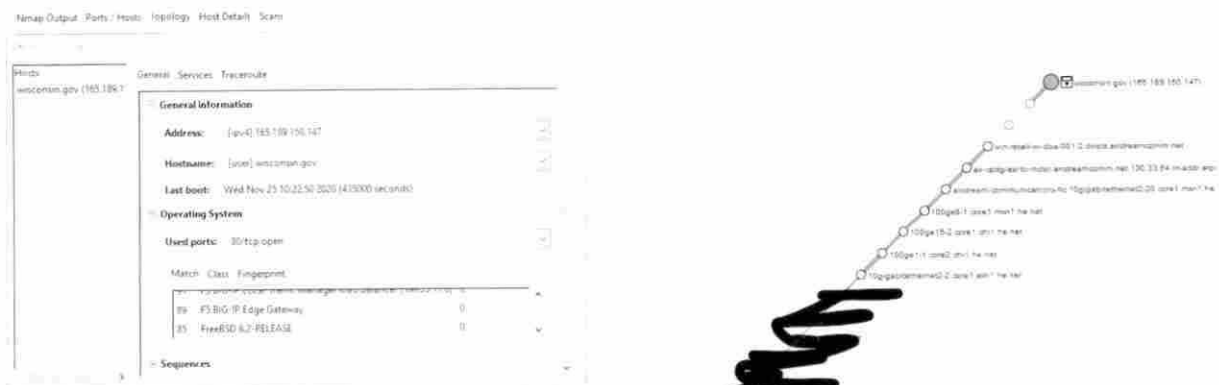
122.

123.

124. AKAMAI Technologies services SCYTL.

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

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



127.

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

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

Hosts	General	Services	Traceroute
wisconsin.gov (165.189.150.147)			
	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
		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 results." Reproduction of this document is prohibited without express permission of the subject.

OCTOBER 26, 2020

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

SEPTEMBER 12, 2019

September 2017 Nominative Sergeant's 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.

RETRIEVED FROM DEMOCRACYDOCKET.COM

	23230	Gutierrez	Ivialy	Jarie	(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.

A handwritten signature in black ink, appearing to read 'Terpsehore P Maras', with a stylized, cursive script.

Terpsehore P Maras

RETRIEVED FROM DEMOCRACYDOCKET.COM

EXHIBIT E

Brad Raffensperger Certification Documents,

RETRIEVED FROM DEMOCRACYDOCKET.COM



OFFICE OF SECRETARY OF STATE

I, Brad Raffensperger, Secretary of State of the State of Georgia, do hereby certify that

the Georgia Voter Registration System is being maintained in a manner consistent with the standards set forth in section (b) of Georgia Rule 590-8-3-.01 and that the standards set forth in said rule have been reviewed to ensure that they remain generally consistent with industry standards.

RETRIEVED FROM DEMOCRACYDOCKET.COM

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 31st day of December, in the year of our Lord Two Thousand and Nineteen and of the Independence of the United States of America the Two Hundred and Forty-Fourth



Brad Raffensperger
Brad Raffensperger, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Brad Raffensperger, Secretary of State of the State
of Georgia, do hereby certify that*

the Dominion Voting System (EAC Certification Number DVS-DemSuite5.5-A), consisting of the Democracy Suite 5.5-A Election Management System Version 5.5.12.1, EMS Adjudication Version 5.5.8.1, ImageCast X Prime (ICX BMD) Ballot Marking Device Version 5.5.10.30, ImageCast Precinct (ICP) Precinct Scanning Device Version 5.5.3-0002, and ImageCast Central (ICC) Central Scanning Device Versions 5.5.3-0002 and 5.5.3.3, manufactured by Dominion Voting Systems, Inc., 1201 18th Street, STE 210, Denver, Colorado 80202, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code and Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Chapter 2 of Title 21 of the Official Code of Georgia; provided however, that I hereby reserve my opinion to reexamine this voting system and its components at anytime so as to ensure that it continues to be one that can be safely used by the voters of this state.



IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 19th day of February, in the year of our Lord Two Thousand and Twenty and of the Independence of the United States of America the Two Hundred and Forty-Fourth

Brad Raffensperger
Brad Raffensperger, Secretary of State



OFFICE OF SECRETARY OF STATE

I, Brad Raffensperger, Secretary of State of the State of Georgia, do hereby certify that

the Dominion Voting System (EAC Certification Number DVS-DemSuite5.5-A), consisting of the Democracy Suite 5.5-A Election Management System Version 5.5.12.1, EMS Adjudication Version 5.5.8.1, ImageCast X Prime (ICX BMD) Ballot Marking Device Version 5.5.10.30, ImageCast Precinct (ICP) Precinct Scanning Device Version 5.5.3-0002, and ImageCast Central (ICC) Central Scanning Device Versions 5.5.3-0002 and 5.5.3.3, manufactured by Dominion Voting Systems, Inc., 1201 18th Street, STE 210, Denver, Colorado 80202, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code and Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Chapter 2 of Title 21 of the Official Code of Georgia; provided however, that I hereby reserve my opinion to reexamine this voting system and its components at anytime so as to ensure that it continues to be one that can be safely used by the voters of this state.



IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 19th day of February, in the year of our Lord Two Thousand and Twenty and of the Independence of the United States of America the Two Hundred and Forty-Fourth

Brad Raffensperger
Brad Raffensperger, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Brad Raffensperger, Secretary of State of the State
of Georgia, do hereby certify that*

the Dominion Voting System (EAC Certification Number DVS-DemSuite5.5-A), consisting of the Democracy Suite 5.5-A Election Management System Version 5.5.12.1, EMS Adjudication Version 5.5.8.1, ImageCast X Prime (ICX BMD) Ballot Marking Device Version 5.5.10.32, ImageCast Precinct (ICP) Precinct Scanning Device Version 5.5.3-0002, and ImageCast Central (ICC) Central Scanning Device Versions 5.5.3-0002 and 5.5.3.3, manufactured by Dominion Voting Systems, Inc., 1201 18th Street, STE 210, Denver, Colorado 80202, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code and Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Chapter 2 of Title 21 of the Official Code of Georgia; provided however, that I hereby reserve my opinion to reexamine this voting system and its components at anytime so as to ensure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 5th day of October, in the year of our Lord Two Thousand and Twenty and of the Independence of the United States of America the Two Hundred and Forty-Fourth



Brad Raffensperger

Brad Raffensperger, Secretary of State



OFFICE OF SECRETARY OF STATE

*I, Brad Raffensperger, Secretary of State of the State
of Georgia, do hereby certify that*

pursuant to the authority granted to the Secretary of State by Title 21, Chapter 2 of the Official Code of Georgia, the AccuVote Voting System, consisting of the Global Election Management System (GEMS), AccuVote TS R6 DRE Voting Station, AccuVote TSX DRE Voting Station, AccuVote OS Optical Scanner, ExpressPoll 4000 Electronic Poll Book, and ExpressPoll 5000 Electronic Poll Book, can no longer be lawfully used in Georgia beginning on January 1, 2020. Therefore, the previous certifications for the aforementioned system are hereby revoked, and the system is no longer certified for use in any primaries or elections in this state.



IN TESTIMONY WHEREOF, I have hereunto set my hand and
affixed the seal of my office, at the Capitol, in the City
of Atlanta, this 30th day of December, in the year of our
Lord Two Thousand and Nineteen and of the
Independence of the United States of America the
Two Hundred and Forty-Fourth

Brad Raffensperger
Brad Raffensperger, Secretary of State



OFFICE OF SECRETARY OF STATE

I, Brad Raffensperger, Secretary of State of the State of Georgia, do hereby certify that

the attached one (1) page constitutes a true and correct copy of the decertification of the AccuVote Voting System, consisting of the Global Election Management System (GEMS), AccuVote TS R6 DRE Voting Station, AccuVote TSX DRE Voting Station, AccuVote OS Optical Scanner, ExpressPoll 4000 Electronic Poll Book, and ExpressPoll 5000 Electronic Poll Book, as signed by the Secretary of State on December 30, 2019, all as the same appear on file in this office.



IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 30th day of December, in the year of our Lord Two Thousand and Nineteen and of the Independence of the United States of America the Two Hundred and Forty-Fourth.

Brad Raffensperger
Brad Raffensperger, Secretary of State

EXHIBIT F

Halderman Declaration,

RETRIEVED FROM DEMOCRACYDOCKET.COM

**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 nor 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

EXHIBIT G

Williamson County, TN, EAC Report,

RETRIEVED FROM DEMOCRACYDOCKET.COM

United States Election Assistance Commission Report of Investigation

**Dominion Voting Systems D-Suite 5.5-B
Williamson County, Tennessee**

March 31, 2022



Jonathon Panek
Director, Voting System Testing and Certification



U.S. ELECTION ASSISTANCE COMMISSION
633 3rd St. NW, Suite 200
Washington, DC 20001

Contents

Introduction	2
Reported Anomaly	2
Formal Investigation	3
Testing and Analysis	3
Conclusion of Formal Investigation	4

RETRIEVED FROM DEMOCRACYDOCKET.COM



U.S. ELECTION ASSISTANCE COMMISSION

633 3rd St. NW, Suite 200
Washington, DC 20001

Introduction

In late 2002, Congress passed the Help America Vote Act of 2002 (HAVA), which created the U.S. Election Assistance Commission (EAC) and vested it with the responsibility of setting voting system standards and providing for the testing and certification of voting systems. This mandate represented the first time the Federal government provided for the voluntary testing, certification, and decertification of voting systems nationwide. In response to this HAVA requirement, the EAC has developed the Federal Voting System Testing and Certification Program.

The EAC's Testing and Certification Program includes several quality monitoring tools that help ensure that voting systems continue to meet the EAC's voting system standards as the systems are manufactured, delivered, and used in Federal elections. These aspects of the program enable the EAC to independently monitor the continued compliance of fielded voting systems. One of these tools is field anomaly reporting.

Election officials may submit notices of voting system anomalies directly to the EAC. An anomaly is defined as an irregular or inconsistent action or response from the voting system, or system component, which resulted in the system or component not functioning as intended or expected. Anomaly reports may indicate a voting system is not in compliance with the Voluntary Voting System Guidelines or the procedural requirements of this EAC Testing and Certification Program.

An informal inquiry is the first step taken when information of this nature is presented to the EAC. The sole purpose of the informal inquiry is to determine whether a formal investigation is warranted. The outcome of an informal inquiry is limited to a decision on referral for investigation. A formal investigation is an official investigation by the EAC to determine whether a voting system warrants decertification. The result of a formal investigation is a Report of Investigation.

Reported Anomaly

On November 3, 2021, the EAC received a report from the Tennessee Secretary of State's (TN SoS) office that they were planning an investigation into an anomaly observed in Williamson County, Tennessee during a municipal election held on October 26, 2021, regarding Dominion D-Suite 5.5-B ImageCast Precinct (ICP) tabulators. Close poll reports from 7 of the 18 ICP tabulators used during the election did not match the number of ballots scanned. Subsequent tabulation on the jurisdiction's ICC central count scanner provided the correct tally. The central count tabulation was confirmed via hand count of the paper ballot records on October 27, 2021.

Discussions with the TN SoS on December 17, 2021, and January 5, 2022, following their investigation, provided additional details to the EAC. The details of the anomaly were



U.S. ELECTION ASSISTANCE COMMISSION

633 3rd St. NW, Suite 200

Washington, DC 20001

confirmed and reproduced during the state investigation, though the root cause of the anomaly was not determined.

Formal Investigation

Based upon the information obtained from the TN SoS, the EAC initiated a formal investigation into the matter to determine the necessary actions to obtain the root cause and remedy the issue. The investigation was conducted at the Williamson County Elections Commission facility on January 19 through January 22, 2022. This analysis was performed by both EAC accredited Voting System Test Laboratories (VSTL), Pro V&V and SLI Compliance. The EAC, Williamson County staff, TN SoS, and Dominion staff were present during the analysis.

Testing and Analysis

The first step of the VSTL analysis was verification of the system configuration. Hashes of all components involved were collected and compared to the repository of hashes for the EAC certified system. It was discovered that the system was installed with outdated versions of two configuration files when the system was upgraded from D-Suite 5.5 to D-Suite 5.5-B in January of 2021.

Next, a copy of the election definition used on election day was used to make Compact Flash (CF) cards for the ImageCast Precinct (ICP) scanners and ImageCast X (ICX) ballot marking devices. This election definition was imported into the D-Suite 5.5-B system from a definition originally created on the D-Suite 5.5 system.

Ballots were printed from the ICX and tabulated through the ICP scanners. Multiple ICP scanners were used for tabulation including some that originally exhibited the anomaly during the election and some that did not. Following tabulation, close poll reports and audit logs from the ICP scanners were examined. Results showed that the anomaly was recreated on each of the ICP scanners. This process was repeated several times to understand and isolate the details of exactly when the anomaly occurred and circumstances that may have led to the anomaly occurring.

Analysis of audit log information revealed entries that coincided with the manifestation of the anomaly; a security error "QR code signature mismatch" and a warning message "Ballot format or id is unrecognizable" indicating a QR code misread occurred. When these events were logged, the ballot was rejected. Subsequent resetting of the ICP scanners and additional tabulation demonstrated that each instance of the anomaly coincided with the previously mentioned audit log entries, though not every instance of those audit log entries resulted in the anomaly.

Further analysis of the anomaly behavior showed that the scanners correctly tabulated all ballots until the anomaly was triggered. Following the anomaly, ballots successfully scanned



U.S. ELECTION ASSISTANCE COMMISSION

633 3rd St. NW, Suite 200

Washington, DC 20001

and tabulated by the ICP were not reflected in the close poll reports on the affected ICP scanners.

Additional iterations of testing were performed after updating the configuration files previously mentioned to the proper versions associated with the D-Suite 5.5-B system. The anomaly was recreated using the correct configuration files with the originally programmed election definition.

A final test was performed using an election definition recreated entirely on the D-Suite 5.5-B system with identical parameters to the definition used during the election and for prior testing. The anomaly was not observed during this test, and there were no instances of the security error "QR code signature mismatch" or warning message "Ballot format or id is unrecognizable" in the audit log.

Conclusion of Formal Investigation

The direct cause of the anomaly was inconclusive. Based on the investigation, it's reasonable to conclude that the anomaly is related to the imported D-Suite 5.5 election definition used on the D-Suite 5.5-B system.

On February 11, 2022, Dominion submitted a Root Cause Analysis (RCA) to the EAC. The report indicates that erroneous code is present in the EAC certified D-Suite 5.5-B and D-Suite 5.5-C systems. The RCA report states that when the anomaly occurs, it's due to a misread of the QR code. If the QR code misread affects a certain part of the QR code, the ICP scanner mistakenly interprets a bit in the code that marks the ballot as provisional. Once that misread happens, the provisional flag is not properly reset after that ballot's voting session. The result is that every ballot scanned and tabulated by the machine after that misread is marked as provisional and thus, not included in the tabulator's close poll report totals.

Dominion has submitted Engineering Change Orders (ECO)s for the ICP software in the D-Suite 5.5-B and D-Suite 5.5-C systems: ECO 100826 and ECO 100827. Modified ICP source code was submitted by Dominion that resets the provisional flag following each voting session. The ECO analysis included source code review to confirm the change to both systems and to ensure no other code is changed. A Trusted Build of the modified source code was performed to produce the updated ICP software. This software was then tested for accuracy by processing two thousand ballots printed by an ICX, utilizing the same election definition used in Williamson County, TN on October 26, 2021.

The analysis and testing of the ECOs has demonstrated that the anomaly was successfully fixed. No instance of the anomaly or the associated error or warning messages in the ICP audit logs were observed during the testing. The EAC has approved ECO 100826 and ECO 100827 on March 31, 2022.

EXHIBIT H

SPECKIN FORENSICS, LLC REPORT,

RETRIEVED FROM DEMOCRACYDOCKET.COM

Speckin Forensics, LLC

120 N. WASHINGTON SQUARE, SUITE 300
PMB 506B
LANSING, MICHIGAN 48933
517-349-3528 • FAX 954-839-8219

PLEASE DIRECT CORRESPONDENCE & PAYMENT HERE:
2450 HOLLYWOOD BOULEVARD, SUITE 700
HOLLYWOOD, FLORIDA 33020
954-763-6134 • FAX 954-839-8219

www.4N6.com

LEONARD A. SPECKIN
RETIRED DOCUMENT ANALYST

MICHAEL J. SINKE
RETIRED LATENT PRINT SPECIALIST
RETIRED CRIME SCENE RECONSTRUCTION
RETIRED FORENSIC DOCUMENT ANALYST

DR. GEORGE F. JACKSON Ph.D.
FORENSIC TOXICOLOGIST

ERICH J. SPECKIN
FORENSIC DOCUMENT ANALYST
INK DATING SPECIALIST

PHILLIP MATUSIAK
COMPUTER & GRAPHICS SPECIALIST

THOMAS K. HUARD Ph.D.
DNA ANALYST & CONSULTANT

MARSHAUN BLAKE
ARSON & FIRE SPECIALIST

ANTHONY A. MILONE
COMPUTER & GRAPHICS SPECIALIST
FORENSIC DOCUMENT SPECIALIST

DR. JULIE HOWENSTINE
SEROLOGIST
DNA ANALYST & CONSULTANT
CRIME SCENE RECONSTRUCTION

September 15, 2022

Speckin Forensics was retained to acquire forensic Images of hard drives in Fulton County, Pennsylvania. The images of the drives that are the subject of this report were created on July 13-14, 2022.

A total of six hard drives were tendered for copying and analysis. The hard drives were in the corresponding device and were removed for copying and analysis. The record of the drive and the corresponding machine was recorded. One of the hard drives was not operable at the time of our imaging and therefore was not copied. This can be attempted at a later time with a more time-consuming procedure but has not yet been attempted. The remaining five drives were copied during the time onsite in Pennsylvania. The forensic image of each drive was saved on its own new unused Western Digital 4TB USB hard drive. This allowed for later duplication and examination of the evidence.

Using forensically sound procedures we documented the service tag numbers for all machines and the serial numbers of the corresponding hard drives contained within. Photographs were taken to record this. The drives copied are labeled as follows:

	Service Tag	Computer Name	Serial Number	Machine Model
1	3095PY2	EMSSERVER	59PUPSi1T/ 59PUPSi0T	Dell Precision 3430
3	1FPLNY2	Adjudication01	59OUPRS2T	Dell OptiPlex 3050
4	1FNPHY2	Failed drive	59OUPRRRT	Dell OptiPlex 3050
5	30C4PY2	EMSCIENT02	59PUPSHNT	Dell Precision 3430
6	30B4PY2	EMSCIENT01	59PUPSiST	Dell Precision 3430

The key findings are summarized below:

1. The security measures necessary to harden and secure the machines was not completed. The last update or security patch to the devices shows to be April 10, 2019, and no patches or updates were performed after this date.

2. External USB drives have been inserted on several occasions. We are unaware of any current list of approved external drives that could have been used. Therefore, there is no way to determine if any of the inserted USB drives was from an unauthorized source or if the USB drive further comprised the data or the system.
3. There have been substantial changes to the drives as seen with the inclusion of over 900 .dll files and links created since the date of installation of the Dominion software. This .dll additional pathway is a security breach because of the introduction of an unauthorized script.
4. There have also been no updates to the usernames or passwords as the passwords use default settings like "admin" and "guest". The group policies of the devices remain at default settings which in simple terms allows the username "admin" with password "admin"; complete access to the device.
5. The Adjudication01 workstation has a python script installed after the certification date of the system. This should not be added to the drive after a system has already been certified. This python script can exploit and create any number of vulnerabilities including, external access to the system, data export of the tabulations, or introduction of other metrics not part of or allowed by the certification process.
6. As expected and normal, each of the drives are interconnected in a system to one another. This would be required to provide sharing of data and counts between devices. Because of this networking, unauthorized access any one device, allows unauthorized access to any device connected to the network of devices.
7. An external IP address that is associated with Canada is found on the Adjudication 01. This shows that at least one of the network devices has connected to an external device on an external network. This is the same device that the post certification python script is found.

Procedure:

The hard drives from the computers were removed and connected them to a Forensic workstation. The hard drives were mounted as READ ONLY. Using FTK Imager a bit for bit copy was created using the Expert Witness file format. This is an industry standard format for storing forensic images. During the image creation process a hash value was computed to ensure the integrity of evidence. One of the main uses of hash values is to determine the integrity of data.

The copied data was analyzed using standard computer forensic software generally accepted in the field to search for the elements contained in this report.

Results:

Windows defender was found on the machines which dates to July 2016. No updates have been made since this time. Simply stated this means that viruses or malicious software components created after that date would not be combatted by this protection without the updates.

Further, Dominion published hardening procedures in 2019 that would reduce the chance of the system being compromised and provide additional security measures for the integrity of the system.

Below is a chart that shows external drives that have been connected to the devices examined.

The Dominion voting Systems software was installed on the devices on 04/10/19, 8/16/19 and 8/23/19. This last install date is consistent with the drives Generic, Canyon, and ScanDisk listed below. However, the 2021 drives do not fit this pattern and are unexplained at this point.

Computer Name	Device	Last Connection Date	Connection Time
3095PY2	PNY USB 2.0 Drive	2019-07-31	16:11
3095PY2	Generic USB Flash Drive	2019-08-23	16:54
3095PY2	Canyon USB Drive	2019-08-23	18:07
3095PY2	ScanDisk Cruzer FIT	2019-08-23	18:15
3095PY2	Samsung Flash Drive	2021-04-22	13:49
3095PY2	Kingston Data Traveler	2021-05-03	20:27
1FPLNY2	Samsung Flash Drive	2021-04-30	19:27
1FPLNY2	Kingston Data Traveler	2021-05-05	13:22

The following chart shows a small sample of .dll activity after the installation date of the voting software.

Name	Deleted	Last Accessed	File Created	Last Written	Entry Modified
UIAutomationTypes.ni.dll	•	08/29/19 08:02:12AM	08/29/19 08:02:12AM	08/29/19 08:02:12AM	10/02/19 04:44:27AM
System.Management.ni.dll		08/29/19 08:02:13AM	08/29/19 08:02:13AM	08/29/19 08:02:13AM	05/18/20 06:50:50AM
UIAutomationProvider.ni.dll	•	08/29/19 08:02:13AM	08/29/19 08:02:13AM	08/29/19 08:02:13AM	10/02/19 04:44:27AM
System.Drawing.ni.dll		08/29/19 08:02:15AM	08/29/19 08:02:15AM	08/29/19 08:02:15AM	10/02/19 04:44:24AM
System.Windows.Forms.ni.dll		08/29/19 08:02:19AM	08/29/19 08:02:19AM	08/29/19 08:02:19AM	10/02/19 04:44:26AM
System.Web.ni.dll		08/29/19 08:02:31AM	08/29/19 08:02:31AM	08/29/19 08:02:32AM	10/17/19 05:55:54AM
System.Messaging.ni.dll		08/29/19 08:02:33AM	08/29/19 08:02:33AM	08/29/19 08:02:33AM	10/17/19 05:55:53AM
System.EnterpriseServices.ni.dll		08/29/19 08:02:34AM	08/29/19 08:02:34AM	08/29/19 08:02:34AM	10/17/19 05:55:52AM

At least six different user and administrator accounts on the devices still have the password "Dvscorp2018!!!". This is the default password for the software at the time of installation. It has never been updated nor was it set to expire as should be the case. This is a glaring issue as this is specifically addressed by the Pennsylvania Secretary of State and referencing NIST.

"All jurisdictions implementing the Democracy Suite 5.5x must ensure that no default passwords are used on any devices and that all passwords are complex and secured. Counties must implement an audit process to review and ensure that no default passwords are used upon equipment install/reinstall and routinely change passwords to avoid any password compromise. The passwords and permissions management must at a minimum comply to the password requirements outlined in NIST 800-63".

The log files for the Adjudication device shows an IP address, 172.102.16.22. This IP address comes back to a location in Quebec, Canada, this is a serious issue to be connected remotely to a Canadian system. We cannot determine when this connection occurred or what data was transmitted, but an external connection was made at some point.

① 127.14.36.25 (2)
 ② 127.14.36.41 (2)
 ③ 127.15.23.146 (2)
 ④ 127.15.23.146 (2)
 ⑤ 127.15.23.146 (2)
 ⑥ 127.15.23.146 (2)
 ⑦ 127.15.23.146 (2)
 ⑧ 127.15.23.146 (2)
 ⑨ 127.15.23.146 (2)
 ⑩ 127.15.23.146 (2)
 ⑪ 127.15.23.146 (2)
 ⑫ 127.15.23.146 (2)
 ⑬ 127.15.23.146 (2)
 ⑭ 127.15.23.146 (2)
 ⑮ 127.15.23.146 (2)
 ⑯ 127.15.23.146 (2)
 ⑰ 127.15.23.146 (2)
 ⑱ 127.15.23.146 (2)
 ⑲ 127.15.23.146 (2)
 ⑳ 127.15.23.146 (2)
 ㉑ 127.15.23.146 (2)
 ㉒ 127.15.23.146 (2)
 ㉓ 127.15.23.146 (2)
 ㉔ 127.15.23.146 (2)
 ㉕ 127.15.23.146 (2)
 ㉖ 127.15.23.146 (2)
 ㉗ 127.15.23.146 (2)
 ㉘ 127.15.23.146 (2)
 ㉙ 127.15.23.146 (2)
 ㉚ 127.15.23.146 (2)
 ㉛ 127.15.23.146 (2)
 ㉜ 127.15.23.146 (2)
 ㉝ 127.15.23.146 (2)
 ㉞ 127.15.23.146 (2)
 ㉟ 127.15.23.146 (2)
 ㊱ 127.15.23.146 (2)
 ㊲ 127.15.23.146 (2)
 ㊳ 127.15.23.146 (2)
 ㊴ 127.15.23.146 (2)
 ㊵ 127.15.23.146 (2)
 ㊶ 127.15.23.146 (2)
 ㊷ 127.15.23.146 (2)
 ㊸ 127.15.23.146 (2)
 ㊹ 127.15.23.146 (2)
 ㊺ 127.15.23.146 (2)
 ㊻ 127.15.23.146 (2)
 ㊼ 127.15.23.146 (2)
 ㊽ 127.15.23.146 (2)
 ㊾ 127.15.23.146 (2)
 ㊿ 127.15.23.146 (2)

RETRIEVED FROM DEMOCRACYDOCKET.COM

Q. K.

Donald A. Smith

Computer Data Specialist

EXHIBIT I

Pearson VS Kemp/Raffensperger Case Law,

RETRIEVED FROM DEMOCRACYDOCKET.COM

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

CORECO JA'QAN PEARSON,
VIKKI TOWNSEND
CONSIGLIO; GLORIA KAY
GODWIN; JAMES KENNETH
CARROLL; CAROLYN HALL
FISHER; CATHLEEN ALSTON
LATHAM; and BRIAN JAY VAN
GUNDY,

Plaintiffs,

v.

BRIAN KEMP; BRAD
RAFFENSPERGER; DAVID J.
WORLEY; REBECCA N.
SULLIVAN; MATTHEW
MASHBURN; and ANH LE,

Defendants.

CIVIL ACTION FILE

NO. 1:20-cv-4809-TCB

ORDER

Plaintiffs have filed an emergency motion [6] for temporary injunctive relief. In their motion, Plaintiffs seek an order directing Defendants to allow Plaintiffs' expert(s) to inspect the Dominion voting

machines in Cobb, Gwinnett, and Cherokee Counties. The Court conducted a Zoom hearing at 7:45 p.m. EST to consider Plaintiffs' motion.

During the hearing, Defendants' counsel argued that the secretary of state has no lawful authority over county election officials, citing *Jacobson v. Florida Secretary of State*, 974 F.3d 1236, 1256–58 (11th Cir. 2020). Plaintiffs' counsel responded that Plaintiffs could amend their complaint to add the elections officials in Cobb, Gwinnett, and Cherokee Counties, thus obviating the issue of whether the proper officials had been named as Defendants to this case.

Defendants' counsel also argued that allowing such forensic inspections would pose substantial security and proprietary/trade secret risks to Defendants. Plaintiffs' counsel responded that Defendants' concerns could be alleviated by an order from the Court (1) allowing Defendants' own expert(s) to participate in the requested inspections, which would be video-recorded, and (2) directing the experts to provide whatever information they obtain to the Court—and no one else—for an *in camera* inspection.

After considering the parties' email submissions today and the arguments advanced at the Zoom hearing, it is hereby ORDERED, ADJUDGED and DECREED as follows:

1.

Defendants shall have until Wednesday, December 2, at 5:00 p.m. EST, to file a brief setting forth in detail the factual bases they have, if any, against allowing the three forensic inspections. The brief should be accompanied and supported by affidavit or other evidence, if appropriate.

2.

Defendants are hereby ENJOINED and RESTRAINED from altering, destroying, or erasing, or allowing the alteration, destruction, or erasure of, any software or data on any Dominion voting machine in Cobb, Gwinnett, and Cherokee Counties.

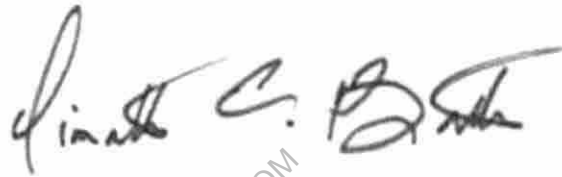
3.

Defendants are ORDERED to promptly produce to Plaintiffs a copy of the contract between the State and Dominion.

4.

This temporary restraining order shall remain in effect for ten days, or until further order of the Court, whichever comes first.

IT IS SO ORDERED this 29th day of November, 2020, at 10:10 p.m. EST.

A handwritten signature in black ink, appearing to read "Timothy C. Batten, Sr.", is written over a horizontal line.

Timothy C. Batten, Sr.
United States District Judge

RETRIEVED FROM DEMOCRACYDOCKET.COM

EXHIBIT J

CISA Report on Vulnerabilities,

RETRIEVED FROM DEMOCRACYDOCKET.COM



ICS Advisory (ICSA-22-154-01)

[More ICS-CERT Advisories](#)

Vulnerabilities Affecting Dominion Voting Systems ImageCast X

Original release date: June 03, 2022

Legal Notice

All information products included in <https://us-cert.cisa.gov/ics> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <https://us-cert.cisa.gov/tlp/>.

1. SUMMARY

This advisory identifies vulnerabilities affecting versions of the Dominion Voting Systems Democracy Suite ImageCast X, which is an in-person voting system used to allow voters to mark their ballot. The ImageCast X can be configured to allow a voter to produce a paper record or to record votes electronically. While these vulnerabilities present risks that should be mitigated as soon as possible, CISA has no evidence that these vulnerabilities have been exploited in any elections.

Exploitation of these vulnerabilities would require physical access to individual ImageCast X devices, access to the Election Management System (EMS), or the ability to modify files before they are uploaded to ImageCast X devices. Jurisdictions can prevent and/or detect the exploitation of these vulnerabilities by diligently applying the mitigations recommended in this advisory, including technical, physical, and operational controls that limit unauthorized access or manipulation of voting systems. Many of these mitigations are already typically standard practice in jurisdictions where these devices are in use and can be enhanced to further guard against exploitation of these vulnerabilities.

2. TECHNICAL DETAILS

TLP:WHITE

2.1 AFFECTED PRODUCTS

The following versions of the Dominion Voting Systems ImageCast X software are known to be affected (other versions were not able to be tested):

- ImageCast X firmware based on Android 5.1, as used in Dominion Democracy Suite Voting System Version 5.5-A
- ImageCast X application Versions 5.5.10.30 and 5.5.10.32, as used in Dominion Democracy Suite Voting System Version 5.5-A
 - **NOTE:** After following the vendor's procedure to upgrade the ImageCast X from Version 5.5.10.30 to 5.5.10.32, or after performing other Android administrative actions, the ImageCast X may be left in a configuration that could allow an attacker who can attach an external input device to escalate privileges and/or install malicious code. Instructions to check for and mitigate this condition are available from Dominion Voting Systems.

Any jurisdictions running ImageCast X are encouraged to contact Dominion Voting Systems to understand the vulnerability status of their specific implementation.

2.2 VULNERABILITY OVERVIEW

NOTE: Mitigations to reduce the risk of exploitation of these vulnerabilities can be found in Section 3 of this document.

2.2.1 IMPROPER VERIFICATION OF CRYPTOGRAPHIC SIGNATURE CWE-347

The tested version of ImageCast X does not validate application signatures to a trusted root certificate. Use of a trusted root certificate ensures software installed on a device is traceable to, or verifiable against, a cryptographic key provided by the manufacturer to detect tampering. An attacker could leverage this vulnerability to install malicious code, which could also be spread to other vulnerable ImageCast X devices via removable media.

CVE-2022-1739 has been assigned to this vulnerability.

2.2.2 MUTABLE ATTESTATION OR MEASUREMENT REPORTING DATA CWE-1283

The tested version of ImageCast X's on-screen application hash display feature, audit log export, and application export functionality rely on self-attestation mechanisms. An attacker could leverage this vulnerability to disguise malicious applications on a device.

CVE-2022-1740 has been assigned to this vulnerability.

2.2.3 HIDDEN FUNCTIONALITY CWE-912

The tested version of ImageCast X has a Terminal Emulator application which could be leveraged by an attacker to gain elevated privileges on a device and/or install malicious code.

CVE-2022-1741 has been assigned to this vulnerability.

2.2.4 IMPROPER PROTECTION OF ALTERNATE PATH CWE-424

The tested version of ImageCast X allows for rebooting into Android Safe Mode, which allows an attacker to directly access the operating system. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.

CVE-2022-1742 has been assigned to this vulnerability.

2.2.5 PATH TRAVERSAL: '../FILEDIR' CWE-24

The tested version of ImageCast X can be manipulated to cause arbitrary code execution by specially crafted election definition files. An attacker could leverage this vulnerability to spread malicious code to ImageCast X devices from the EMS.

CVE-2022-1743 has been assigned to this vulnerability.

2.2.6 EXECUTION WITH UNNECESSARY PRIVILEGES CWE-250

Applications on the tested version of ImageCast X can execute code with elevated privileges by exploiting a system level service. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.

CVE-2022-1744 has been assigned to this vulnerability.

2.2.7 AUTHENTICATION BYPASS BY SPOOFING CWE-290

The authentication mechanism used by technicians on the tested version of ImageCast X is susceptible to forgery. An attacker with physical access may use this to gain administrative privileges on a device and install malicious code or perform arbitrary administrative actions.

CVE-2022-1745 has been assigned to this vulnerability.

2.2.8 INCORRECT PRIVILEGE ASSIGNMENT CWE-266

The authentication mechanism used by poll workers to administer voting using the tested version of ImageCast X can expose cryptographic secrets used to protect election information. An attacker could leverage this vulnerability to gain access to sensitive information and perform privileged actions, potentially affecting other election equipment.

CVE-2022-1746 has been assigned to this vulnerability.

2.2.9 ORIGIN VALIDATION ERROR CWE-346

The authentication mechanism used by voters to activate a voting session on the tested version of ImageCast X is susceptible to forgery. An attacker could leverage this vulnerability to print an arbitrary number of ballots without authorization.

CVE-2022-1747 has been assigned to this vulnerability.

2.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS** Government Facilities / Election Infrastructure
- **COUNTRIES/AREAS DEPLOYED:** Multiple
- **COMPANY HEADQUARTERS LOCATION:** Denver, Colorado

2.4 RESEARCHER

J. Alex Halderman, University of Michigan, and Drew Springall, Auburn University, reported these vulnerabilities to CISA.

3. MITIGATIONS

CISA recommends election officials continue to take and further enhance defensive measures to reduce the risk of exploitation of these vulnerabilities. Specifically, for each election, election officials should:

- Contact Dominion Voting Systems to determine which software and/or firmware updates need to be applied. Dominion Voting Systems reports to CISA that the above vulnerabilities have been addressed in subsequent software versions.
- Ensure all affected devices are physically protected before, during, and after voting.
- Ensure compliance with chain of custody procedures throughout the election cycle.
- Ensure that ImageCast X and the Election Management System (EMS) are not connected to any external (i.e., Internet accessible) networks.
- Ensure carefully selected protective and detective physical security measures (for example, locks and tamper-evident seals) are implemented on all affected devices, including on connected devices such as printers and connecting cables.
- Close any background application windows on each ImageCast X device.
- Use read-only media to update software or install files onto ImageCast X devices.
- Use separate, unique passcodes for each poll worker card.
- Ensure all ImageCast X devices are subjected to rigorous pre- and post-election testing.
- Disable the "Unify Tabulator Security Keys" feature on the election management system and ensure new cryptographic keys are used for each election.
- As recommended by Dominion Voting Systems, use the supplemental method to validate hashes on applications, audit log exports, and application exports.
- Encourage voters to verify the human-readable votes on printout.
- Conduct rigorous post-election tabulation audits of the human-readable portions of physical ballots and paper records, to include reviewing ballot chain of custody and conducting voter/ballot reconciliation procedures. These activities are especially crucial to detect attacks where the listed vulnerabilities are exploited such that a barcode is manipulated to be tabulated inconsistently with the human-readable portion of the paper ballot. (**NOTE:** If states and jurisdictions so choose, the ImageCast X provides the configuration option to produce ballots that do not print barcodes for tabulation.)

Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov

Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: <https://us-cert.cisa.gov/ics>
or incident reporting: <https://us-cert.cisa.gov/report>

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

This product is provided subject to this Notification and this Privacy & Use policy.

RETRIEVED FROM DEMOCRACYDOCKET.COM

EXHIBIT K

Ryan Germany Memo

RETRIEVED FROM DEMOCRACYDOCKET.COM



OFFICIAL ELECTION BULLETIN

May 27, 2022

TO: County Election Officials and County Registrars

FROM: Ryan Germany, General Counsel

RE: Open Records Request for Ballot Images

Many counties have received a request for copies of physical ballots (as opposed to ballot images). Physical ballots are not subject to public disclosure and Georgia courts have held that such documents are by law prohibited from being open to inspection by the general public. Ballot images created by the voting system are public, and you should provide copies of ballot images once your election project (which contains the ballot images) has been certified and you are able to fulfill the request.

Physical ballots are not subject to open records. OCGA 21-2-574 makes possession of ballots by "any person, other than an officer charged by law with the care of ballots" a felony. Physical ballots should always be in your custody and control prior and required to be kept under seal. The argument made by the requestors that the ballots are not yet under seal is wrong and has been specifically rejected by Georgia courts. In an case seeking election records, the Georgia Court of Appeals concluded that when materials (such as ballots) are "statutorily designated to be kept under seal, it is by law prohibited or specifically exempted from being open to inspection by the general public and, therefore, is not an open record subject to disclosure." *Smith v. DeKalb County*, 288 Ga. App. 574 (2007). Physical ballots are election documents that are by law to be kept under seal. The timing of the open records request does not change that designation or magically make documents that the law requires to be kept under seal open to public inspection.

The requestor also asks that instead of giving him access to the actual ballots, that you make a photocopy of the ballots. Under no circumstances should local election officials make copies of voted ballots as this would open you up to allegations of copying ballots or attempting to stuff the ballot box. It should not happen.

Georgia law has dealt with the issue of transparency regarding voted ballots by expressly making scanned ballot images created by the voting system subject to public disclosure. OCGA 50-18-71(k). Physical ballots other than the ballot images that will be part of your certified election project are not subject to public disclosure and are specifically prohibited by law from being open to public disclosure.

EXHIBIT L

DeKalb Commission Letter,

RETRIEVED FROM DEMOCRACYDOCKET.COM



SUBJECT : Preliminary Expert Analysis of Commissioner District 2 Discrepancies

To:

Dele Lowman Smith dlsmith@dekalbcountyga.gov (chair)
Nancy Jester njester@dekalbcountyga.gov (vice-chair)
Susan Motter smotter@dekalbcountyga.gov
Anthony Lewis antlewis@dekalbcountyga.gov
Karli Swift kswift@dekalbcountyga.gov
Keisha Smith klsmith@dekalbcountyga.gov (Elections Director)

June 3, 2022

Dear DeKalb Co. Board Members and Director Smith,

I want to thank each of you again for your commitment and dedication to ensure the accuracy of the 2022 Primary races by ordering a full hand count audit of the District2 Commission race. The hard work of the staff and volunteers found results and outcome **totally different** than the results and outcome the Dominion voting system reported. You are now faced with a difficult task of determining why the discrepancies exist and what to do.

To assist your efforts, **I asked our international team of experts to review the discrepancies.** The team includes a half dozen experts who are highly experienced in information technology, voting system forensics, data analysis and investigative research. I personally have over 40 years of Information Technology experience in a wide variety of disciplines as well as 20 years of part time research into electronic voting systems.

We have heard the discrepancies found in the District2 race could have been created by error after one candidate withdrew from the race. This error could have caused a candidate alignment mismatch in the ballot definitions between Ballot Marking Devices (BMD) and scanner/tabulators. We sought to answer the question: ***"Could such a ballot definition misalignment of candidates be the sole reason for the results discrepancies found?"*** Even when we consider the five precincts affected by redistricting (see Appendix), the unanimous answer is ***"No!"***.

A ballot definition misalignment of candidates could **not** be the sole reason for the discrepancies found because:

- There is over a 1,300-vote difference between the voting system total votes cast and the hand count audit votes cast. **This total vote discrepancy has nothing to do with a ballot definition alignment.** The current Dominion system simply **failed** to count those votes regardless of how the candidates are aligned.
- A ballot definition alignment mismatch would typically show all of one candidate's votes for another candidate and all of that candidate's votes for still another candidate. That was not the case for District2 as **there are a variety of different types of inexplicable discrepancies that fit no particular pattern.**
- A ballot definition alignment mismatch between scanners and BMDs would show similar discrepancies for all in person voting. Instead, **the inexplicable discrepancies are dramatically more pronounced on Election Day as opposed to Early Voting.**



Given these facts we make the following logical conclusions:

- **There is a far more serious counting problem with the Dominion voting system than a ballot definition mis-alignment of candidates would cause.**
- **There is no single mistake that DeKalb Co. staff could have made to cause the dramatic, voting system counting errors that have been uncovered since some of the errors are outside the staff's control.**
- **Since the voting system counting errors cannot be attributed to candidate withdrawal, DeKalb County must audit the other races on the ballot to ensure that they are accurate.**
- **Copies of ballots produced independently of the voting system are necessary to verify the results of other races if audits are not conducted before certification.**
- **Since this is the only Georgia 2022 primary race that has been audited, the findings of the audit have dire implications for the validity of certifications by other counties throughout the state.**

I want to conclude by thanking all the members of the DeKalb County Election Board and the staff for recognizing your paramount duty is to ensure the accuracy of the election and by not succumbing to outside pressure to certify an election that you know has incorrect results. Although you have inherited a difficult problem you are laying the foundation for building DeKalb County into a shining example of how to handle severe election reporting problems through your commitment to election integrity and transparency.

Should you need assistance in auditing other races or performing other activities, we are glad to help supply volunteers from the greater metropolitan area for such a critical effort.

Sincerely,

Garland Favorito
garlandf@voterga.org
404 664-4044





Appendix:

District 2 results reported on May 24

Candidate	Election Day	Advance Voting	Absentee by Mail	Provisional	Total
Lauren Alexander	2671	1428	283	0	4382
Marshall Orson	3343	1490	393	0	5226
Michelle Long Spears	589	2019	423	0	3031
Total Votes	6603	4937	1099	0	12639

Votes omitted by a redistricting error should be added to table above

Candidate	Election Day	Advance Voting	Absentee by Mail	Provisional	Total
Lauren Alexander	322	141	21	0	484
Marshall Orson	181	100	20	0	301
Michelle Long Spears	440	175	24	0	639
Total Votes	943	416	65	0	1424

District 2 results of hand count reported on June 1

Candidate	Election Day	Advance Voting	Absentee by Mail	Provisional	Total
Lauren Alexander	3008	1457	265	7	4737
Marshall Orson	2069	1492	362	5	3928
Michelle Long Spears	4080	2152	415	4	6651
Donald Broussard	53	41	39	0	133
Total Votes	9210	5142	1081	16	15449

From:
Lori Portillo
210 Carmichael Road
Woodstock, GA 30189
, 2022

To:
Honorable Superior Court of Cherokee County
Cherokee County Georgia

Re: Verified Complaint for Declaratory Judgment and Injunction

AFFIDAVIT OF FACT

I, Lori Portillo, hereinafter affiant, personally appeared before the undersigned notary public, and under oath or affirmation state the following facts:

I am a citizen of Georgia. I am lawfully registered to vote in Cherokee County for all elections and have participated in that franchise since December 2005 .

I am a taxpayer in Cherokee County and Georgia.

I hereby attest, based on the facts presented to this honorable court in the accompanying Complaint for Declaratory Judgment and Injunctive Relief, that I do not believe my vote is counted nor cast for my true selection nor intention.

I hereby attest, that due to the lack of certification, the fact that machine voting was never voted on by electors to replace paper ballots, and the fact that electors never voted on an increase of the indebtedness of Cherokee County nor an increase of taxes in Cherokee County to pay for these voting machines, that these machines are illegal and were unconstitutionally and illegally forced upon me and the People of Cherokee County.

I hereby attest, that the parties involved in this voting scheme have denied, infringed upon or abridged my right to vote.

I, Lori Portillo, have no contract relinquishing Rights or Property to the state of Georgia, nor any subdivisions thereof.


I, Lori Portillo, DO NOT COMPLY with voting on an illegal voting machine.

I am not an expert in law; however, I do know right from wrong. If there is any man or woman damaged by any statements herein, if he will inform me by facts, I will sincerely make every effort to amend. I hereby and herein reserve the right to amend and make amendments to this

document as necessary, in order that the truth may be ascertained and proceedings justly determined.

My signature verifies that I, Lori Portillo, will testify as to these facts, in open court, I do hereby swear and affirm that all herein be true to the best of my knowledge and belief under penalty of perjury.

Executed on this 17th day, of the 10th month, in the year of our Lord and Savior, two thousand twenty two


Signature

Lori Portillo
Printed Name

Subscribed and affirmed, or sworn to, before me this 17 day of
October, 20 22, in the County of
Cherokee, State of Georgia.

[Notary Seal]


Notary Public Signature

Aug 4, 2025
Commission Expire Date

