




Transcription of Highlight Text:

Effective Through February 24, 2017

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

10.

United States Department of Commerce
National Institute of Standards and Technology



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 Certificate dated January 2009).*

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



John S. Gammie
For the National Voluntary Laboratory Accreditation Program

11. VSTL's are VERY important because equipment vulnerabilities allow for deployment of algorithms and scripts to intercept, alter and adjust voting tallies.

12. There are only TWO accredited VSTLs (VOTING SYSTEM TEST LABORATORIES). In order

to meet its statutory requirements under HAVA § 15371(b), the EAC has developed the EAC's Voting System Test Laboratory Accreditation Program. The procedural requirements of the program are established in the proposed information collection, the EAC Voting System Test Laboratory Accreditation Program Manual. Although participation in the program is voluntary, adherence to the program's procedural requirements is mandatory for participants. The procedural requirements of this Manual will supersede any prior laboratory accreditation requirements issued by the EAC. This manual shall be read in conjunction with the EAC's Voting System Testing and Certification Program Manual (OMB 3265-0019).

U.S. Election Assistance Commission

 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 I 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 any of the state requirements. MICA. 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/sog/1607.7-127-1633_8716_45458---,00.html

U.S. Election Assistance Commission



WISCONSIN

State Participation:

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

Applicable Statute(s):

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

Applicable Regulation(s):

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

State Certification Process:

The Board of Election Commissioners accepts applications for the approval of electronic voting systems. Once the application is completed, the vendor must set up the voting system for three mock elections using; (1) offices, (2) referenda questions and (3) candidates. A panel of local election officials can assist the Board in the review of the voting system. The Board conducts the test using a mock election for the partisan primary, general election, and nonpartisan election. The Board may also require that the voting

system be used in an actual election as a condition of the approval. WIS. ADMIN. CODE GAB §§ 7.01, 7.02 (2009).

Fielded Voting Systems:

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

U.S. Election Assistance Commission

 **GEORGIA**

State Participation:

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

Applicable Statute(s):

“Any person or organization owning, manufacturing, or selling, or being interested in the manufacture or sale of, any voting machine may request the Secretary of State to examine the machine. Any ten or more electors of this state may, at any time, request the Secretary of State to reexamine any voting machine previously examined and approved by him or her. Before any such examination or re-examination, the person, persons, or organization requesting such examination or re-examination 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 S 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 de-

termination on whether to certify the voting system.
GA. COMP. R. & RES. 590-8-1-.01(2009).

Fielded Voting Systems:

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

U.S. Election Assistance Commission

 **PENNSYLVANIA**

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/HowtoVotehabid/74/language/en-US/Default.aspx>

U.S. Election Assistance Commission

 **ARIZONA**

State Participation:

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

Applicable Statute(s):

“On completion of acquisition of machines or devices that comply with HAVA, machines or devices used at any election for federal, state or county offices may only be certified for use in this state and may only be used in this state if they comply with HAVA and if those machines or devices have been tested and approved by a laboratory that is accredited pursuant to HAVA.” ARIZ. REV. STAT. § 16-442(13)(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/electiort/equipment/default.htm>

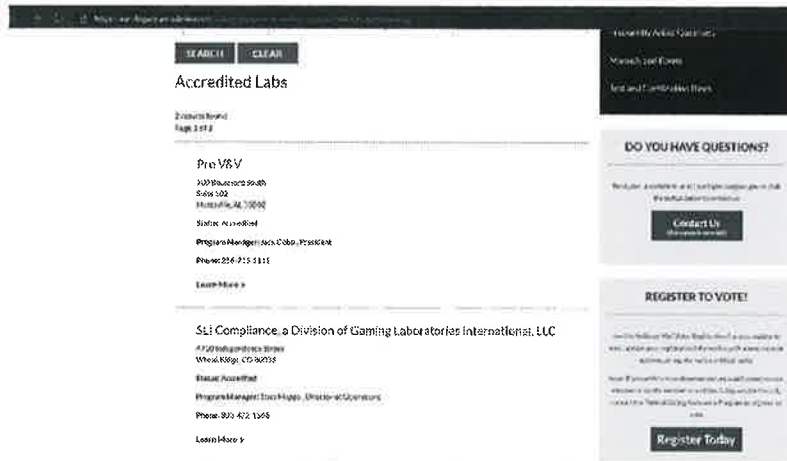
[* * *]

17.

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

App.360a

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.



Transcription:

SEARCH

CLEAR

ACCREDITED LABS

2 results found.

Page 1 of 3

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 30033

Status: Accredited

Program Manager: Traci Mapps,
Director of Operations

Phone: 303-422-1666

[Learn More>](#)

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

21. "Wyle became involved with the testing of electronic voting systems in the early 1990's and has tested over 150 separate voting systems. Wyle was the first company to obtain accreditation by the National Association of State Election Directors (NASSED). Wyle is accredited by the Election Assistance Commission (EAC) as a Voting System Testing Laboratory (VSTL). Our scope of accreditation as a VSTL encompasses all aspects of the hardware and software of a voting

machine. Wyle also received NVLAP accreditation to ISO/IEC 17025:2005 from NIST.” Testimony of Jack Cobb 2009

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

23. The proprietary voting system software is done so and created with cost efficiency in mind and therefore relies on 3rd party software that is AVAIL-ABLE 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 com-

ponents 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.

Asian offices

Akamai Technologies - India

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


Akamai Technologies - China

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

Akamai Japan K.K.

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

Akamai Technologies - Singapore

Akamai, Regus Centre, 36-01 UOB Plaza 1
80 Raffles Place
Singapore 048624
 Driving directions


Akamai Technologies - Australia and New Zealand

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

27.

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

IP	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



Transcription:

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.

U.S.A. 4.30.228.74

ISP/Organization: Level 3 Communications

Location: Alexandria 22304, Virginia (VA), United States (US)

Latitude: 38.8115/38°48'41" N

Longitude: -77.1285/77°7'42" W

Timezone: America/New_York

Local Time: Thu, 12 Jul 2018 19:27:40-0400

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

29.

{ Image with unclear text and graphic omitted }

30.

{ Image with unclear text and graphic omitted }

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 commu-

App.367a

nications 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.

Basic Tracking Info

Domain: Michigan.gov

IP Address: 23.78.81.34

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 Location: Unknown

ISP: Akamai Technologies

Organization: Akamai Technologies

AS Number: AS1299 Tella Company AB

something went wrong! something went wrong!

Time Zone: America/North_Dakota/Center

Local Time: 13:48:46

Timezone GMT offset: -21600

Sunrise/Sunset: 07:27 / 17:12

Extra Information for an IP: Michigan.gov

Continent Lat/Lon: 46.07305 /-100.546

Country Lat/Lon: 38 / .98

City Lat/Lon: (37.751) / (-91.822)

IP Language: English

Geolocation on IP Map

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.

App.370a

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-Swiss-Post 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.

App.371a

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).

51.

{ Complex Flowchart with small text omitted }

App.373a

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

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

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

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

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

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

56.

Commitment_{CRYPT} = CM_c

Scytl sets commitment - simple math ↓

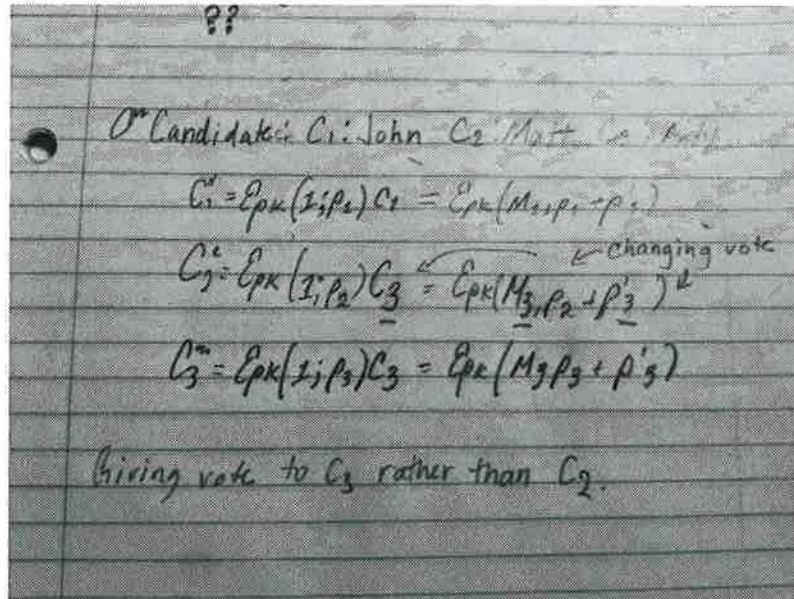
$$CM_c(\vec{a}; r) = H(G^{\vec{a}}) = H \cdot G^{\vec{a}}$$

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

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

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

57. Within the trapdoor this is how the algorithm behaves to move the goal posts in elections without being detected by this proof. During the mixing phase this is the algorithm you would use to “reallocate” votes via an algorithm to achieve the goal set.



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

App.377a

elections in 2020 confirm the deployment of an algorithm due to the BEHAVIOR which is indicative of an algorithm in play that had no pivoting parameters applied.

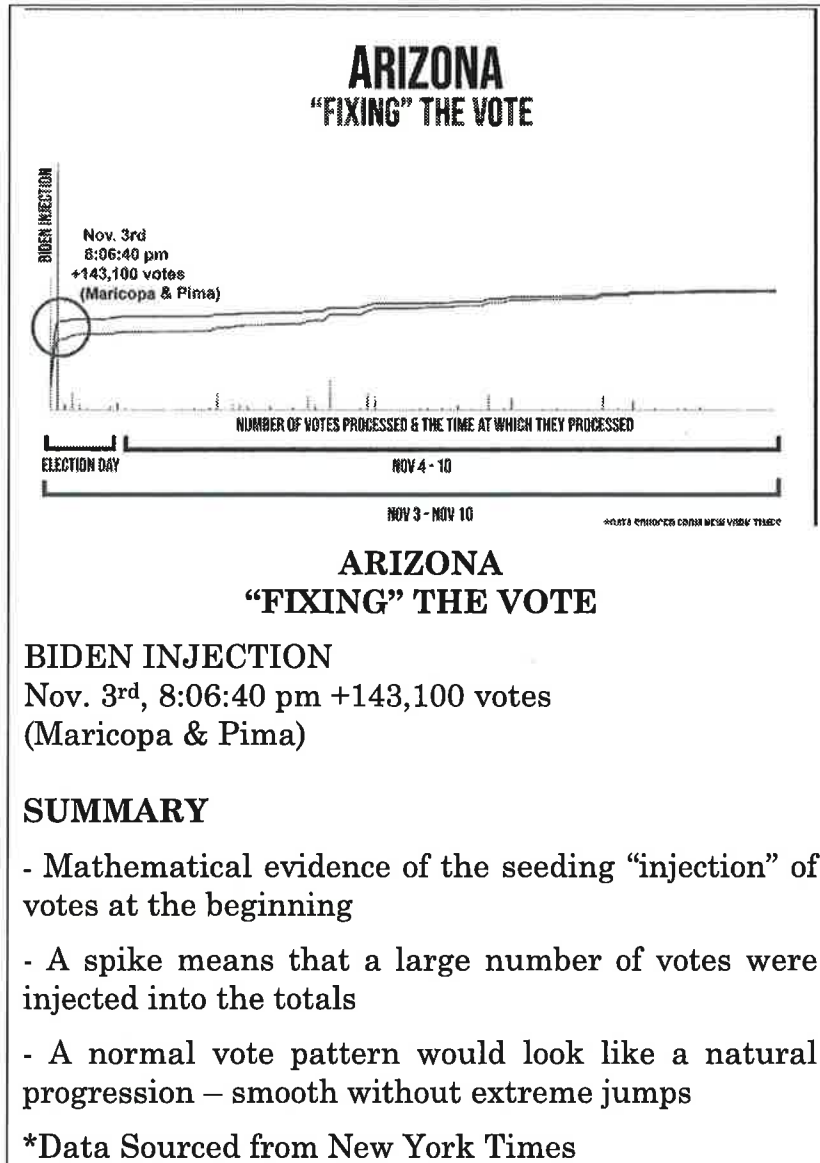
65. The behavior of the algorithm is that one point (B) is the greatest point within the allocated set. It is the greatest number within the A B points given. Point A would be the smallest. Any points outside the A B points are not necessarily factored in yet can still be applied.

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

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

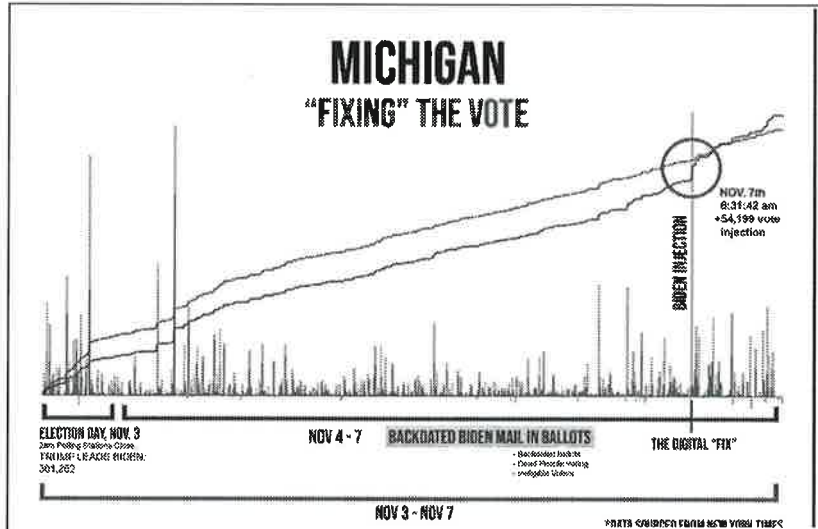
68. Post block allocation of votes the two points of the algorithm were narrowed ensuring a BIDEN win hence the observation of NO Trump Votes and some BIDEN votes for a period of time.

69.



70. Gaussian Elimination without pivoting explains how the algorithm would behave and the

election results and data from Michigan confirm FAILURE of algorithm.



MICHIGAN "FIXING" THE VOTE

Election Day, Nov. 3 2am Polling Stations Close
Trump Leads Biden 301,262

Nov. 4-7, Backdated Biden Mail in Ballots Results in
-Backdated ballots
-Dead People Voting
-Ineligible Voters

BIDEN INJECTION

Nov. 7th, 6:31:42 am +54,199 vote Injection

THE DIGITAL "FIX" NOV 3 -

NOV 7 6:31:42 am +54,199 vote injection

SUMMARY

- Trump wins on election night / Polling locations in

Detroit shut down at 2am

- Ballot counters told to go home / Voting station windows covered
- Dominion Exec shows up in Detroit polling station after midnight
- Trump's election night lead disappears / Biden "INJECTION" appears

*Data Sourced from New York Times

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 :

72.

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

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,

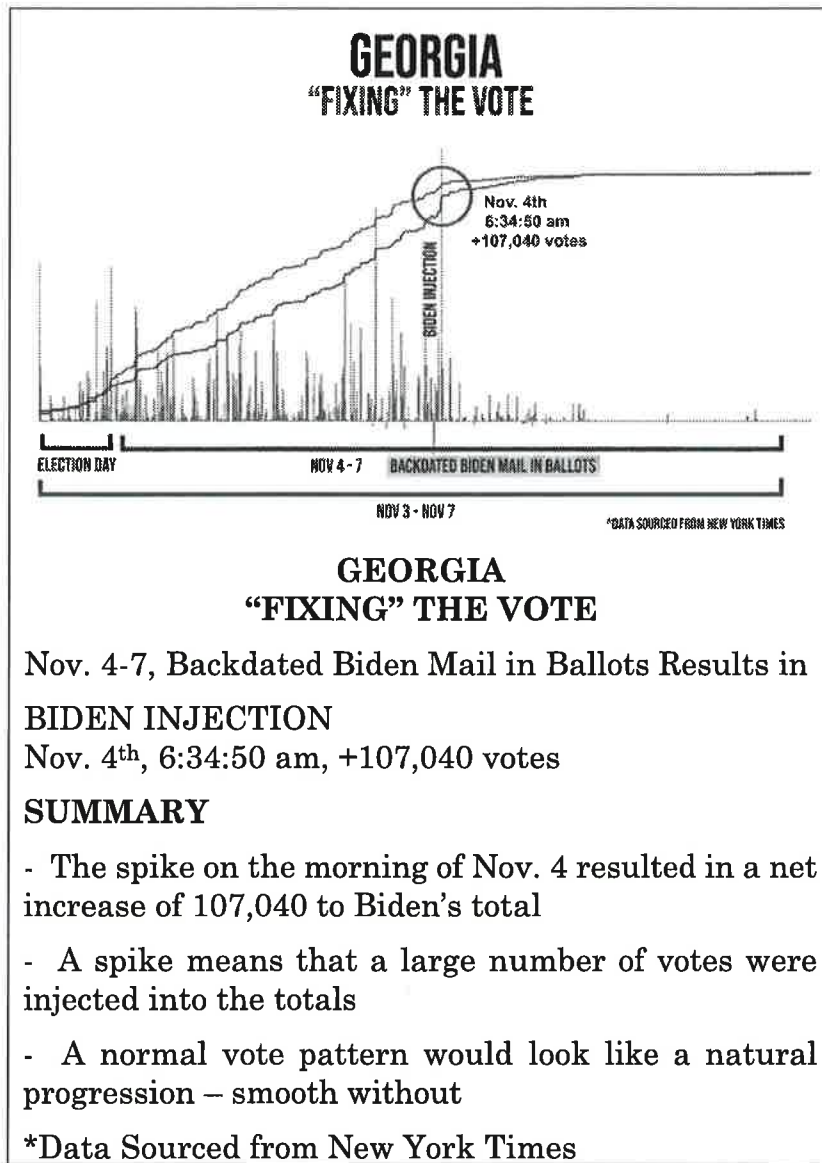
where they insert an algorithm. Block spikes in votes for JOE BIDEN were NOT paper ballots being fed or THUMB DRIVES. The algorithm block adjusted itself and the PEOPLE were creating the evidence to BACK UP the block allocation.

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

App.383a

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.

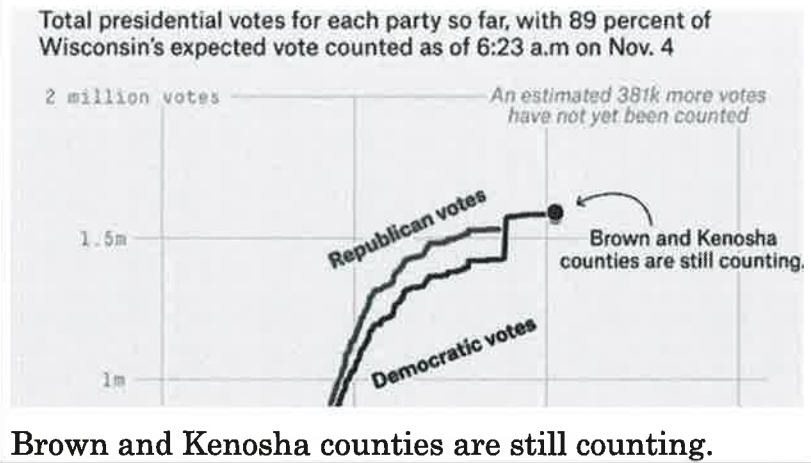
80. In the state of Wisconsin, we observed a considerable BLOCK vote allocation by the algorithm at the SAME TIME it happened across the nation. All systems shut down at around the same time.

81.

Transcription:

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

An estimated 381k more votes have not yet been counted.



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

83.

{ Detailed data table with illegible text omitted }

84.

{ Detailed data table with illegible text omitted }

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

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

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

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

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

90.

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

President Obama and Vice President Biden have made U.S. support for Ukraine an urgent priority as the Ukrainian government works to establish security and stability, pursue democratic elections and constitutional reform, revive its economy, and ensure government institutions are transparent and accountable to the Ukrainian people. Ukraine embarks on this reform path in the face of severe challenges to its sovereignty and territorial integrity, which we are working to address together with Ukraine and our

partners in the international community. The United States is committed to ensuring that Ukrainians alone are able to determine their country's future without intimidation or coercion from outside forces. To support Ukraine, we are today announcing a new package of assistance totaling **\$50 million** to help Ukraine pursue political and economic reform and strengthen the partnership between the United States and Ukraine.

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

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

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

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

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

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

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

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

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

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

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

102. If the “accredited” non-federal entities have NOT received EAC accreditation this is a failure of the

states to uphold their own states standards that are federally regulated.

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

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

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

106.



Transcription of highlighted text:

Effective date: 2020-03-26 through 2021-03-31

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

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

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

110.

* Compact Flash Cards

*** SanDisk Ultra:

SDCFHS-004G

SDCFHS-008G

RiDate:

CFC-14A

RDF8G-233XMCB2-1

RDF16G-233XMCB2-1

RDF32G-233XMCB2-1

SanDisk Extreme:

SDCFX-016G

SDCFX-032G

SanDisk:

SDFAA-008G

Memory device for ICP and ICR 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

App.391a

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

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

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

114.



Transcription of highlighted text:

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

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.

122.

123.

Image# 13941014755

SCHEDULE B-P

ITEMIZED DISBURSEMENTS

FOR LINE NUMBER

(check only one)

23

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 or political committee to solicit contribution from such committee.

Name of Committee (In full)

John McCain 200, Inc.

Full Name

A. 3EC LLC

Date of Disbursement

03 17 2008

Mailing Address

211 North Union St Ste 200

City

Alexandria

State

VA

Zip Code

22314

Purpose of Disbursement

Web Service

Disbursement for: 2008

Primary

Transaction ID: SB23.10515

Amount of Each Disbursement this period

399916.09

B. Fare Extraordinaire

Mailing Address: 2035 Marshall

City: Houston

State: TX

Zip Code: 77098

Date of Disbursement

03 17 2008

Purpose of Disbursement

Facility Rental/Catering

Transaction ID: SB23.10049

23697.69

Disbursement For: 2008

Primary

C. ADMINISTAFF

Mailing Address: PO BOX 203332

City: Houston

State: TX

Zip Code: 77216

Date of Disbursement

03 05 2008

Transaction ID: SB23.10117

489.68

Disbursement For: 2008

Primary

Subtotal of Receipts This Page (optional)

424097.46

124. AKAMAI Technologies services SCYTL.

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

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

127.

{ Complex diagram with illegible text omitted }

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

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

130.

Hosts	Services	Traceroute
wisconsin.gov (165.189.137)	3.00	207.89.33.137
	4.00	10.40.50.7
	5.00	172.22.7.24
	6.00	206.126.236.37
	7.00	10gigabitethernet2-2.core1.ash1.he.net
	8.00	100ge1-1.core2.chi1.he.net
	9.00	100ge15-2.core1.chi1.he.net
	10.00	100ge8-1.core1.man1.he.net
	11.00	216.66.73.242
	12.00	airstream-communications-llc.10gigabitethernet2-20.core1.man
	13.00	air-cpdg-asr-to-mdsn.airstreamcomm.net.130.33.64.in-addr.arp
	14.00	win-retail-wi-dos-001-2.direct.airstreamcomm.net
	15.00	<unknown>
		<unknown>
		165.189.150.147

App.397a

131. AKAMAI Technologies has locations around the world.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

152. GEMS ----- General Hayden.

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

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

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

October 26, 2020

**U.S. Army STAND-TO! |
Army Readines Training**

September 12, 2019

September 2017

Nominate Sergeants 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.

{ Dense data table omitted }

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



Terpsehore P. Maras

App.401a

**REQUEST FROM THE INFORMATION
TECHNOLOGY DEPARTMENT TO APPROVE
THE MEMBERSHIP AGREEMENT WITH
MULTI-STATE INFORMATION SHARING
AND ANALYSIS CENTER
(MARCH 2, 2018)**



**BRAZOS COUNTY
BRYAN, TEXAS**

DEPARTMENT: Information Technology

NUMBER:

DATE OF COURT MEETING: 3/13/2018

ITEM: Request from the Information Technology Department to approve the membership agreement with Multi-State Information Sharing and Analysis Center.

TO: Commissioners Court

FROM: Eric V. Caldwell, CGCIO

DATE: 03/02/2018

FISCAL IMPACT: False

BUDGETED: False

DOLLAR AMOUNT: \$0.00

SOURCE OF FUNDS: There is no cost to join MS-ISAC.

App.402a

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a voluntary and collaborative effort based on a strong partnership between the Center for Internet Security and the Office of Cybersecurity and Communications within the U.S. Department of Homeland Security (DHS). The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal (SLTT) governments. Through its state-of-the-art 24/7 Security Operations Center, the MS-ISAC serves as a central resource for situational awareness and incident response for SLTT governments. *There is no cost to be a member.*

NOTES/EXCEPTIONS:

Membership in the MS-ISAC will give us access to several important benefits such as:

- Cybersecurity advisories & daily tips
- Cyber event notifications
- Awareness/education materials
- Network monitoring
- Vulnerability assessment services
- Secure portals for communication & document sharing
- Malicious Code Analysis tools
- Assistance with cybersecurity incident emergency response

ACTION REQUESTED OR ALTERNATIVES:

Sharing information with MS-ISAC is completely voluntary

App.403a

We request the approval of the MS-ISAC membership agreement.

ATTACHMENTS:

File Name – MS-ISAC Overview.pdf

Description – Overview of MS-ISAC

Type – Backup Material

File Name – MS ISAC Member Agreement-Brazos County TX.pdf

Description – Membership Agreement

Type – Exhibit

**CENTER FOR INTERNET SECURITY
MULTI-STATE ISAC
Member Agreement**

This Agreement (“Agreement”) is made between Brazos County, TX and the Multi-State Information Sharing and Analysis Center of the United States (MS-ISAC), a division of the Center for Internet Security

The MS-ISAC will enable information sharing, analysis, gathering and distribution in a secure manner using facilities and methods designed to permit individual Members to submit information about security threats, vulnerabilities, incidents, and solutions securely. Only MS-ISAC members have access to review and retrieve this information. When submitting information to the MS-ISAC, Primary Custodians will identify information to the MS-ISAC in the following categories

App.404a

Category A. information that is provided only to the MS-ISAC and will not be shared with the MS-ISAC members or others except as authorized by the Primary Custodian Category A information also consists of any non-categorized information provided to the MS-ISAC and/or pre-cleansed category B information

Category B: information which is shared with the MS-ISAC and in consultation with the Primary Custodian s cleansed by the MS-ISAC of all identifying information and then, consistent with applicable laws, will be shared only with MS-ISAC members, or the Department of Homeland Security consistent with paragraph six (6).

Category C information which is shared with the MS-ISAC and does not need to be cleansed and may be shared within the MS-ISAC and outside the MS-ISAC as appropriate

MS-ISAC members acknowledge that Primary Custodian has certain cyber and/or critical infrastructure information and material that is exempt from disclosure to the public or other unauthorized persons under federal or state laws including the Homeland Security Act of 2002 (6 USC § 133) MS-ISAC members may provide access to this information and material in order to facilitate interstate communication regarding cyber and/or critical infrastructure readiness and response efforts These efforts include, but are not limited to, disseminating early warnings of physical and cyber system threats, sharing security incident information between U S states, territories, the District of Columbia, tribal nations and local governments, providing trends and other analysis for security planning, and distributing current proven security practices and suggestions As a participating member of the MS-

ISAC, Primary Custodian agrees that when sharing this information with MS-ISAC members it will do so through the MS-ISAC in accordance with the categories established in this document. MS-ISAC members agree to the terms and conditions contained in this Agreement.

NOW THEREFORE, in consideration of the above promises recited herein, the parties agree to the following

Definitions:

1. Primary Custodian — the entity that developed or owns the Data. Each collection of Data (database, file, etc) shall have a single Primary Custodian

2. MS-ISAC members — the members (U.S. states, territories, the District of Columbia, tribal nations and local governments) who may be in possession or use of Data acquired from the Primary Custodian or from the MS-ISAC.

Purpose:

3. MS-ISAC members acknowledge that the protection of Category A information is essential to the security of Primary Custodian and the mission of the MS-ISAC. The purpose of this Agreement is to enable Primary Custodian to make disclosures of Category A information to MS-ISAC while still maintaining rights in, and control over, Category A information. The purpose is also to preserve confidentiality of the Category A information and to prevent its unauthorized disclosure. It is understood that this Agreement does not grant MS-ISAC or members an express or implied license or an option on a license, or any other

App.406a

rights to or interests in the Category A information, or otherwise If Primary Custodian retracts any information it sent to the MS-ISAC, then, upon notification by the Primary Custodian, the MS-ISAC will destroy such information and all copies thereof, and notify MS-ISAC members to destroy the information If an MS-ISAC member is unable to destroy the information based on applicable law, then the member will continue to maintain the confidentiality of the information consistent with this agreement. Upon receiving such notification, MS ISAC members will destroy such information and all copies thereof

MS-ISAC and Member Duties:

4. MS-ISAC and members who are authorized by the Primary Custodian to receive Category A information shall, and shall cause their contractors, subcontractors, agents or any other entities acting on their behalf (hereinafter referred to as the "Affiliates") to

- (a) copy, reproduce or use Category A information only for the purposes of the MS-I SAC mission and not for any other purpose unless specifically authorized to do so in writing by Primary Custodian; and
- (b) not permit any person to use or disclose the Category A information for any purpose other than those expressly authorized by this Agreement; and
- (c) implement physical, electronic and managerial safeguards to prevent unauthorized access to or use of Category A information

App.407a

Such restrictions will be at least as stringent as those applied by the MS-ISAC and/or members to their own most valuable and confidential information

MS-ISAC agrees to promptly notify Primary Custodian of any unauthorized release of Category A information.

5. MS-ISAC and members will not remove, obscure or alter any notice of patent, copyright, trade secret or other proprietary right from any Category A information without the prior written authorization of Primary Custodian

Multi-State ISAC Duties:

6. The MS-ISAC and members may share with the Department of Homeland Security (DHS) pursuant to 6 U S C § 133, Category A, B, and C information, unless the Primary Custodian has designated in writing that the information in question cannot be shared with our federal partners All other information is voluntarily submitted and may be shared with the Federal Government with expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002

7. If any third party makes a demand for any Category A or B information, the MS-ISAC or member shall immediately forward such request to the Primary Custodian and consult and cooperate with the Primary Custodian and will make reasonable efforts, consistent with applicable law to protect the confidentiality of the information Primary Custodian will, as needed, have the opportunity to seek judicial or other appropriate avenues of redress to prevent any release

8. In non-emergency situations, as part of its multi-state communication sharing efforts, the MS-ISAC may prepare written reports. For such reports, the Primary Custodian shall be provided a period of time to review such reports, papers, or other writings and has the right to edit out its Category A information, correct factual inaccuracies, make recommendations and comments to the content of the report, and append comments to the final version of the report. The MS-ISAC members and Primary Custodian agree to work together in good faith to reach mutually agreed upon language for the report. If the parties are unable to reach agreement on an issue, Primary Custodian has the right to edit out its Category A information.

General Terms:

9. Should any court of competent jurisdiction consider any provision of this Agreement to be invalid, illegal, or unenforceable, such provisions shall be considered severed from this Agreement. All other provisions, rights, and obligations shall continue without regard to the severed provision(s).

10. The term of the Agreement shall continue so long as Primary Custodian remains a member of the MS-ISAC, and paragraph 3 the obligations of confidentiality as provided herein shall survive the expiration of this Agreement.

11. This Agreement will be construed and enforced in all respects in accordance with United States (U S) federal law or other applicable laws as addressed herein.

12. This Agreement contains the entire understanding between the parties with respect to the

App.409a

proprietary information described herein and super-
sedes all prior understandings whether written or oral.
Any modification, amendment, assignment or waiver
of the terms of this Agreement shall require the
written approval of the authorized representative of
each party

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

AGREED BY

Primary Custodian:

/s/ Duane Peters

County Judge

Date: 3/13/18

**Center for Internet Security
Multi-State ISAC Division**

/s/ Thomas Duffy

MS-ISAC Chair

Date: 3/19/2018

App.410a



**BRAZOS COUNTY
BRYAN, TEXAS**

DEPARTMENT: Purchasing

NUMBER:

DATE OF COURT MEETING: 3/13/2018

ITEM: Order exempting the contract with Argyle Security from competitive solicitation pursuant to the Texas Local Government Code 262.024(a)(7)(A).

TO: Commissioners Court

FROM: Mandy Rutledge

DATE: 03/07/2018

FISCAL IMPACT: False

BUDGETED: False

DOLLAR AMOUNT: \$0.00

ACTION REQUESTED OR ALTERNATIVES:

Order exempting the contract with Argyle Security from competitive solicitation pursuant to the Texas Local Government Code 262.024(a)(7)(A).

ATTACHMENTS:

File Name – Order-Sole Source-
Securitycontrolupgrade.docx

Description – Order

Type – Backup Material

App.411a

File Name – 1Attestation.pdf

Description – Attestation

Type – Backup Material

File Name – 1Attestation.pdf

Description – Attestation

Type – Backup Material

App.412a

**DENTON COUNTY
COMMISSIONERS COURT**

08/06/2019

Court Order Number 19-0539

14. A. The Order:

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

Motion by Mitchell Seconded by Marchant

County Judge Andy Eads Yes X

Commissioner Pet No 1 Hugh Coleman Yes X

Commissioner Pet No 2 Ron Marchant Yes X

Commissioner Pet No 3 Bobbie J. Mitchell Yes X

Commissioner Pet No 4 Dianne Edmondson Yes X

Motion Carried 5-0-0

Other Action:

BY ORDER OF THE COMMISSIONERS COURT:

[signatures not legible]

[SEAL]

**MEMORANDUM OF AGREEMENT BETWEEN
THE CENTER FOR INTERNET SECURITY/
ELECTION INFRASTRUCTURE
INFORMATION SHARING AND
ANALYSIS CENTER AND FOR
CYBERSECURITY SERVICES
(Federally Funded Election Services)**

Denton County, Texas

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

WITNESSETH:

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

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

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

App.414a

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

I. Purpose

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

II. Definitions

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

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

III. Consideration

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

IV. Responsibilities

Appendix A, which is attached hereto and incorporated herein, contains the specific responsibilities for Entity and CIS regarding the CSS. Entity understands

App.415a

and agrees that, as a condition to commencement of CSS under the terms of this Agreement, it must:

- A. agree to comply with the terms and conditions applicable to Entity as set forth in Appendix A; and
- B. execute the Entity Certification form attached as part of Appendix A.

V. Title

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

VI. Term of this Agreement

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

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

The ability and obligation of CIS to provide these Cybersecurity Services and devices to the Entity is, at
--

all times, contingent on the availability and allocation of federal funds for this purpose.

VII. Amendments to this Agreement

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

VIII. No Third Party Rights

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

IX. Disclaimer

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

X. Confidentiality Obligation

CIS acknowledges that information regarding the infrastructure and security of Entity information systems, assessments and plans that relate specifically and uniquely to the vulnerability of Entity information systems, the results of tests of the security of Entity information systems insofar as those results may reveal specific vulnerabilities or otherwise marked as confidential by Entity ("Confidential Information") may be provided by Entity to CIS in connection with the services provided under this Agreement. The Entity acknowledges that it may receive from CIS trade secrets and confidential and proprietary information

App.417a

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

XI. Notices

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

1. via certified or registered United States mail, return receipt requested;
2. by facsimile transmission;

App.418a

3. by personal delivery;
4. by expedited delivery service; or
5. by e-mail with acknowledgement of receipt of the notice.

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

CIS

Name: Mark Perry

Title: Program Executive

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

Telephone Number: (518) 266-3476

Facsimile Number: (518) 283-3087

E-Mail Address: Mark.Perry@cisecurity.org

Entity

Name: Kevin Carr

Title: Chief Information officer

Address: 701 Kimberly Drive, Suite 285,
Denton, TX 76208

Telephone Number: (940) 349-4500

Facsimile Number:

E-Mail Address: kevin.carr@dentoncounty.com

App.419a

- B. Any such notice shall be deemed to have been given either at the time of personal delivery or, in the case of expedited delivery service or certified or registered United States mail, as of the date of first attempted delivery at the address and in the manner provided herein, or in the case of facsimile transmission or email, upon receipt.
- C. The Parties may, from time to time, specify any new or different contact information as their address for purpose of receiving notice under this Agreement by giving fifteen (15) days written notice to the other Party sent in accordance herewith. The Parties agree to mutually designate individuals as their respective representatives for the purposes of receiving notices under this Agreement. Additional individuals may be designated in writing by the Parties for purposes of implementation and administration, resolving issues and problems and/or for dispute resolution.

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

App.420a

**Center for Internet Security,
Inc.**

By: /s/ Benjamin Sper
Name: Benjamin Sper
Title: Director, EI-ISAC
Date: 8/12/19

Denton County, TX

By: /s/ Andy Eads
Name: Andy Eads
Title: County Judge
Date: August 6, 2019

Appendix A

CSS Responsibilities

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

- A. For purposes of this Agreement, Entity acknowledges and agrees that only those security devices supported by CIS fall within the scope of this Agreement. Entity will ensure the correct functioning of devices except where Entity elects to have CIS manage the devices.
- B. Entity shall provide logistic support in the form of rack space, electricity, Internet connectivity, and any other infrastructure necessary to support communications at Entity’s expense.
- C. Entity shall provide the following to CIS prior to the commencement of service and at any time during the term of the Agreement if the information changes:
 1. Current network diagrams to facilitate analysis of security events on the portion(s) of Entity’s network being monitored. Network diagrams will need to be revised whenever there is a substantial network change;

App.422a

2. In-band access via a secure Internet channel to manage the device(s).
3. Outbound access via a secure Internet channel for log transmission.
4. Reasonable assistance to CIS as necessary, to enable CIS to deliver and perform the CSS for the benefit of Entity;
5. Maintenance of all required hardware, virtual machines, or software necessary for the sensor located at Entity's site, and enabling access to such hardware, virtual machines, or software as necessary for CIS to provide the CSS;
6. Public and Private IP address ranges including a list of servers being monitored including the type, operating system and configuration information; and list of IP ranges and addresses that are not in use by the Entity (DarkNet space);
7. Completed Pre-Installation Questionnaires (PIQ). The PIQ will need to be revised whenever there is a change that would affect CIS's ability to provide the Cybersecurity Services;
8. Accurate and up-to-date information, including the name, email, landline, mobile, and pager numbers for all designated, authorized Point of Contact(s) who will be provided access to the portals, and;
9. The name, email address, and landline, mobile, and pager numbers for all

App.423a

shipping, installation and security points of contact.

- D. With respect to the shipping and delivery of any required hardware, Entity agrees to the following:
 - 1. For any hardware shipped directly to Entity, upon receipt of the hardware, Entity shall contact CIS to confirm the serial number of the hardware. Upon confirmation of the serial number, CIS will ship an identification tag to Entity. Entity agrees to place the identification tag on the hardware as per the accompanying instructions, and upon placement of the identification tag, to confirm in writing to CIS that the tag has been placed on the hardware.
 - 2. In certain instances, CIS may ship hardware and software to Entity prior to the final execution of this Agreement. Notwithstanding the foregoing, Entity acknowledges that commencement of CSS is contingent on the execution of this Agreement by the parties.
- E. During the term of this Agreement Entity shall provide the following:
 - 1. Written notification to CIS SOC (SOC@MSISAC.ORG) at least thirty (30) days in advance of changes in hardware or network configuration affecting CIS's ability to provide Cybersecurity Services, or a change to the physical location of the hardware; any notice relating to

App.424a

change in physical location shall include the new physical address of the hardware;

2. Written notification to CIS SOC (SOC@MSISAC.ORG) at least twelve (12) hours in advance of any scheduled downtime or other network and system administration scheduled tasks that would affect CIS's ability to provide the service;
3. A completed Escalation Procedure Form including the name, e-mail address and 24/7 contact information for all designated Points of Contact (POC). A revised Form must be submitted when there is a change in status for any POC;
4. Sole responsibility for maintaining current maintenance and technical support contracts with Entity's software and hardware vendors for any device affected by CSS that has not been supplied by CIS;
5. Active involvement with CIS SOC to resolve any tickets requiring Entity input or action;
6. Reasonable assistance in remotely installing and troubleshooting devices including hardware and communications,
7. Upon reasonable notice from CIS and during normal business hours, access for CIS to inspect the hardware.
8. Response to biennial written confirmation notice from MS-ISAC as to the

App.425a

physical location of all hardware provided by CIS.

- F. Certification. Entity shall complete the attached Entity Certification documenting compliance with the following:
1. That the Entity provides notice to its employees, contractors and other authorized internal network users (collectively, "Computer Users") that contain in sum and substance the following provisions:
 - (a) Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity's information system; and
 - (b) Any communications or data transiting, stored on or traveling to or from the Entity's information system may be monitored, disclosed or used for any lawful government purpose; and
 2. That all Entity Computer Users execute some form of documentation or electronic acceptance acknowledging his/her understanding and consent to the above notice. Examples of notice documentation include, but are not limited to:
 - a) log-on banners for computer access with an "I Agree" click through;
 - b) consent form signed by the Computer User acknowledging Entity's computer use policy; or

- c) computer use agreement executed by the Computer User.

II. CIS Responsibilities

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

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

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

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

App.427a

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

E. CIS Security Operation Center. CIS will provide 24/7 telephone (1866-787-4722) availability for assistance with events detected by the CSS.

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

ENTITY CERTIFICATION

On behalf of Denton County, Texas (“Entity”) I hereby certify the following:

1. Entity provides notice to its employees, contractors and other authorized internal network users (“collectively “Computer Users”) that contain in sum and substance the following provisions:
 - Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity’s information system; and
 - Any communications or data transiting, stored on or traveling to or from the Entity’s information system may be monitored, disclosed or used for any lawful government purpose.

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

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

Dated this 6th day of August, 2019.

/s/ Andy Eads
Name: Andy Eads
Title: County Judge

**MEMORANDUM OF AGREEMENT BETWEEN
THE CENTER FOR INTERNET
SECURITY/ELECTION INFRASTRUCTURE
INFORMATION SHARING AND ANALYSIS
CENTER AND
Dallas County Texas
FOR
CYBERSECURITY SERVICES
(Federally Funded Election Services)**

This MEMORANDUM OF AGREEMENT ("Agreement") by and between the Center for Internet Security, Inc. ("CIS"), operating in its capacity as the Elections Infrastructure Information Sharing and Analysis Center ("EI-ISAC"), located at 31 Tech Valley Drive, East Greenbush, NY 12061-4134, and Dallas County, Texas ("Entity") with its principal place of business at: 411 Elm Street, Dallas, TX 75202 for Cybersecurity Services, as defined herein below (CIS and Entity each a "Party" and collectively referred to as the "Parties;").

WITNESSETH:

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

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

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

App.430a

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

I. Purpose

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

II. Definitions

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

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

III. Consideration

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

IV. Responsibilities

Appendix A, which is attached hereto and incorporated herein, contains the specific responsibilities for Entity and CIS regarding the CSS. Entity understands

App.431a

and agrees that, as a condition to commencement of CSS under the terms of this Agreement, it must:

- A. agree to comply with the terms and conditions applicable to Entity as set forth in Appendix A; and
- B. execute the Entity Certification form attached as part of Appendix A.

V. Title

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

VI. Term of this Agreement

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

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

<p>The ability and obligation of CIS to provide these Cybersecurity Services and devices to the Entity is, at</p>

all times, contingent on the availability and allocation of federal funds for this purpose.

VII. Amendments to this Agreement

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

VIII. No Third Party Rights

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

IX. Disclaimer

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

X. Confidentiality Obligation

CIS acknowledges that information regarding the infrastructure and security of Entity information systems, assessments and plans that relate specifically and uniquely to the vulnerability of Entity information systems, the results of tests of the security of Entity information systems insofar as those results may reveal specific vulnerabilities or otherwise marked as confidential by Entity ("Confidential Information") may be provided by Entity to CIS in connection with the services provided under this Agreement. The Entity acknowledges that it may receive from CIS trade secrets and confidential and proprietary infor-

mation (“Confidential Information”). Both Parties agree to hold each other’s Confidential Information in confidence to the same extent and the same manner as each Party protects its own confidential information; but in no event will less than reasonable care be provided and a Party’s information will not be released in any identifiable form without the express written permission of such Party or as required pursuant to lawfully authorized subpoena or similar compulsive directive or is required to be disclosed by law, provided that the Entity shall be required to make reasonable efforts, consistent with applicable law to limit the scope and nature of such required disclosure. CIS shall, however, be permitted to disclose relevant aspects of such Confidential. Information to its officers, employees, agents and CIS’s cybersecurity partners, including federal partners, provided that such partners have agreed to protect the Confidential Information to the same extent as required under this Agreement. The Parties agree to use all reasonable steps to ensure that Confidential Information received under Agreement is not disclosed in violation of this Section. These confidentiality obligations shall survive any future non-availability of federal funds to continue the program that supports this Agreement or the termination of this Agreement.

XI. Notices

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

1. via certified or registered United States mail, return receipt requested;
2. by facsimile transmission;

App.434a

3. by personal delivery;
4. by expedited delivery service; or
5. by e-mail with acknowledgement of receipt of the notice.

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

CIS

Name: Mark Perry

Title: Program Executive

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

Telephone Number: (518) 266-3476

Facsimile Number: (518) 283-3087

E-Mail Address: Mark.Perry@cisecurity.org

Entity

Name: Clay Jenkins

Title: County Judge

Address: 411 Elm Street, Dallas, TX 75202

Telephone Number: 214-653-6649

Facsimile Number: 214-653-6327

E-Mail Address: stanley.victrum@dallascounty.org

- B. Any such notice shall be deemed to have been given either at the time of personal delivery or, in the case of expedited delivery service or certified or registered United States mail, as of the date of first attempted delivery at the address and in the manner provided herein, or in the case of facsimile transmission or email, upon receipt.
- C. The Parties may, from time to time, specify any new or different contact information as their address for purpose of receiving notice under this Agreement by giving fifteen (15) days written notice to the other Party sent in accordance herewith. The Parties agree to mutually designate individuals as their respective representatives for the purposes of receiving notices under this Agreement. Additional individuals may be designated in writing by the Parties for purposes of implementation and administration, resolving issues and problems and/or for dispute resolution.

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

Dallas County, TX

By: /s/ Clay Jenkins
Name: Clay Jenkins
Title: County Judge
Date: Oct 19, 2018

App.436a

Approved as to Form:*

Faith Johnson
District Attorney

/s/ Ben Stool
Assistant District Attorney

***BY LAW, THE DISTRICT ATTORNEY'S OFFICE MAY ONLY ADVISE OR APPROVE CONTRACTS OR LEGAL DOCUMENTS ON BEHALF OF ITS CLIENTS. IT MAY NOT ADVISE OR APPROVE A LEASE, CONTRACT, OR LEGAL DOCUMENT ON BEHALF OF OTHER PARTIES. OUR REVIEW OF THIS DOCUMENT WAS CONDUCTED SOLELY FROM THE LEGAL PERSPECTIVE OF OUR CLIENT. OUR APPROVAL OF THIS DOCUMENT WAS OFFERED SOLELY FOR THE BENEFIT OF OUR CLIENT. OTHER PARTIES SHOULD NOT RELY ON THIS APPROVAL, AND SHOULD SEEK REVIEW AND APPROVAL BY THEIR OWN RESPECTIVE ATTORNEY(S).**

other Party sent in accordance herewith. The Parties agree to mutually designate individuals as their respective representatives for the purposes of receiving notices under this Agreement. Additional individuals may be designated in writing by the Parties for purposes of implementation and administration, resolving issues and problems and/or for dispute resolution.

App.437a

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

Dallas County, TX

By: /s/ Clay Jenkins

Name: Clay Jenkins

Title: County Judge

Date: 10/19/2018

Appendix A

CSS Responsibilities

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

- A. For purposes of this Agreement, Entity acknowledges and agrees that only those security devices supported by CIS fall within the scope of this Agreement. Entity will ensure the correct functioning of devices except where Entity elects to have CIS manage the devices.
- B. Entity shall provide logistic support in the form of rack space, electricity, Internet connectivity, and any other infrastructure necessary to support communications at Entity's expense.
- C. Entity shall provide the following to CIS prior to the commencement of service and at any time during the term of the Agreement if the information changes:
 - 1. Current network diagrams to facilitate analysis of security events on the portion(s) of Entity's network being monitored. Network diagrams will need

App.439a

to be revised whenever there is a substantial network change;

2. In-band access via a secure Internet channel to manage the device(s).
3. Outbound access via a secure Internet channel for log transmission.
4. Reasonable assistance to CIS as necessary, to enable CIS to deliver and perform the CSS for the benefit of Entity;
5. Maintenance of all required hardware, virtual machines, or software necessary for the sensor located at Entity's site, and enabling access to such hardware, virtual machines, or software as necessary for CIS to provide the CSS;
6. Public and Private IP address ranges including a list of servers being monitored including the type, operating system and configuration information; and list of IP ranges and addresses that are not in use by the Entity (DarkNet space);
7. Completed Pre-Installation Questionnaires (PIQ). The PIQ will need to be revised whenever there is a change that would affect CIS's ability to provide the Cybersecurity Services;
8. Accurate and up-to-date information, including the name, email, landline, mobile, and pager numbers for all designated, authorized Point of Contact(s) who will be provided access to the portals, and;

App.440a

9. The name, email address, and landline, mobile, and pager numbers for all shipping, installation and security points of contact.
- D. With respect to the shipping and delivery of any required hardware, Entity agrees to the following:
1. For any hardware shipped directly to Entity, upon receipt of the hardware, Entity shall contact CIS to confirm the serial number of the hardware. Upon confirmation of the serial number, CIS will ship an identification tag to Entity. Entity agrees to place the identification tag on the hardware as per the accompanying instructions, and upon placement of the identification tag, to confirm in writing to CIS that the tag has been placed on the hardware.
 2. In certain instances, CIS may ship hardware and software to Entity prior to the final execution of this Agreement. Notwithstanding the foregoing, Entity acknowledges that commencement of CSS is contingent on the execution of this Agreement by the parties.
- E. During the term of this Agreement Entity shall provide the following:
1. Written notification to CIS SOC (SOC@MSISAC.ORG) at least thirty (30) days in advance of changes in hardware or network configuration affecting CIS's ability to provide Cybersecurity Services,

App.441a

or a change to the physical location of the hardware; any notice relating to change in physical location shall include the new physical address of the hardware;

2. Written notification to CIS SOC (SOC@MSISAC.ORG) at least twelve (12) hours in advance of any scheduled downtime or other network and system administration scheduled tasks that would affect CIS's ability to provide the service;
3. A completed Escalation Procedure Form including the name, e-mail address and 24/7 contact information for all designated Points of Contact (POC). A revised Form must be submitted when there is a change in status for any POC;
4. Sole responsibility for maintaining current maintenance and technical support contracts with Entity's software and hardware vendors for any device affected by CSS that has not been supplied by CIS;
5. Active involvement with CIS SOC to resolve any tickets requiring Entity input or action;
6. Reasonable assistance in remotely installing and troubleshooting devices including hardware and communications,

App.442a

7. Upon reasonable notice from CIS and during normal business hours, access for CIS to inspect the hardware.
 8. Response to biennial written confirmation notice from MS-ISAC as to the physical location of all hardware provided by CIS.
- F. Certification. Entity shall complete the attached Entity Certification documenting compliance with the following:
1. That the Entity provides notice to its employees, contractors and other authorized internal network users (collectively, "Computer Users") that contain in sum and substance the following provisions:
 - (a) Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity's information system; and
 - (b) Any communications or data transiting, stored on or traveling to or from the Entity's information system may be monitored, disclosed or used for any lawful government purpose; and
 2. That all Entity Computer Users execute some form of documentation or electronic acceptance acknowledging his/her understanding and consent to the above

App.443a

notice. Examples of notice documentation include, but are not limited to:

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

II. CIS Responsibilities

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

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

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

1. Analysis of logs from monitored security devices for attacks and malicious traffic;
2. Analysis of security events;
3. Correlation of security data/logs/events with information from other sources;
4. Notification of security events per the Escalation Procedures provided by Entity.

App.444a

5. Ensuring that all upgrades, patches, configuration changes and signature upgrades are applied to managed devices. CIS will provide the appropriate license and support agreements for the upgrade for devices provided by CIS. The Entity is responsible for maintaining the appropriate license and support agreements for devices own by the Entity.

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

E. CIS Security Operation Center. CIS will provide 24/7 telephone (1866-787-4722) availability for assistance with events detected by the CSS.

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

ENTITY CERTIFICATION

On behalf of Dallas County, Texas ("Entity") I hereby certify the following:

1. Entity provides notice to its employees, contractors and other authorized internal network users ("collectively "Computer Users") that contain in sum and substance the following provisions:
 - Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity's information system; and
 - Any communications or data transiting, stored on or traveling to or from the Entity's information system may be monitored, disclosed or used for any lawful government purpose.

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

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

Dated this ___ day of _____, 2018.

Name: Stanley "Vic" Victrum
Title: Chief Information Officer

ENTITY CERTIFICATION

On behalf of Dallas County, Texas (“Entity”) I hereby certify the following:

1. Entity provides notice to its employees, contractors and other authorized internal network users (“collectively “Computer Users”) that contain in sum and substance the following provisions:
 - Computer Users have no reasonable expectation of privacy regarding communications or data transiting, stored on or traveling to or from Entity’s information system; and
 - Any communications or data transiting, stored on or traveling to or from the Entity’s information system may be monitored, disclosed or used for any lawful government purpose.

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

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

Dated this 19 day of October, 2018.

/s/ Clay Jenkins
Name: Clay Jenkins
Title: County Judge

COMBINED AFFIDAVITS

IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF TEXAS

STRONGIN, ET AL.

v.

SCOTT, ET AL.

Case No. 4:2022cv00576

AFFIDAVIT

AFFIDAVIT OF AMBER CLOY

Pursuant to 28 U.S.C. 1746, I, Amber Cloy, make the following declaration/affidavit:

1. During the course and leading up to the 2020 General Election, my 1st Amendment right to free speech was censored, suppressed, and restricted by on-line social media platforms. From personal experience and observations, my political view points are not allowed to enter into the public space on social media platforms. See attached examples

2. I have personally been “flagged,” had posts removed, and “fact checked” as a result of posting articles, photos, videos or messages with regard to above mentioned areas by social media companies. Additionally, I was banned from exercising any and all free speech from approximately 1/16/2021 until 1/26/2020 (see attached).

3. Content creators that I follow were de-platformed, and de-monetized. I was restricted from viewing and sharing their content and contributing funds to support their efforts to create new content. (Example: Toresays, Gateway Pundit, Project Veritas are but a few)

4. One post that was censored and marked as “False Information” was regarding January 6th of 2020 by the Texas Attorney General Ken Paxton.

5. I personally have sourced, read, and can affirm that the Defendants of this case have colluded with the federal government to monitor, censor, and violate my First Amendment rights to freedom of speech by contracting with the Department of Homeland security through the Center for Internet Security. In turn this agency partnered up with other federal agencies (FBI, ONDI, DOJ, IA, CISA) and shared my personal identifiable information through the Texas voter rolls in violation of 52 U.S.C § 552a(b).

6. I have suffered government-induced online censorship barring me from free, fair and open political process of petitioning my government directly by the Defendants continued relationships with the federal government.

7. The Defendants have colluded with the federal government through these relationships via meetings with NGOs (Election Integrity Partners) that are the polar opposite of my political views and execute political viewpoint censorship.

8. The Defendants currently are members of organizations that meet with the above federal agencies and NGOs to plan, organize, coerce, and execute governmental restriction of my freedom of speech that

App.449a

does not align with governmental or NGO viewpoint-based political norm.

9. These organizations that all Defendants are members of are the following:

- a. National Association of Secretaries of State (MASS)
 - i. Defendant Hughs – EIP formation 2020
 - ii. Defendant Scott – Continuation of EIP association 2021-2022
 - iii. Defendant Nelson – Admittance into EIP association 2023
- b. National Association of Election Directors (NASED)
 - i. Defendant Ingram – EIP formation, Tabletop meetings with social media platforms, planning, organizing, coercion, and execution of censorship.
- c. EIS-GCC
 - i. Defendant Ingram – EIS-GCC ExComm Principle role and member. Knowingly – Tabletop meetings with social media platforms, planning, organizing, coercion, and execution of censorship.
- d. EI-ISAC
 - i. All Defendants through the Center for Internet Security
 1. Access to EIP to report “ticketing” on restriction of free speech to social media platforms.

2. Access to CrowdTangle to report “ticketing” on restriction of free speech to social media platforms.
 3. Access to CISA general inbox and employee email addresses report “switchboarding” on restriction of free speech to social media platforms.
- ii. Defendant Ingram, Hughs, Scott, Nelson – EIP formation, Tabletop meetings with social media platforms, planning, organizing, coercion, and execution of censorship.
1. All of the above with limitless access.

10. It is my belief through public sourcing of Defendants’ emails and calendar appointments that All Defendants have colluded with the federal government, privately-owned third-party companies, non-government organizations (NGO), and elections officials to suppress, coerce, organize with, and execute my First Amendment right to free speech.

I declare under penalty of perjury that the forgoing complaint with injunction has been reviewed and I personally know or believe that all allegations are true and correct to the best of my knowledge. Executed this 30th day of April, 2023.

Signature

/s/ Amber Cloy

421 Palisades Trail
Keller, Texas 76248

{ Dense images with illegible text omitted }

App.451a

IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF TEXAS

STRONGIN, ET AL.

v.

SCOTT, ET AL.

Case No.

AFFIDAVIT

AFFIDAVIT OF LINDSEY GREMONT

Pursuant to 28 U.S.C. 1746, I, Lindsey Gremont, make the following declaration/affidavit: Affiant supports in writing a cause that demonstrates Plaintiffs actions and injury and continued injury as outlined above in this verified complaint/petition with injunction violate several state and federal laws, which are against The People of Texas, and also, against the peace and dignity of the State.

1. I am a registered voter in Travis County and the State of Texas and have resided in Texas for a majority of my life.

2. During the course and leading up to the 2020 General Election, my 1st Amendment right to free speech was censored, suppressed, restricted and shadow banned by on-line social media platforms. Below are but a few examples of my view points that are not allowed to enter into the public space on social media platforms. See attached examples.

a. Mainstream media / propaganda

App.452a

- b. Covid 19 related
- c. Health related
- d. Political views
- e. Hunter Biden laptop

3. I continue to get red flags on posts from as old as 2-3 years ago related to the topics mentioned above on Facebook or Instagram due "fact checking" and "flagging as mis-information". I have even been put into a "timeout" on Instagram where others could not tag my instagram handle in their stories or on their posts. I have been told my posts would be limited in reach and saw my story views drop each time I was put into one of these "timeouts".

4. I have over 10,000 followers on Instagram and there have been many times since 2020 that many of my followers reported to me that they could not see my posts or had been automatically dropped from following me by Instagram and not them. They had to re-follow me.

5. I had to change the way I worded things in my Facebook and Instagram posts to avoid the "timeouts" and "flagging". Saying things like "poke" or "jab" vs. "vaccination".

6. I saw many of the friends/influencers I follow and know personally be completely banned from Instagram or put into similar "timeouts" and also be shadow banned (reach limited).

7. Facebook groups and pages were how I grew my business and communicated with my various members and followers across Facebook with over 20,000+ group members in multiple Facebook groups

and 75,000+ likes on multiple Facebook pages. Due to my now limited reach I am unable to communicate with them via Facebook any longer because the majority of them no longer see my posts due to shadow banning. I use text and email instead. My business has suffered tremendously from this drop in reach due to flagging, timeouts and shadow banning. I was put into Facebook "jail" until I deleted certain posts deemed to be "harmful to the community" due to "misinformation". I tried to appeal and was only told I must delete these posts.

8. YouTube deleted a video of mine because I mentioned vaccination in it. They notified me and said they deleted it and why. I have over 5,000 subscribers on YouTube and you can see by the numbers of views that many of my videos over the last number of years have been suppressed or shadow banned. I believe if given discovery I would find my name on a "black list" of some kind due to my discussions about GMOs and natural health.

9. Facebook deleted a video of mine without notifying me and never explained why when asked. The video was about probiotics.

10. Links I shared related to the Hunter Biden laptop on Twitter were flagged, comments were limited and then the post was deleted altogether. Posts about vaccination and Covid 19 were flagged and comments and retweets were limited. My overall reach was highly limited on twitter due to shadow banning. I suspect and could find out via discovery if I was on a "blacklist" for shadow banning many years ago due to posts about GMOs.