

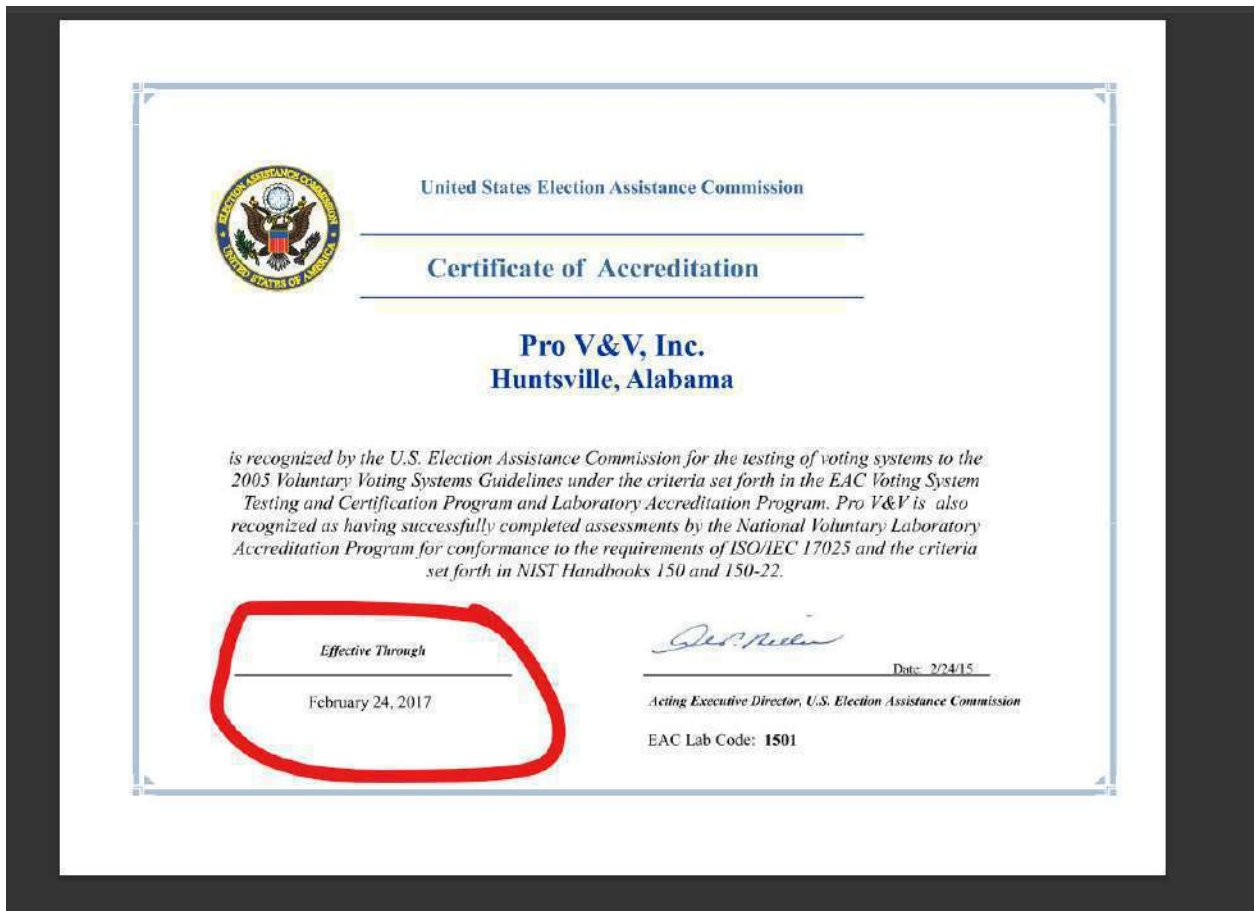
Appendix D

Declaration of [REDACTED]

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

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

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



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

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 Communique 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]." WIS. STAT. ANN. § 5.91 (West 2009).
<i>Applicable Regulation(s):</i>	"An application for approval of an electronic voting system shall be accompanied by all of the following ... [r]eports from an independent testing authority accredited by the national association of state election directors (NASED) demonstrating that the voting system conforms to all the standards recommended by the federal elections commission." WIS. ADMIN. CODE GAB § 7.01 (2009).
<i>State Certification Process:</i>	The Board of Election Commissioners accepts applications for the approval of electronic voting systems. Once the application is completed, the vendor must set up the voting system for three mock elections using: (1) offices, (2) referenda questions and (3) candidates. A panel of local election officials can assist the Board in the review of the voting system. The Board conducts the test using a mock election for the partisan primary, general election, and nonpartisan election. The Board may also require that the voting system be used in an actual election as a condition of the approval. WIS. ADMIN. CODE GAB §§ 7.01, 7.02 (2009).
<i>Fielded Voting Systems:</i>	<i>[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].</i> http://elections.state.wi.us/section.asp?linkid=643&locid=47



GEORGIA

State Participation:

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

Applicable Statute(s):

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

Applicable Regulation(s):

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

State Certification Process:

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

Fielded Voting Systems:

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



PENNSYLVANIA

State Participation:

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

Applicable Statute(s):

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

Applicable Regulation(s):

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

State Certification Process:

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

Fielded Voting Systems:

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



ARIZONA

State Participation:

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

Applicable Statute(s):

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

Applicable Regulation(s):

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

State Certification Process:

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

Fielded Voting Systems:

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

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.

The screenshot displays the Pro V&V website interface. At the top, there is a search bar with 'SEARCH' and 'CLEAR' buttons. Below the search bar, the 'Accredited Labs' section lists two results. The first result is for 'Pro V&V' located at 700 Boulevard South, Suite 102, Huntsville, AL 35802. The second result is for 'SLI Compliance, a Division of Gaming Laboratories International, LLC' located at 4720 Independence Street, Wheat Ridge, CO 80033. Both labs are listed as 'Accredited'. To the right of the search results, there are sections for 'Frequently Asked Questions', 'Manuals and Forms', 'Test and Certification Blogs', 'DO YOU HAVE QUESTIONS?' with a 'Contact Us' button, and 'REGISTER TO VOTE!' with a 'Register Today' button. At the bottom of the page, there is a contact form with fields for 'Your Name (required)', 'Your Email (required)', 'Subject', and 'Your Message', along with a 'Send' button. The footer includes the copyright notice '© 2020 Pro V&V, Inc. All rights reserved.' and the text 'Theme by Tescart'.

https://eac-legacy.ae-admin.com/voting-equipment/voting-system-test-laboratories-vstl/

SEARCH CLEAR

Accredited Labs

2 results found.
Page 1 of 1

Pro V&V
700 Boulevard South
Suite 102
Huntsville, AL 35802
Status: Accredited
Program Manager: Jack Cobb, President
Phone: 256-713-1111
[Learn More >](#)

SLI Compliance, a Division of Gaming Laboratories International, LLC
4720 Independence Street
Wheat Ridge, CO 80033
Status: Accredited
Program Manager: Traci Mapps, Director of Operations
Phone: 303-422-1566
[Learn More >](#)

Frequently Asked Questions
Manuals and Forms
Test and Certification Blogs

DO YOU HAVE QUESTIONS?
Send your questions to us at clearinghouse@eac.gov or click the button below to contact us.
[Contact Us](#)
(Link opens in new tab)

REGISTER TO VOTE!
Use the National Mail Voter Registration Form to register to vote, update your registration information with a new name or address, or register with a political party.
Note: If you wish to vote absentee and are a uniformed service member or family member or a citizen living outside the U.S., contact the Federal Voting Assistance Program to register to vote.
[Register Today](#)

Not secure | www.provandu.com/contact/

Your Name (required)
Your Email (required)
Subject
Your Message
[Send](#)

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

© 2020 Pro V&V, Inc. All rights reserved.
Theme by Tescart

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

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

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

28 046 Madrid

Asian offices

Akamai Technologies - India

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

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

Akamai Technologies - China

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

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

Akamai Japan K.K.

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

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

Akamai Technologies - Singapore

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

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


Akamai Technologies - Australia and New Zealand

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

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

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

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

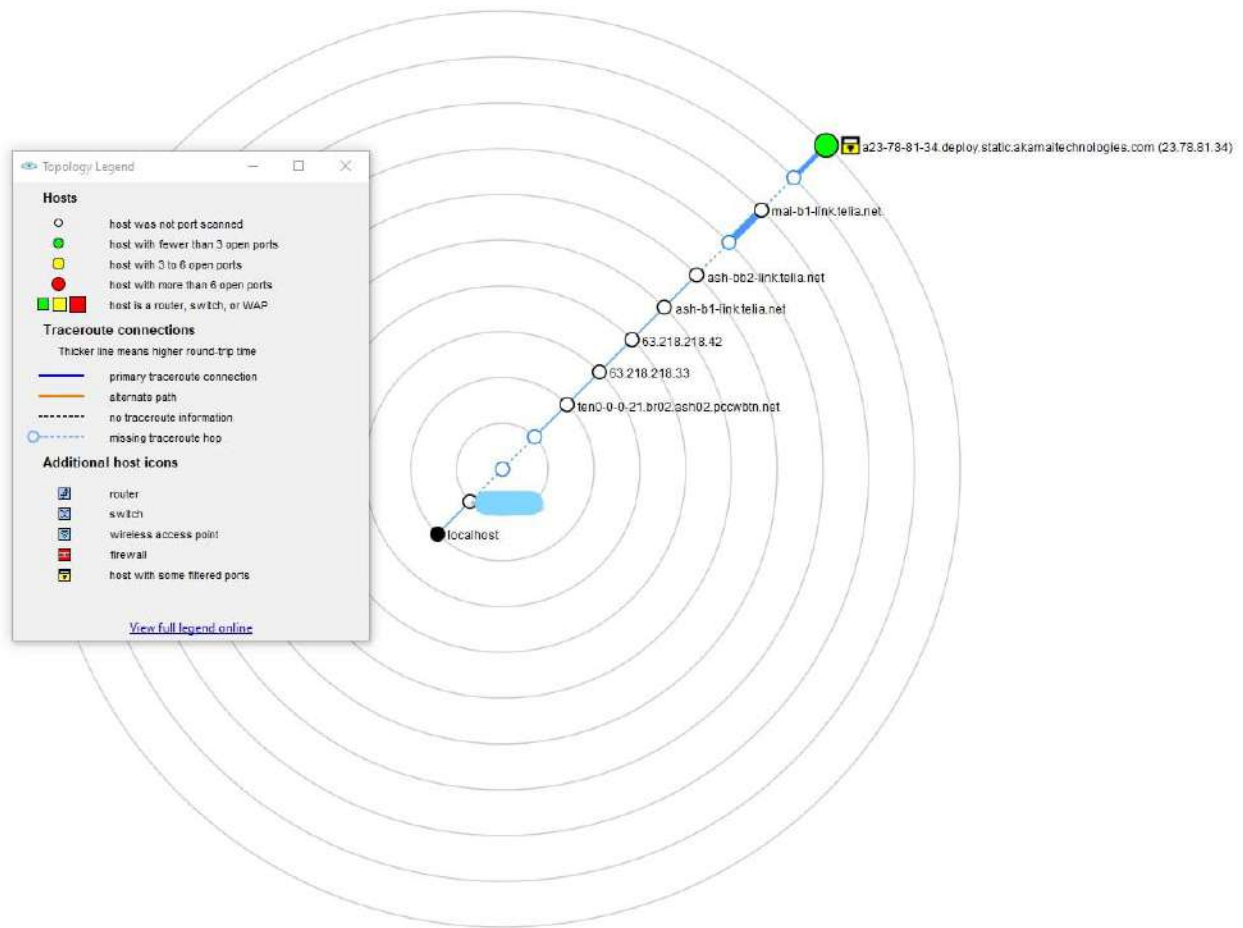


27.

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



29.



30.

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

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

Advertisements	Basic Tracking Info
	Domain: Michigan.gov [Whois Lookup - Domain Country - Domain To IP]
	IP Address: 23.78.81.34 [IP Blacklist Check]
	Reverse DNS: 34.81.78.23.in-addr.arpa
	Hostname: a23-78-81- 34.deploy.static.akamaitechnologies.com
	a12-67.akam.net >> 184.26.160.67
	a11-66.akam.net >> 84.53.139.66
	a1-35.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: -21600
	Sunrise / Sunset: 07:27 / 17:12
	Extra Information for an IP: Michigan.gov
	Continent: 46.07305 / -100.546
	Country: 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 Scytl (offshore) for configuration of data. All e-voting is sent to CONFIGURATION OF DATA then back to the e-voting machine and then to the next phase called CLEANSING. **CONCERNS:** Here we see an “OR PROOF” as coined by mathematicians – an “or proof” is that votes that have been pre-tallied parked in the system and the algorithm then goes back to set the outcome it is set for and seeks to make adjustments if there is a partial pivot present causing it to fail demanding manual changes such as block allocation and narrowing of parameters or self-adjusts to ensure the predetermined outcome is achieved.
45. STEP 2|CLEANSING | The Process is when all the votes come in from the software run by Dominion and get “cleansed” and put into 2 categories: invalid votes and valid votes.
46. STEP 3|Shuffling /Mixing | This step is the most nefarious and exactly where the issues arise and carry over into the decryption phase. Simply put, the software takes all the votes, literally mixes them a and then re-encrypts them. This is where if ONE had the commitment key- TRAPDOOR KEY – one would be able to see the parameters of the algorithm deployed as the votes go into this mixing phase, and how algorithm redistributes the votes.
47. This published PAPER FROM University College London depicts how this shuffle works. In essence, when this mixing/shuffling occurs, then one doesn’t have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes when mixed.

48.

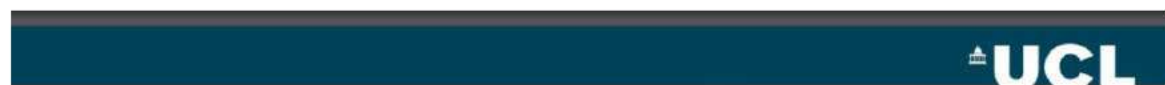
Background - ElGamal encryption

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

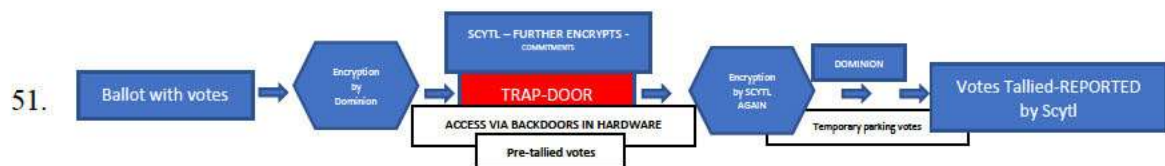
$$\mathcal{E}_{pk}(m; r) \times \mathcal{E}_{pk}(M; R) = \mathcal{E}_{pk}(mM; r + R)$$

- Re-encryption:

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



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



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

“Generators” and therefore together build “commitments.”

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

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

54. Scytel 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, Scytel or anyone that knows the commitment parameters can take all the votes and give them to any one they want. If they have a total of 1000 votes an algorithm can distribute them among all races as it deems necessary to achieve the goals it wants. (Case Study: Estonia)

Commitment_{CRYPT} = CM_C

Scytl sets commitment - simple math

$$CM_C(\vec{a}; r) = H \left[\prod_{i=1}^n G_i^{a_i} \right]$$

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

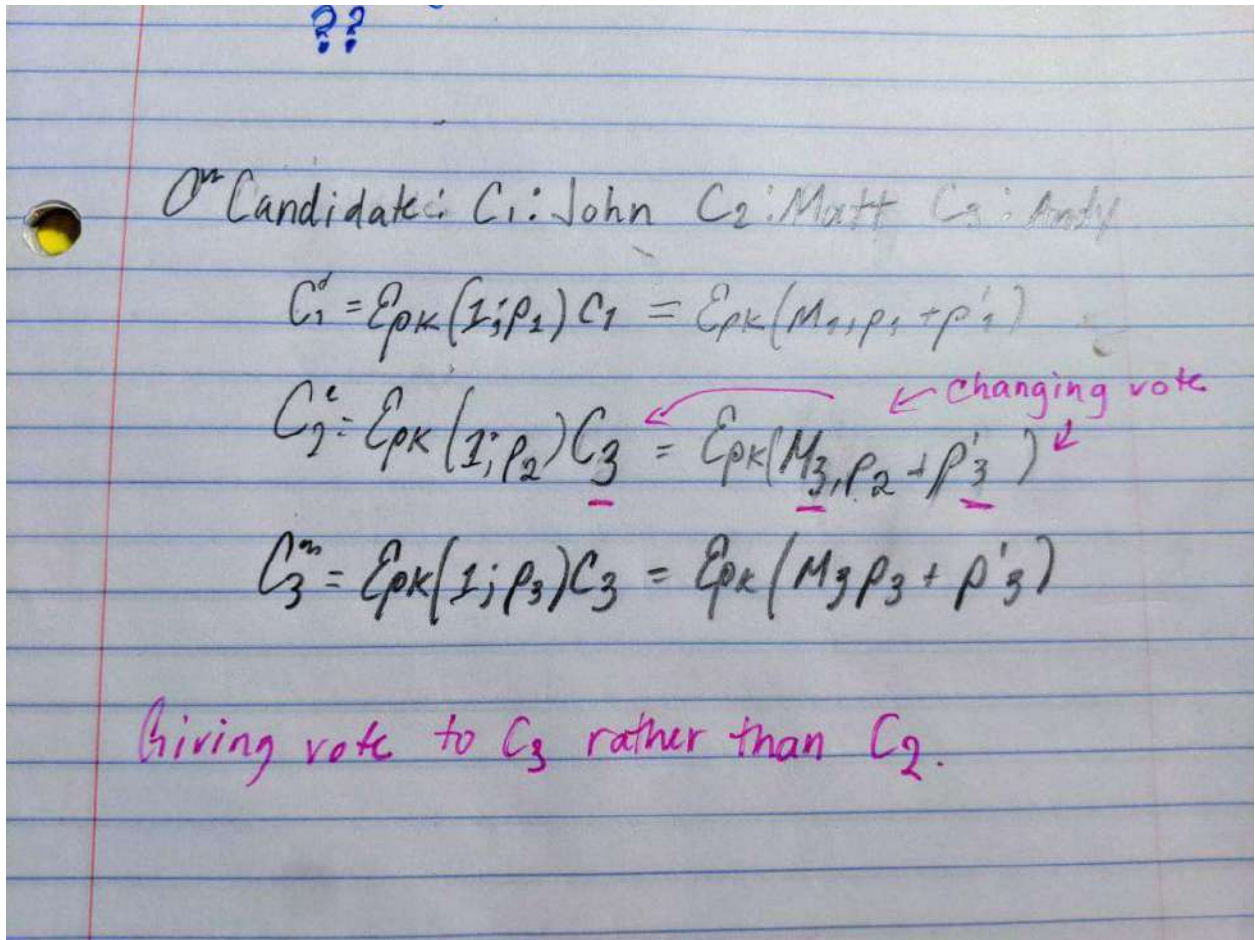
$$CM_C(\vec{a}; r) = CM_C(\vec{a}; r')$$

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

56.

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

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

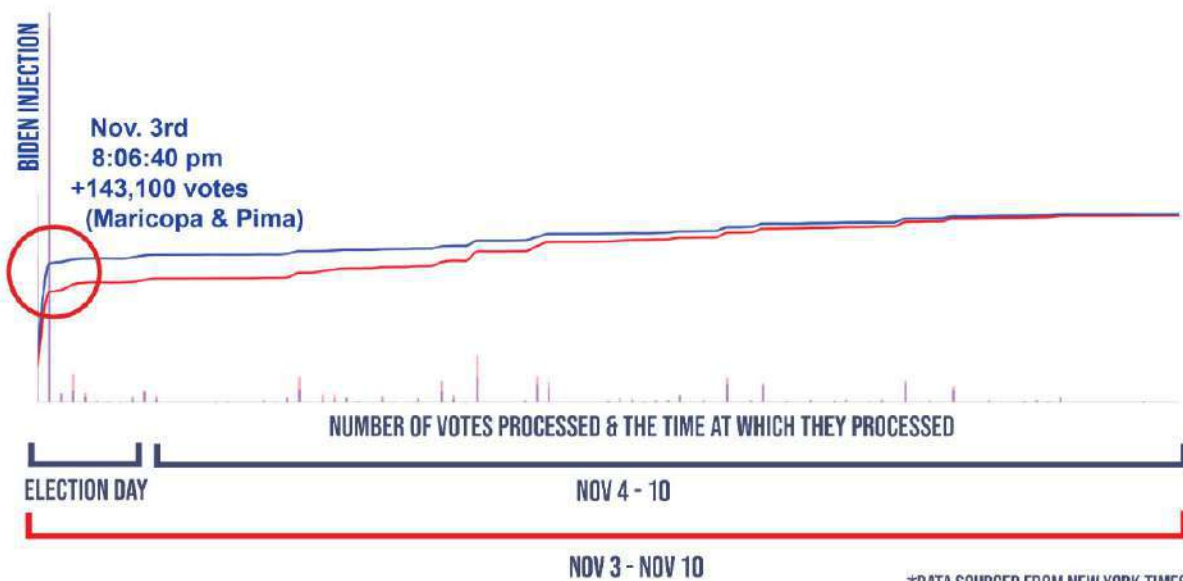


58. STEP 4|Decryption would be the decryption phase and temporary parking of vote tallies before reporting. In this final phase before public release the tallies are released from encrypted format into plain text. As previously explained, those that know the trapdoor can easily change any votes that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

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

ARIZONA

"FIXING" THE VOTE

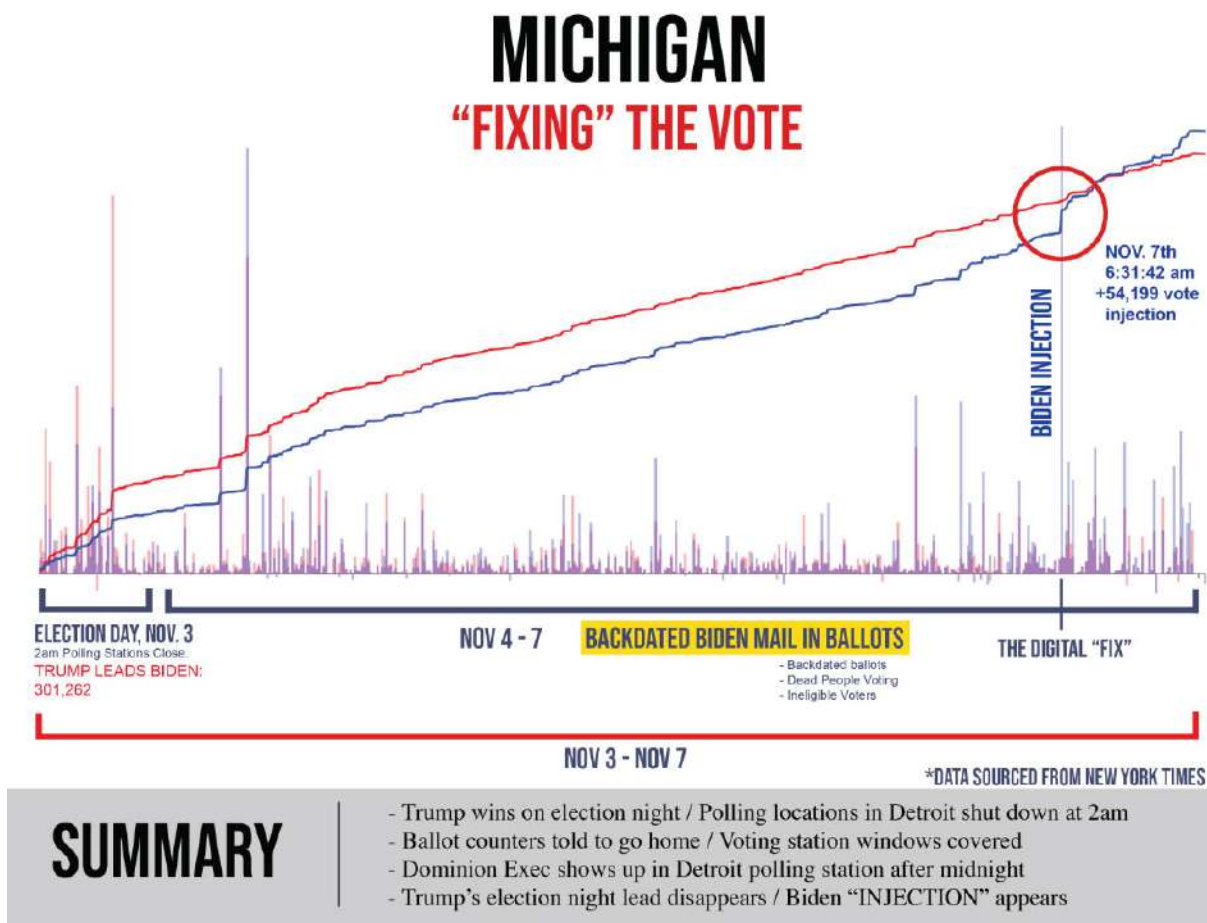


SUMMARY

- 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

69.

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



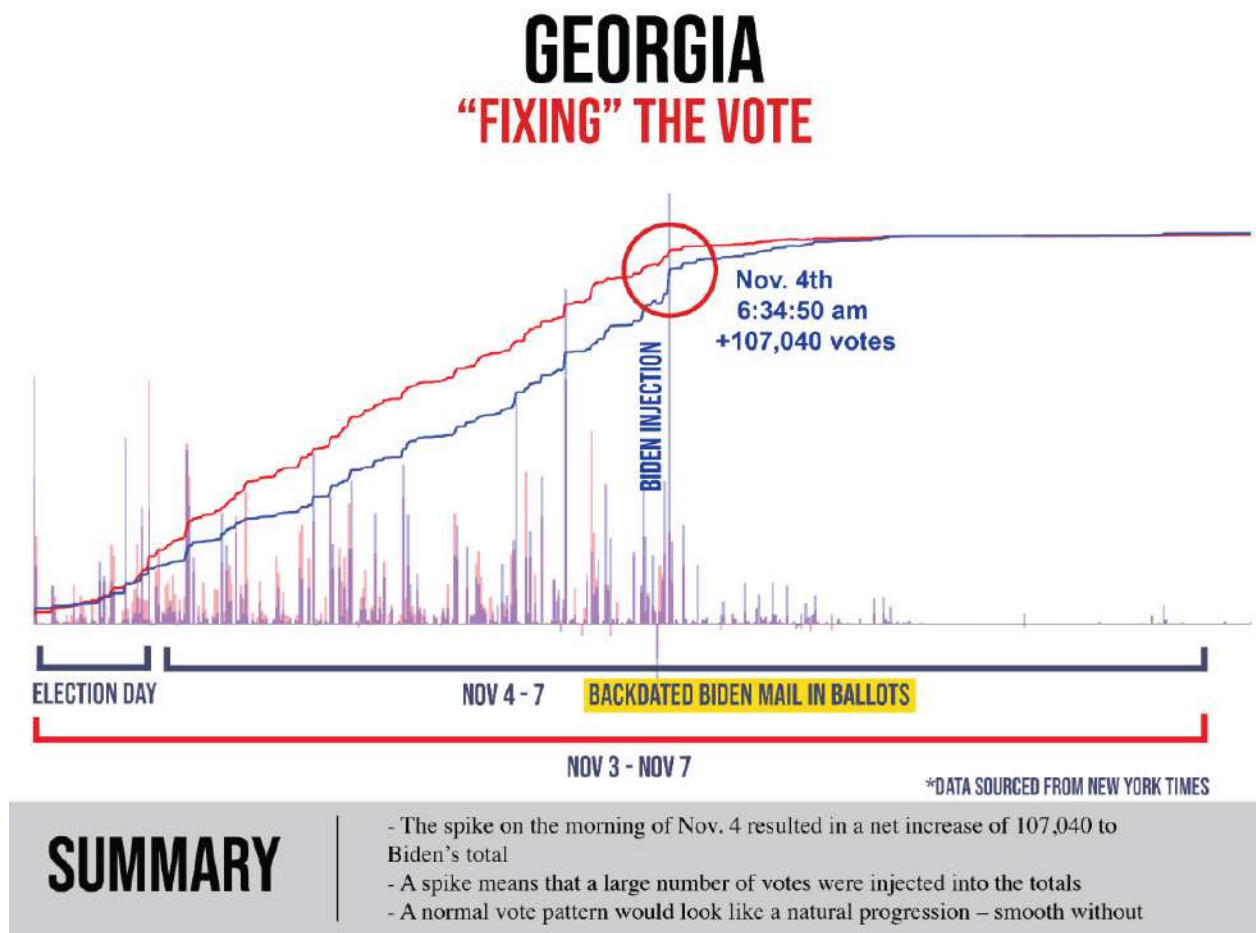
71. The "Digital Fix" observed with an increased spike in VOTES for Joe Biden can be determined as evidence of a pivot. Normally it would be assumed that the algorithm had a Complete Pivot. Wilkinson's demonstrated the guarantee as :

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

- 72.
73. Such a conjecture allows the growth factor the ability to be upper bound by values closer to n . Therefore, complete pivoting can't be observed because there would be too many floating points. Nor can partial as the partial pivoting would overwhelm after the "injection" of votes. Therefore, external factors were used which is evident from the "DIGITAL FIX"
74. Observing the elections, after a review of Michigan's data a spike of 54,199 votes to Biden. Because it is pushing and pulling and keeping a short distance between the 2 candidates; but then a spike, which is how an algorithm presents; - and this spike means there was a pause and an insert was made, where they insert an algorithm. Block spikes in votes for JOE BIDEN were NOT paper

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

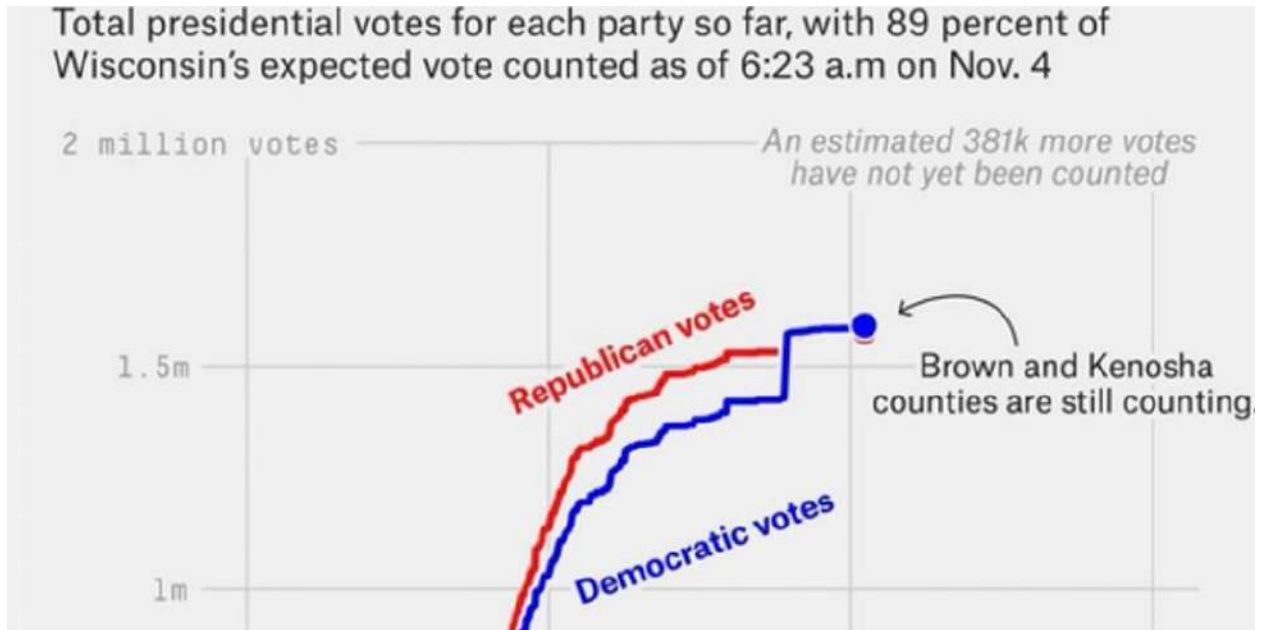
75. I have witnessed the same behavior of the election software in countries outside of the United States and within the United States. In -----, the elections conducted behaved in the same manner by allocating BLOCK votes to the candidate “chosen” to win.
76. Observing the data of the contested states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



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

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

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



81.

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

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

83.

84.

- 90.

Case 2:20-cv-01771-PP Filed 12/01/23 Page 27 of 37 Document 9-13

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.

106.



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

Case 2:20-cv-01771-PP Filed 12/01/23 Page 29 of 37 Document 9-13

*Compact Flash Cards	***SanDisk Ultra: 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 Communique 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)

A. 3EDC LLC

Mailing Address 211 NORTH UNION ST STE 200

City ALEXANDRIA State VA Zip Code 22314

Purpose of Disbursement
WEB SERVICE

Candidate Name

Category/
Type

Office Sought: ☐ House
☐ Senate
☐ President

Disbursement For: 2008
☒ Primary ☐ General
☐ Other (specify) ▼

State: District:

Date of Disbursement

MM / DD / YYYY
03 / 17 / 2008

Transaction ID : SB23.10515

Amount of Each Disbursement this Period

399916.09

Full Name (Last, First, Middle Initial)

B. A FARE EXTRAORDINAIRE

Mailing Address 2035 MARSHALL

City HOUSTON State TX Zip Code 77098

Purpose of Disbursement
FACILITY RENTAL/CATERING

Candidate Name

Category/
Type

Office Sought: ☐ House
☐ Senate
☐ President

Disbursement For: 2008
☒ Primary ☐ General
☐ Other (specify) ▼

State: District:

Date of Disbursement

MM / DD / YYYY
03 / 17 / 2008

Transaction ID : SB23.10049

Amount of Each Disbursement this Period

23697.69

Full Name (Last, First, Middle Initial)

C. ADMINISTAFF

Mailing Address PO BOX 203332

City HOUSTON State TX Zip Code 77216

Purpose of Disbursement
INSURANCE

Candidate Name

Category/
Type

Office Sought: ☐ House
☐ Senate
☐ President

Disbursement For: 2008
☒ Primary ☐ General
☐ Other (specify) ▼

State: District:

Date of Disbursement

MM / DD / YYYY
03 / 05 / 2008

Transaction ID : SB23.10117

Amount of Each Disbursement this Period

483.68

Subtotal Of Receipts This Page (optional).....

424097.46

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

122.

123.

124. AKAMAI Technologies services SCYTL.

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

happen to be using Dominion Machines.

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

"I'm extremely proud to announce that the Soldiers of the 91st Cyber Brigade have completed the construction and rollout of ShadowNet, a world-class enterprise solution designed to propel operational innovation in the field of cyber training," said Col. Adam C. Volant, commander of the 91st Cyber Brigade. "ShadowNet will allow us to leverage the expertise of cyber professionals across our four cyber protection battalions to build Soldier-centric programs and collective training environments that deliver best-in-class training and support." ShadowNet is a custom-built private cloud-based solution that provides 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.

OCTOBER 26, 2020

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

SEPTEMBER 12, 2019

September 2017 Nominative Sergeant: Major Assignments

SEPTEMBER 12, 2019

DA ANNOUNCES ROTATIONAL DEPLOYMENTS

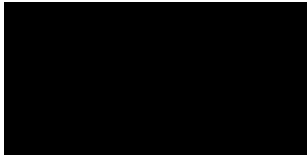
154. Based on my research of voter data – it appears that there are approximately 23,000 residents of a Department of Corrections Prison with requests for absentee ballot in Wisconsin. We are currently reviewing and verifying the data and will supplement.

	23230	Gutierrez	Mary	Jane		(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	

155.

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

Executed this November 29th, 2020.

A large black rectangular redaction box covering the signature area.A small black rectangular redaction box covering a single line of text.

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF TENNESSEE
CHATTANOOGA DIVISION**

TERPSEHORE MARAS,

Plaintiff,

v.

**REPRESENTATIVE STEVE COHEN, US
DOMINION, INC., DOMINION VOTING
SYSTEMS, INC., DOMINION VOTING
SYSTEMS CORPORATION, MEDIA
MATTERS FOR AMERICA and ALI
ABDUL RAZAQ AKBAR A/KA/ ALI
ALEXANDER,**

Defendants.

Case. No. 1:21-cv-00317-DCLC-CHS

District Judge Clifton L. Corker

Magistrate Judge Christopher H. Steger

**PLAINTIFF TERPSEHORE MARAS' SUPPLEMENTAL BRIEF TO
PLAINTIFF'S MOTION TO COMPEL PRODUCTION OF DOCUMENTS
IDENTIFIED IN NON-PARTY J. ALEXANDER HALDERMAN'S SUBPOENA**

COMES NOW Plaintiff Terpsehore Maras and, by and through undersigned counsel and pursuant to LR7.01(d), hereby files Plaintiff Terpsehore Maras' Supplemental Brief to Plaintiff Terpsehore Maras' Supplemental Brief to Plaintiff's Motion to Compel Production of Documents Identified in Non-Party J. Alexander Halderman's Subpoena, and Plaintiff respectfully shows unto this Honorable Court the following:

**I. THE HALDERMAN REPORT IS NECESSARY AS CORROBORATING
EVIDENCE THAT WILL BE USED IN PLAINTIFF'S CASE IN CHIEF IN
PROVING HER DEFAMATION CASE AGAINST THE DEFENDANTS.**

After Plaintiff filed her Motion to Compel Production of Documents Identified in Non-Party J. Alexander Halderman's Subpoena, new information was obtained regarding the apparent election fraud in the 2020 elections. The Plaintiff is a former private intelligence contractor, a whistleblower

and an investigative journalist seeking to remedy the damages to her reputation due to the statements of libel/defamation made by the Defendants. While Dr. J. Alexander Halderman's purported lawyer (David Cross) did not initially object to being counsel for Dr. Halderman, Mr. Cross now objects to being counsel for Dr. Halderman. *See* Exhibit A, E-mail Correspondence from David Cross. As such, Plaintiff's Certificate of Service will be updated to serving Dr. Halderman at his last known address.

As an investigative journalist, Plaintiff has confidential sources that have provided her with both the public seven page summary and a non-public unredacted twenty-four-page summary of the Halderman Report that she has obtained from sources that are protected, as they are privileged and confidential. *See* Exhibit B, September 21, 2021, Declaration of J. Alexander Halderman; *see* Exhibit C, August 2, 2021 Declaration of J. Alexander Halderman. As the court can see, both of Dr. Halderman's reports directly relate to matters contained in Plaintiff's Affidavit, which forms the basis and impetus of the Defendants' defamation. The Plaintiff presented evidence of election fraud in her affidavit and she now needs Dr. Halderman's full unredacted twenty-five-thousand-word report to use as corroborating evidence in proving her defamation case in chief against the Defendants.

Both of Dr. Halderman's election fraud declarations, which are summaries of his details reports and they are proof positive of election fraud, which expressly named the Dominion equipment. Dr. Halderman's Declarations show different perspectives and aspects of the severe vulnerabilities that demonstrate that the right to vote by citizens is unprotected when using Dominion Voting machines. In her Affidavit, Plaintiff testified that vulnerabilities from COTS (components off the shelf) as Shellshock¹ and patch management systems in place are still vulnerable to domestic and foreign hacking and it was made public. Thus far, Georgia's Center for Election Systems were found to have **not** had a patch in either 2016 or 2018. *See* Exhibit D, Georgia election systems could have

¹ Shellshock is a vulnerability that allows systems containing a vulnerable version of Bash to be exploited to execute commands with higher privileges. This allows attackers to potentially take over that system.

been hacked before 2016 vote, <https://www.politico.com/news/2020/01/16/georgia-election-systems-could-have-been-hacked-before-2016-vote-100334> (last visited March 17, 2022).

In fact, Dr. Halderman's two Declarations regarding election fraud concur with Plaintiff's Affidavit and her testimony regarding the COTS (components off the shelf) vulnerabilities. Many states have ignored the patch vulnerabilities of COTS and many state and/or electronic voting systems remain unpatched and are compromised (knowingly or unknowingly), despite the repeated Department of Homeland Security alerts that were sent out to states. This compromise makes the states and/or electronic voting systems vulnerable to Shellshock, which means that the electronic voting machines are at a continuous state of vulnerability to domestic and/or foreign hacking. In addition, it is public knowledge that Georgia's Center for Election Systems were determined to be vulnerable from even before the 2016 elections, which concurs with Plaintiff's sworn testimony of ongoing long standing voting integrity concerns. *See* Exhibit D.

II. ARGUMENT AND CITATION OF AUTHORITY

Pursuant to Local Rule 7.1(d),

Supplemental Briefs. No additional briefs, affidavits, or other papers in support of or in opposition to a motion shall be filed without prior approval of the Court, **except that a party may file a supplemental brief of no more than 5 pages to call to the Court's attention developments occurring after a party's final brief is filed.** Any response to a supplemental brief shall be filed within 7 days after service of the supplemental brief and shall be limited to no more than 5 pages.

Local Rule 7.1(d) (emphasis added).

In the case at bar, this Court should compel Dr. Halderman to produce his full and unredacted Report because it contains corroborating sworn testimony regarding election fraud that Plaintiff needs in order to prove her defamation case against the Defendants. Dr. Halderman's

Report on the election fraud is not privileged. Dr. Halderman's report is discoverable. Plaintiff needs this report as corroborating evidence in order to prove her election fraud case.

Respectfully submitted this *17th* day of March, 2022.

THE NEWMAN LAW FIRM

/s/ Russell A. Newman

Russell A. Newman, BPR No. 033462

6688 Nolensville Road

Suite 108-22

Brentwood, TN 37027

(615) 554-1510 (Telephone)

(615) 283-3529 (Facsimile)

E-mail: russell@thenewmanlawfirm.com

Attorney for Plaintiff Terpsehore Maras

CERTIFICATE OF SERVICE

I, Russell A. Newman, do hereby certify that I am counsel for Plaintiff Terpsehore Maras in the above-captioned matter and that a copy of the **PLAINTIFF TERPSEHORE MARAS' SUPPLEMENTAL BRIEF TO PLAINTIFF'S MOTION TO COMPEL PRODUCTION OF DOCUMENTS IDENTIFIED IN NON-PARTY J. ALEXANDER HALDERMAN'S SUBPOENA** was filed and served via the CM/ECF system for the United States District Court, Eastern District of Tennessee, Chattanooga Division via electronic mail to the following CM/ECF filers:

W. Scott Sims, Esq.
Michael R. O'Neill, Esq.
Sims | Funk, PLC
3322 West End Ave., Suite 200
Nashville, TN 37203
(615) 292-9355 (Telephone)
(615) 649-8565 (Facsimile)
ssims@simsfunk.com
moneill@simsfunk.com
Attorneys for Dominion Defendants

Robb Harvey, Esq.
511 Union Street, Suite 2700
P.O. Box 198966
Nashville, TN 37219-8966
Robb.harvey@wallerlaw.com

Todd B. Tatelman, Esq.
Sarah Clouse, Esq.
5140 O'Neill House Office Building
Washington D.C. 20515
Todd.tatelman@mail.house.gov
Sarah.clouse@mail.house.gov
Attorneys for Congressman Steve Cohen

Moziano S. Reliford, Esq.
William J. Harbison, II, Esq.
1201 Demonbreun Street, Suite 1000
Nashville, TN 37213
treliford@nealharwell.com
jharbison@nealharwell.com
Attorneys for Defendant Media Matters for America

And via E-Mail on the following non-registered CM/ECF filers:

Baron Coleman, Esq.
Three South Jackson Street
P.O. Box 789
Montgomery, AL 36101-0789
baron@baroncoleman.com
Attorney for Defendant Ali Abdul Razaq Akbar

And via U.S. Mail on the following non-registered CM/ECF filers:

Dr. J. Alexander Halderman
632 N 4th Ave.
Ann Arbor, MI 48104

Respectfully submitted this *17th* day of March, 2022.

THE NEWMAN LAW FIRM

By: /s/ Russell A. Newman
Russell A. Newman, BPR # 033462

Subject: RE: Halderman Subpoena: Curling v. Raffensperger

Date: Wednesday, March 16, 2022 at 10:47:01 Central Daylight Time

From: Cross, David D.

To: Russell Newman

Mr. Newman -

I received a hardcopy by regular mail of a motion to compel it appears you have filed against Dr. Halderman in your case. It's unclear why you did not send a courtesy copy by email given we have corresponded by email regarding the subpoena. You also must know that these days folks often are not in the office given many business facilities remain closed with employees working remotely.

In any event, you have not properly served your motion. I did not agree to accept service of the motion on behalf of Dr. Halderman, nor did you ask that I do so. I also do not have authority for him to do that. If you intend to pursue this motion, you need to effect proper service. Please confirm that you will let the court know that the motion has not been served.

I once again encourage you to withdraw this motion and not to pursue the subpoena. Your motion misstates the law and is completely lacking in merit. I also understand that the court has not yet authorized discovery to begin in your case, which makes the subpoena and the motion doubly improper. Please understand that we will seek all fees and costs associated with this subpoena if you persist given its obvious impropriety and the frivolousness of your pursuit in light of the order from Judge Totenberg prohibiting Dr. Halderman from disclosing the report you seek.

Best,
DC

From: Cross, David D. <DCross@mofo.com>

Date: Monday, Feb 14, 2022, 10:56 PM

To: Russell Newman <russell@thenewmanlawfirm.com>

Subject: RE: Halderman Subpoena: Curling v. Raffensperger

Mr. Newman -

The Court repeatedly has ordered the parties and Dr. Halderman not to disclose the report to third parties. It also has repeatedly denied motions by third parties filed in our case for a copy of the report, just as you're seeking. Judge Totenberg's orders are publicly available on the docket in our case.

What authority do you have that one federal judge can order disclosure of something another federal judge has ordered not to be disclosed? You fundamentally misunderstand the jurisdiction of federal courts which is national, not regional as you wrongly posit — which is of course why courts can and often do enter injunctions and other orders that apply across the US, not just in a particular district or circuit.

Again, if you make us brief this in your court, we'll seek fees and costs and any other appropriate relief. A motion to compel would be utterly frivolous.

Best,
DC

From: Russell Newman <russell@thenewmanlawfirm.com>
Date: Monday, Feb 14, 2022, 7:28 PM
To: Cross, David D. <DCross@mofo.com>
Subject: Re: Halderman Subpoena: Curling v. Raffensperger

External Email

Good evening, Mr. Cross.

Thank you for your e-mail. We will direct future correspondence to you as counsel for Dr. Alex Halderman as it relates to Plaintiff's subpoena.

Plaintiff intends to move forward by filing a motion to compel, but before doing so I wanted to have a brief conversation with you in a good faith effort to amicably resolve our dispute without involving our judge. Plaintiff contends that the Northern District of Georgia, Atlanta Division does not have subject matter jurisdiction over the Eastern District of Tennessee, Chattanooga Division. Even at the appellate level, we are in Sixth Circuit Court of Appeals and the Curling case is in the Eleventh Circuit Court of Appeals. As such, neither the district court nor court of appeals have subject matter jurisdiction over our court. Could you please share with us the authority that you are relying on to withhold production of otherwise discoverable items?

Kindly provide us with a response as soon as possible, but in any event please do so by the close of business on Wednesday (02/16/22). In advance, thank you for your consideration of this matter.

Best regards,

Russell A. Newman, Esq.

The Newman Law Firm

6688 Nolensville Road

Suite 108-22

Brentwood, TN 37027

T: [\(615\) 554-1510](tel:(615)554-1510)

F: [\(615\) 283-3529](tel:(615)283-3529)

Email: russell@thenewmanlawfirm.com

<https://www.thenewmanlawfirm.com/>

CONFIDENTIALITY NOTICE: This e-mail communication, including any attached files was sent by or on behalf of the firm and may contain entity to which it is addressed. If you are not the intended recipient or the person responsible for delivering this Communication to the intended recipient, please immediately notify the sender via return email or telephone.

On Mon, Feb 14, 2022 at 1:09 PM Cross, David D. <DCross@mofo.com> wrote:

Mr. Newman –

Please see the attached correspondence.

Best,

DC

DAVID D. CROSS

CHAIR OF ANTITRUST LITIGATION PRACTICE

Partner | Morrison & Foerster LLP

2100 L Street, NW, Suite 900 | Washington, DC 20037

P: +1 (202) 887-8795

mofo.com | [LinkedIn](#) | [Twitter](#)

=====

This message may be confidential and privileged. Use or disclosure by anyone other than an intended addressee is prohibited. If you received this message in error, please delete it and advise the sender by reply email. Learn about Morrison & Foerster LLP's [Privacy Policy](#).

=====

This message may be confidential and privileged. Use or disclosure by anyone other than an intended addressee is prohibited. If you received this message in error, please delete it and advise the sender by reply email. Learn about Morrison & Foerster LLP's [Privacy Policy](#).

EXHIBIT A

**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. My July 1, 2021, expert report describes numerous security vulnerabilities in Georgia's Dominion ICX BMDs. These include flaws that would allow attackers to install malicious software on the ICX, either with temporary physical access (such as that of voters in the polling place) or remotely from election management systems. They are not general weaknesses or theoretical problems, but

rather specific flaws in the ICX software, and I am prepared to demonstrate proof-of-concept malware that can exploit them to steal votes cast on ICX devices.

3. Some of these critical vulnerabilities could be at least partially mitigated through changes to the ICX software if Dominion implemented such changes and jurisdictions deployed them. However, it would likely take months for Dominion to assess the problems, develop responsive software updates, test them, obtain any necessary approvals from the EAC and state-level certification authorities, and distribute the new software to states, as well as additional time for localities to install the changes. But Dominion cannot begin this process, because (to my knowledge) they have yet to learn what is in my report.

4. My analysis also concludes that the ICX is very likely to contain other, equally critical flaws that are yet to be discovered. Jurisdictions can mitigate this serious risk through procedural changes, such as reserving BMDs for voters who need or request them. Election officials cannot make an informed decision about such urgent policy changes or any other mitigations until they have assessed the technical findings in my report. However, to my knowledge, the Georgia Secretary of State's Office has yet to even request access to it, despite Plaintiffs' repeated offers to make it available to appropriate individuals at the Secretary's Office.

5. Nor do these problems affect Georgia alone. In 2022, the ICX will be used in parts of 16 states.¹ Nevada will use it as the primary method of in-person voting in certain areas of the state. Louisiana is slated to use it for early voting in a DRE configuration where there is not even a paper trail. It will be used for accessible voting in Alaska and large parts of Arizona, California, Colorado, and Michigan. It will also see some use in parts of Illinois, Kansas, Ohio, Missouri, New Jersey, Pennsylvania, Tennessee, and Washington State. Officials in these jurisdictions too must act to update the software and their procedures, but they cannot do so without information about the problems. Continuing to conceal those problems from those who can—and are authorized to—address them, to the extent possible, serves no one and only hurts voters (and heightens the risk of compromise in future elections).

6. The most effective way to ensure that the necessary information gets to the parties responsible (without also falling into the wrong hands) would be to share my report with the Cybersecurity and Infrastructure Security Agency (CISA), which operates a Coordinated Vulnerability Disclosure (CVD) program for just this purpose. CISA is a federal agency that collaborates with state and local governments, election officials, federal partners, and vendors to manage risks to U.S. election

¹ See Verified Voting, “Verifier Search – November 2022,” <https://verifiedvoting.org/verifier/#mode/search/year/2022/model/ImageCast%20X>.

infrastructure.² Under CISA's CVD process, agency staff would independently validate the vulnerabilities, work with Dominion to develop software updates as necessary, and facilitate sufficient time for affected states and localities to apply mitigation strategies.³ CISA strives to disclose "accurate, neutral, objective information focused on technical remediation and mitigation" and to "correct misinformation where necessary,"⁴ making it well qualified to coordinate the disclosure of such sensitive vulnerabilities.

7. Geoff Hale, Director of CISA's Election Security Initiative, has confirmed to me that, if the Court permits it, the agency would be willing to receive my expert report and carry out coordinated vulnerability disclosure activities as appropriate (see Exhibit 1). Mr. Hale requests that I and my assistant Drew Springall be available for consultation with CISA during the CVD process, which we would be willing to do subject to the Court's permission.

8. Informing responsible parties about the ICX's vulnerabilities is becoming more urgent by the day. Foreign or domestic adversaries who are intent on

² Cybersecurity and Infrastructure Security Agency, "Election Infrastructure Initiative," <https://www.cisa.gov/election-security>.

³ Cybersecurity and Infrastructure Security Agency, "Coordinated Vulnerability Disclosure Process," <https://www.cisa.gov/coordinated-vulnerability-disclosure-process>.

⁴ *Id.*

attacking elections certainly could have already discovered the same problems I did, yet Georgia's 2022 primaries are less than nine months away, and other states that use the ICX will conduct high-profile elections even sooner. It is important to recognize the possibility that nefarious actors already have discovered the same problems I detail in my report and are preparing to exploit them in future elections. Providing my report to CISA through its CVD program will ensure that Dominion and affected jurisdictions are able to begin appropriate mitigations as soon as possible. Continuing to withhold my report from CISA puts voters and election outcomes in numerous states at unnecessary, and avoidable, risk.

9. I understand that State Defendants object to disclosure to CISA on the argument that my report should be used only for this lawsuit. But this ignores the implications of my report and my role in this matter. I am not a party to this lawsuit. I am an independent expert who was engaged to conduct an impartial assessment of the security and reliability of the Dominion BMD system, using (in part) election equipment that the Court ordered I be provided. I have done that, as reflected in my lengthy, detailed report and other submissions in this matter. As an independent expert and member of the election integrity community, I have a professional obligation to take appropriate steps to ensure that the severe vulnerabilities my report describes are properly remediated, to the extent possible, and that those tasked with

election security and administration across the country have the information they need to make responsible, informed decisions about election procedures, including the equipment used, the manner and purposes for which it is used (including whether it is used at all), the steps needed to secure that equipment and other aspects of the election systems in which it is used, and more. In short, my professional obligations do not end at the boundaries of this lawsuit, nor do the serious risks to voters and elections that my report discusses in depth. Additionally, I can imagine no prejudice to anyone in this lawsuit (or beyond) from disclosure of my report to CISA, nor am I aware of any claim of prejudice from any of the parties.

10. I of course have complied, and will continue to comply, with all directives from the Court regarding disclosure of my work in this matter. I submit this declaration to explain why I believe disclosure of my report to CISA is critically important (and not just for Georgia) and to respectfully ask that the Court allow that disclosure, rather than accept State Defendants' position that my findings must not be shared beyond the confines of this lawsuit, including with those who are authorized to address the vulnerabilities with the ICX and stand ready to do so. If my findings regarding the ICX actually present no meaningful risks to voters and election outcomes and therefore require no remediation, as I gather State Defendants would have the Court believe, CISA is well positioned to determine that. If, on the other

hand, my findings do warrant remediation, as I believe they do, then CISA is well positioned to work with Dominion and the appropriate authorities around the country to implement remedial measures. I can see no reason to prevent (or further delay) that important work for future elections. And I note that none of State Defendants' experts have disputed my findings regarding the ICX machines. Only Dr. Juan Gilbert has responded to my sealed report, and he has not examined the machines (or used them) to my knowledge.

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 21st day of September, 2021 in Ann Arbor, Michigan.



J. ALEX HALDERMAN

EXHIBIT 1



J. Alex Halderman <halderman@gmail.com>

Vulnerability Disclosure

Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>
To: "J. Alex Halderman" <jhalderm@umich.edu>
Cc: Andrew Springall <andrew.springall@gmail.com>

Thu, Aug 19, 2021 at 12:15 PM

Prof. Halderman,

Thank you for your email. Yes, CISA would be willing to receive the report regarding possible vulnerabilities in election infrastructure for inclusion in CISA's Coordinated Vulnerability Disclosure (CVD) process and would carry out any further coordinated disclosures activities as appropriate. As we share on our public website (<https://www.cisa.gov/coordinated-vulnerability-disclosure-process>), CISA's CVD program coordinates the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s). Note that part of our process may also involve validating any alleged vulnerabilities, planned mitigations, remediations, or patches with the security researcher who discovered the alleged vulnerability, so we would appreciate if you could continue to be available for consultation during the CVD process as well.

As shared on our website, please submit any vulnerability reports for CVD coordination using the form here:
<https://www.kb.cert.org/vuls/report/>

Best,

Geoff

From: J. Alex Halderman <jhalderm@umich.edu>
Sent: Wednesday, August 18, 2021 4:37 PM
To: Hale, Geoffrey <Geoffrey.Hale@cisa.dhs.gov>
Cc: Andrew Springall <andrew.springall@gmail.com>
Subject: Vulnerability Disclosure

CAUTION: This email originated from outside of DHS. DO NOT click links or open attachments unless you recognize and/or trust the sender. Contact your component SOC with questions or concerns.

Dear Mr. Hale,

We are writing to you in your capacity as Director of the Election Security Initiative at the federal Cybersecurity and Infrastructure Security Agency (CISA).

We understand that the Election Security Initiative at CISA works to ensure the physical security and cybersecurity of the systems and assets that support the Nation's elections, including through detection and prevention, information sharing and awareness, and incident response.

As you may be aware from recent press reports, one of us (Halderman) is presently serving as an expert witness for the plaintiffs in *Curling v. Raffensperger* (Civil action no. 1:17-CV-2989-AT, N.D. Ga.), a case that concerns the security of Georgia's election system. A year ago, the court granted plaintiffs access to an ICP ballot scanner and ICX ballot marking device as used in Georgia in order to test their security. Following months of analysis, on July 1, Dr. Halderman submitted an expert report that describes several very serious vulnerabilities we found in the equipment, which, to our knowledge, have not been previously documented or disclosed.

Given the nature of the vulnerabilities and the time that would be necessary to mitigate them before the 2022 midterm elections, we believe it is critical for Dominion and affected jurisdictions (which include Georgia and parts of many other states) to begin taking responsive action soon. It is also vitally important to prevent information sufficient to exploit the vulnerabilities from falling into the wrong hands, and to avoid fueling election-related misinformation if possible.

Currently, disclosure of the expert report to anyone other than outside litigation counsel for the parties is strictly prohibited by the Court's protective order and by recent directives from the judge. However, if permitted by the Court, we would like to share the report with CISA and ask your agency to carry out appropriate further disclosure of the information it contains to Dominion and affected jurisdictions as you see fit, under CISA's coordinated vulnerability disclosure (CVD) program (<https://www.cisa.gov/coordinated-vulnerability-disclosure-process>).

We understand that under this process, CISA will work with the vendor (Dominion) for mitigation development and the issuance of patches or updates and to facilitate sufficient time for affected end users to obtain, test, and apply mitigation strategies. We further understand that CISA strives to disclose "accurate, neutral, objective information focused on technical remediation and mitigation" and to "correct misinformation where necessary".

Please confirm that CISA would be an appropriate agency to handle coordinated vulnerability disclosure for election infrastructure under these circumstances, and that you would be willing to receive the report (subject to the Court's permission) and carry out further disclosures as you deem appropriate.

Sincerely,

J. Alex Halderman

Drew Springall

**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 Niese, “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

