Kristin Vent
2017 Sonnett Street
El Cajon, CA 92019
(619) 729-6202
kristinvent17@cox.com

IN THE UNITED STATES DISTRICT COURT

FOR THE SAN DIEGO DISTRICT OF CALIFORNIA

KRISTIN VENT, Plaintiff, pro se vs. NATHAN FLETCHER, NORA VARGAS, TERRA LAWSON REMER, JIM DESMOND, JOEL ANDERSON, CYNTHIA PAES, MICHAEL VU Defendant	Case No.: Number '22CV1651 RBM DDL PETITION FOR INJUNCTIVE RELIEF (ELECTION MATTER) ~~(TRO REQUESTED)~~ KV

COMPLAINT AND REQUEST FOR EMERGENCY INJUNCTION COME NOW Plaintiff, Kristin Vent, pro se, hereby files this petition against Defendant(s) NATHAN FLETCHER, in his official capacity as Chairman of the Board of Supervisors of the County of San Diego, NORA VARGAS, in her official capacity as Vice Chair of the Board of Supervisors of the County of San Diego, TERRA LAWSON REMER, in her official capacity as Supervisor of the County of San Diego District 3, JIM DESMOND in his official capacity as Supervisor of the County of San Diego District 5, JOEL ANDERSON in his official capacity as Supervisor of the County of San Diego District 2, CYNTHIA PAES in her official capacity as the Registrar of Voters of the County of San Diego, MICHAEL VU, in his prior official capacity as the Registrar of Voters of the County of San Diego. Plaintiff brings this petition to preserve the integrity of the elections for the County of San Diego and the voting systems and machines purchased and used during the November 3,

2020 election, the June 7, 2022 election, and the upcoming Nov 8, 2022 election. In support of the claims set forth herein, Plaintiff alleges and avers as follows:

I. JURISDICTION AND VENUE

1. This verified petition is for a complaint for injunctive relief. Plaintiff incorporates the foregoing paragraphs as if set forth in full herein.

2. This Court has personal jurisdiction because Defendant(s) performs their official duties in the State of California and the County of San Diego, affecting every district therein.

3. This Court has subject matter jurisdiction under Article VI, § 10 of the California Constitution, Article II, § 1 of the California Constitution, California Code of Regulations 20700 (examination of voting equipment), California Election Code § 19212 (definition for certification of voting equipment), and California Election Code § 19101 (voting system standards and regulations governing use of voting machines).

4. Venue is proper pursuant to CCP, § 491.320., Article 2, Creditors Suit [491.310. - 491.370] Defendants perform their official duties within the State of California and the County of San Diego, affecting every district therein.

5. Jurisdiction is proper in this Court pursuant to CCP, Article 6 § 1. The duty to certifying the County of San Diego's election results is a ministerial duty to which the statute specifically describes the manner of performance. The Defendants must certify a lawful election and they may not certify an illegal/unlawful election.

This court has subject matter jurisdiction over Plaintiff's claims under:

- ***Article IV, § 10 of the California Constitution***

- ***Article II, § 1 of the California Constitution***
- ***California Code of Regulations 20700 (examination of voting equipment)***
- ***California Election Code § 19212 (definition for certification of voting equipment)***
- ***California Election Code § 19101 (voting system standards and regulations governing use of voting machines).***

6. Plaintiff incorporates the foregoing paragraphs as if set forth in full herein.

7. This court has subject matter jurisdiction under 28U.S.C. 1331 and 28 U.S.C. 1342.

8. Jurisdiction to grant injunctive relief is conferred by 28U.S.C. 1331 and 28 U.S.C. 1342.

9. Venue is proper under 28 U.S.C. 1391 because "a substantial part of the events or omissions giving rise to the claim occurred" within the County of San Diego, where plaintiff resides and defendants conduct official business.

II. PARTIES

Plaintiff Kristin Vent is a resident and registered voter of San Diego County, California.

Defendant is the governing entity of San Diego in the State of California. At the time of this filing, Defendants actions are decided by five Board Members, each acting in their official capacities: Chairman Nathan Fletcher, Supervisor Nora Vargas, Supervisor Terra Lawson Remer, Supervisor Jim Desmond, Supervisor Joel Anderson.

III. STATEMENT OF FACTS

INTRO

1. The methods by which local, state, and Federal elections conducted in the County of San Diego in the State of California, most recently in 2020 and 2022, cannot be proven to provide the fair elections guaranteed to every citizen under the 14th Amendment of the U.S. Constitution, Elections Clause (Art. I, § 4, cl. 1).

2. The right to vote is protected by the Equal Protection Clause and the Due Process Clause. U.S. CONST. amend XIV, § 1, cl 3-4 Because "the right to vote is personal," Reynolds, 377 U.S. at 561-62. "[e]very voter in a federal…election, whether he votes for a candidate with little chance of winning or for one with little chance of losing, has a right under the Constitution to have his vote fairly counted." Anderson v. United States, 417 U.S. 211, 227 (1974); Baker v. Carr. 369 U.S. 186, 208 (1962). Invalid or fraudulent votes debase or dilute the weight of each validity cast vote. Bush II, 531 U.S. at 105. The unequal treatment of votes within a state, and unequal standards for processing votes raise equal protection concerns.

3. A voter who cast a vote in an election in accordance with the laws of this state shall have that vote counted. CA State Constitution, Article II, § 2.5.

4. The Supreme Court of the United States has recognized that the right to vote consists of not only casting a ballot, but having that vote counted accurately, as it was cast.

5. "We regard it as equally unquestionable that the right to have one's vote counted is as open to protection by Congress as the right to put a ballot in a box. "See United States v. 3 Mosley, 238 U.S. 386 (1915)

6. "No right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens we must live. Other rights, even the most basic, are illusory if the right to vote is undermined. "See Wesberry v. Sanders, 376 U.S. 17 (1964)

7. "We regard it as equally unquestionable that the right to have one's vote counted is as open to protection by Congress as the right to put a ballot in a box. "See United States v. 3 Mosley, 238 U.S. 386 (1915).

8. "No right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens we must live. Other rights, even the most basic, are illusory if the right to vote is undermined. "See Wesberry v. Sanders, 376 U.S. 17 (1964).

9. Voting through the machines does not guarantee that one's vote is counted accurately due to the potential use of the "Trapdoor" mechanism. Therefore, there is no way of knowing if the plaintiff's freedom of speech was abridged according to the 1st Amendment in the Federal Constitution, since voting is an extension of free-speech.

10. "No one would deny that the equal protection clause would…prohibit a law that would expressly give certain citizens a half-vote and others a full vote…[T]he constitutionally guaranteed right to vote and the right to have one's vote counted clearly imply the policy that state election systems, no matter what their form, should be designed to give approximately equal weight to each vote cast…[A] state legislature cannot deny eligible voters the right to vote

for Congressmen and the right to have their vote counted." See Reynolds v. Sims, 377 U.S. 563 (1964), citing Colegrove v. Green, 328 U.S. 549, 328 U.S. 569-571. By utilizing voting machines tested by Voting Systems Test Laboratories with improper Election Assistance Commission accreditation at the time of certification and with the potential for the Trapdoor mechanism described in Exhibit A, (Tore's Affidavit). California has deprived its voters of the capability of knowing that their vote was accurately counted.

11. Plaintiffs are entitled to temporary, preliminary, and permanent injunctive relief by restraining Defendant from both destroying the November 2020 election date as scheduled 22 months after the election, CA Elections Code, Section 17502[1], and from using electronic voting machines until a thorough investigation of the software and its Trapdoor vulnerabilities can be undertaken. Which was requested by a demand letter sent on August 29, 2022.

12. Electronic Voting Machines ('EVMS') are any hardware or software, in part or whole, employed for the use of electronic voting, tabulating and/or systems used to communicate with election results reporting.

13. A cryptographic security risk inherent in all voting machines, more specifically a Trapdoor mechanism described in Exhibit A, makes the output of votes shown in reported election results impossible to reconcile with the ballot inputs, by design, except under a full visual inspection and re-count of all legal paper ballots cast.

[1] https://casetext.com/statute/california-codes/california-elections-code/division-17-retention-and-preservation-of-election-records/chapter-6-miscellaneous-provisions/section-17502-preservation-of-records-reflecting-appointment-of-precinct-officials-in-elections-where-candidates-for-president-vice-president-senator-or-representative-voted-upon

14. The critical security deficiencies plaguing all EVMS, and therefore our elections, are being ignored by elected and appointed officials and the federal and state agencies responsible for securing the integrity of our local, state and federal elections.

15. They have not taken seriously the voluminous studies, reports, testimony and other compilations of evidence, which should have warranted immediate, legitimate and adequate mitigating actions to prove remedy of these vulnerabilities or a ceasing of the further use of the machines. In fact, as the data for electronic election insecurity mounts, state and federal bodies and officials governing the federally regulated practice of vote system accreditation and certification of elections have failed to function within Congressionally passed parameters of law.

16. What is presented here is by no means exhaustive, but rather focuses in on the most pertinent details of electronic vote manipulation – ZERO KNOWLEDGE PROOF VOTE TABULATION ALGORITHMS, EVMS internet connectivity, undetectable vote fraud, and patterns intrinsic to electronic vote manipulation.

17. All persons cited in the following Statement of Facts are computer science/cybersecurity experts, ex-military and/or ex-military subcontractors. All cite experience based upon real-world creation, testing and/or deployment of malicious malware into EVMS, occurring in testing environs and/or in actual, live, real-world elections.

18. Established practice in cybersecurity REQUIRED federal and state officials to promptly subject all EVMS to rigorous testing and hardening based upon white hat hacking testimony from hundreds of cyber professionals for nearly two decades.

19. Also enumerated are the most egregious failures of the Election Assistance Commission and state level officials' duty of due diligence to ensure their systems were lawfully accredited and certified.

20. All EVMS make use of zero proof algorithms, rendering the ability to prove that a vote was legally counted as the voter intended was and is, by design, nearly impossible.

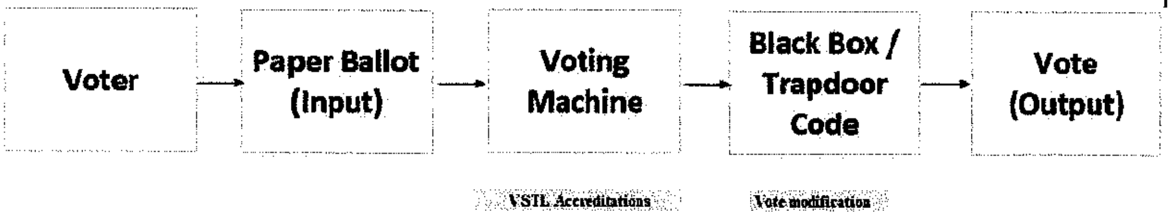
21. The high probability of votes being altered, manipulated or changes once or after the machines read the ballots leaves a critical part of the foundation of the United States' democratic way of life, free and fair elections, vulnerable to the intentions of foreign and domestic bad actors to sway election results at local, state, and Federal levels.

22. Retention of all November 2020 election data beyond the September 3, 2022 required period is critical to ensuring the 2020 election results can be legitimately verified and validated, and ensure the fairness of all future elections in the state of California.

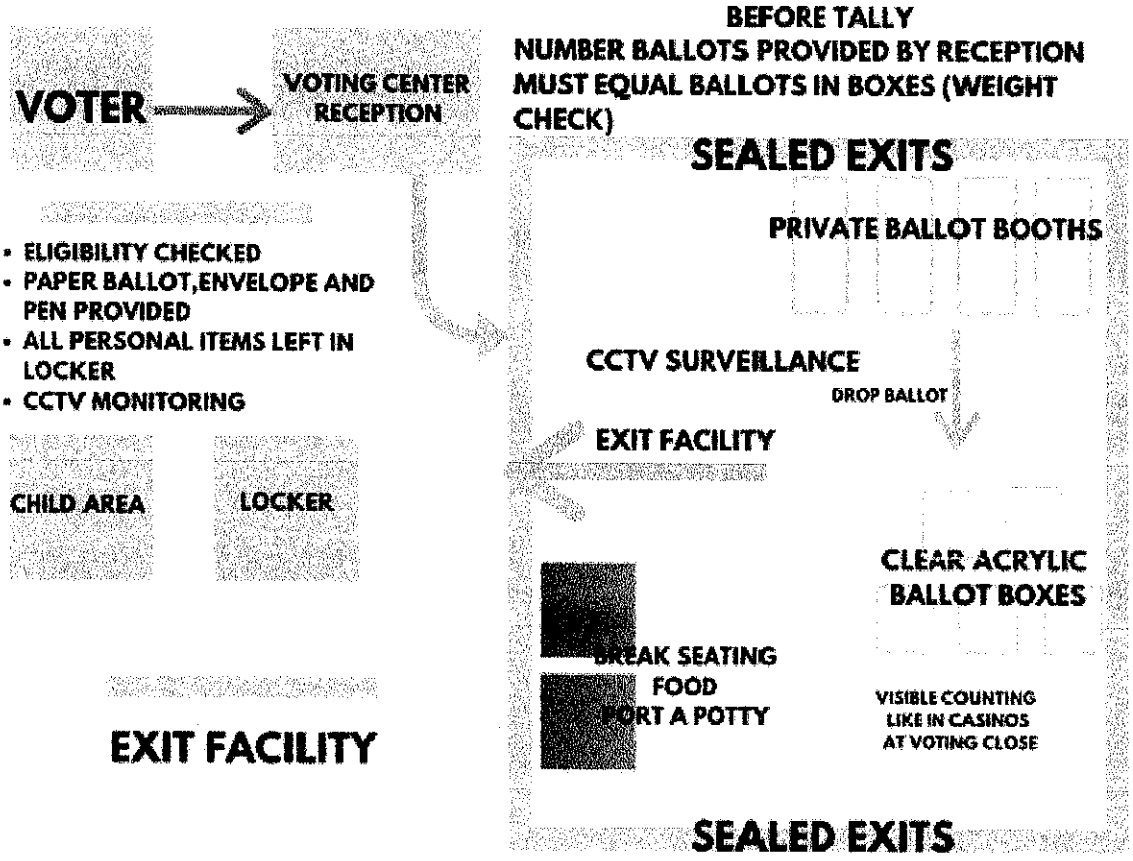
23. Until an in-person, paper ballot, day-of-election voting process is re-established, with results reported immediately after the voting period ends, Americans cannot, do not and will not have any degree of confidence that the reported results of any election is an accurate reflection of the legitimate votes cast.

24. Before and during the November 2020 election, neither of the two Voting System Testing Laboratories ("VSTLs") typically accredited by the Election Assistance Commission ("EAC") had current un-expired accreditations. Therefore, with no valid Federally approved VSTLs, there could be no such VSTL approval of California's voting systems for the November 2020 election.

25. Time is of the essence since the 22-month election data retention requirement expires relative to the November 2020 election in early September of 2022. Plaintiff requested the retention of all voting records for San Diego County via demand letter on August 29, 2022. The following simplified diagram illustrates the election process and claims raised herein; the critical piece is the "Black Box / Trapdoor Code", which is undetected by design and can be used, as Exhibit A conveys, to completely remove the link between the ballot inputs and "vote" outputs:



26. To return to fair elections where votes are counted as they were cast, with proof at every step, a day-of-election voting process can be set up with volunteers from each community, in secure 1 room with closed-circuit camera surveillance of voters and ballot counting (see schematic below, from: https://toresays.com/2019/11/22/proof-that-auditing-election-machines-cannot-detect-manipulation-of-votes/).


VOTER
VOTING CENTER RECEPTION
• ELIGIBILITY CHECKED
• PAPER BALLOT,ENVELOPE AND PEN PROVIDED
• ALL PERSONAL ITEMS LEFT IN LOCKER
• CCTV MONITORING
CHILD AREA
LOCKER
EXIT FACILITY
BEFORE TALLY
NUMBER BALLOTS PROVIDED BY RECEPTION MUST EQUAL BALLOTS IN BOXES (WEIGHT CHECK)
SEALED EXITS
PRIVATE BALLOT BOOTHS
CCTV SURVEILLANCE
DROP BALLOT
EXIT FACILITY
CLEAR ACRYLIC BALLOT BOXES
BREAK SEATING
FOOD
PORT A POTTY
VISIBLE COUNTING LIKE IN CASINOS AT VOTING CLOSE
SEALED EXITS

27. “When California Secretary of State Debra Bowen decertified the use of several brands of electronic voting machines this past week, she sent election officials in El Dorado, and Placer counties scrambling. In May 2007, Bowen authorized a top-to-bottom review of electronic voting machines used in elections in 43 of the state’s 58 counties. The University of California conducted the review and found the machines are vulnerable to manipulation. The systems tested were Diebold Elections Systems, Sequoia Voting Systems and Hart InterCivic. The machines were found to be vulnerable to viruses, malicious software, mischievous insiders and did not protect ballot secrecy, according to the decertification/recertification documents

released by Bowen." (*Reference:*https://www.tahoedailytribune.com/news/secretary-of-state-decertifies-some-electronic-voting-machines/)

28. California elections were conducted in 2020 and June of 2022 and are planned to be conducted in November of 2022 in a manner that cannot ensure that each legal vote is counted as cast.

29. The voting systems used in the November 2020, June 2022, and in the upcoming November 2022 elections in California are manufactured by the following companies: Democracy Live, Dominion Voting Systems (DIMS.net Product Suite, Version 10.7531.25123 specifically used in the County of San Diego, see Exhibit B), Election Systems and Software, Five Cedars Group, Hart InterCivic, KNOWiNK, Los Angeles County VSAP, Robis Elections, RunBeck Election Services Inc. (used in the County of San Diego, Exhibit B), and Tenex Software Solutions; *see "Voting Technology Vendors" on the California Secretary of State website:* (https://www.sos.ca.gov/elections/ovsta/voting-technology-vendors).

30. In February 2020 the County of San Diego began the use of Dominion Voting Machines in San Diego for 2020 and subsequent elections (*Reference "Voting Systems in Use by Counties" on the California Secretary of State Website:* https://votingsystems.cdn.sos.ca.gov/oversight/county-vsys/vot-tech-by-counties-2020-11.pdf).

31. All voting systems in use in the United States, now and in 2020, are subject to tampering through a Trapdoor mechanism inherent in all election systems. This Trapdoor mechanism is described in detail in Exhibit A, affidavit of Terpsehore Maras, filed under penalty of perjury on December 1, 2020 in case #2:20-cv-01771-PP in the 2nd Judicial

District of the Denver District Court in Denver, Colorado, where Ms.Maras identifies her First-hand knowledge of this fact.

32. Terpsehore Marias is a trained Cryptolinguist, holds a completed degree in Molecular and Cellular Physiology with formal training in other sciences such as Computational Linguistics, Game Theory, Algorithmic Aspects of Machine Learning, and Predictive Analytics. Terpesehore Maras, possesses more than two decades of experience in mathematical modeling and pattern analysis as well as lesser experience in network tracing and cryptography. Additionally, she has extensive involvement in overseeing OCONUS elections and the HAVA Act for CONUS elections. The information presented in the affidavit is personal, first-hand account clarifies in detail as to why EAC Accreditation is so important to censure fair elections. Key portions of the affidavit emphasizing proper EAC Accreditation and VSTL testing are as follows:

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

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

"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 changes 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 reword 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."

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

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

"36. The purpose of VSTL's being accredited and their importance of 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 ensure "anonymity." (Exhibit L)

33. The key aspect and summary of this sometimes-technical affidavit, in layman's terms, is paragraph 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."

34. The problem with verifying that any voting machine system gives a fair outcome, where the votes output is identical to the votes input, is that due to the Trapdoor mechanism it is impossible to prove that the election was fair, which is the responsibility of the Secretary of State.

35. It is also impossible to prove that the election was unfair, but the burden is on the State to prove that its systems are not only capable of conducting, but in fact conduct, fair elections. This is an impossibility, as Exhibit A demonstrates.

36. Expired VSTL accreditations leave California elections in violation of the requirement to have EAC-approved VSTLs certify voting machines, despite California accepting Federal funds under HAVA.

37. The Federal Help America Vote Act of 2002 ("HAVA") provides for the accreditation of voting systems by Voting Systems Testing Laboratories ("VSTLs"). States can opt out, but California's application for voting system approval requires Federally approved VSTL reports on the systems seeking approval:

a. "In addition to the completed Application forms and system documentation detailed above, the applicant must also provide the following supplementary materials as part of the Application:

1. All federal Voting System Testing Laboratory (VSTL) reports on the voting system. These must all be in electronic format and must all be sent directly from the VSTL to the Secretary of State. If the reports have not yet been finalized, please have the VSTL sends the most current available versions. The reports must cover the exact version of the system and its components for which approval is sought. If any of the reports are "supplemental" covering the modifications to the system since the previous report, please have the VSTL send all supplemental reports, as well as the original report on which they are based. Finally, if there are modifications to the system for which there is no VSTL report, please have the VSTL send us a statement that modifications are not material and federal testing is not required." *See "California Application for the Approval of a Voting System – Application Instructions", updated October 25, 2016.* (https:// votingsystems.cdn.sos.ca.gov/cert-and-approval/vsysapproval/vsys-applic-instructions.pdf).

2. California accepted Federal Funds for election machines as recently as 2018, totaling $34.6 million, according to the 2018 HAVA Election Security Grant Budget. (https://www.eac.gov/sites/default/files/havadocuments/CA_Narrative_Budget.pdf)

3. In 2020, HAVA Federal funds appropriated to California were $38.7 million, plus another $7.7 million from the state, the highest of any state. (https://www.eac.gov/sites/default/files/news/documents/ 2020HAVA_State_Allocation_Chart_with_Match.pdf)

38. Both VSTLs typically accredited by the EAC, Pro V&V and SLI Gaming, themselves lacked accreditation in the 2020 election. [See Exhibit A].

IV. SPECIFIC VIOLATIONS TO EAC AND HAVA BY SAN DIEGO

1. In reference to Exhibit B, the letter from County of San Diego Registrar of Voters response is they use The San Diego County Registrar of Voters Election Management System is DIMS.net Product Suite, version 10.0.7531.25123, Runbeck Election Services, Inc. (877) 230-2737.

In reviewing Tore's affidavit:

"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 modification and verification of meeting the pertinent standards.

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

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

2. The key aspect and summary of the sometimes-technical affidavit in layman's terms is itsparagraph 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."COMPLAINT FOR INJUNCTIVE RELIEF.

3. Because the County of San Diego's voting systems were not accredited by VSTLs with valid EAC accreditations before the November 2020 election, the County of San Diego did not meet the VSTL requirement, since VSTLs were not operating as required in the United States due to the lack of current accreditations.

4. The County of San Diego implemented new voting systems on February 4, 2020 to be used in the following elections: March 3, 2020; November 3, 2020; September 14, 2021; June 7, 2022; November 2022 election. Therefore, election results were and will be subject and vulnerable to modification by foreign or domestic nefarious actors; such fraudulent results will impact the legitimacy of the Legislative branch of the Federal government and thus affect all 50 states.

5, The County of San Diego and SOE corporation Contract #552907 provides training software updates for elections staff and volunteers. This is problematic as indicated by the following:

a. According to Exhibit A, Terpeschore Maras provides evidence of the conflict of interest in VSM software and election result reporting. Two companies in particular, Huawei and Akamai, the latter of which is partnered with SCYTL, with SCYTL being linked to Dominion Software. SCYTL receives the tallied votes on behalf of Dominion and, under contract with Associated Press (AP), provides the results for reporting. This shows that voting information is under the control of the companies that provide the Voting Systems (Exhibit A.) the Program Director were remiss in their duties in acknowledging the expiration of certification.

b. She further elaborates on the "trapdoor" mechanism available to alter votes via algorithms in the encryption process of which she observed in the 2020 election. Summarizing her example using SCYTL.

Step 1: A ballot containing votes is encrypted by Dominion and sent to SCTYL.

Step 2: SCYTL Takes those ballots and using a key generator agreed to by both parties (Dominion and SCYTL) access the contents of the encrypted ballots.

Step 3: The algorithm then re-encrypts the ballots using the same key generator to create a ciphertext such that the encrypted processed ballots appear as the original from Dominion.

Step 4: Decryption and public release of the vote tallies.

> "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)."
>
> "54. Trapdoor is a cryptotech term that describes a state of a program that knows the commitment parameters and therefore is able to 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 anyone 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)." (Exhibit A).

6. Voting System Test Laboratories, further known as (VSTL), Pro V&V, NTS Huntsville (formerly Wyle Laboratories), know further as (NTS), and SLI Compliance accreditation(s) provided from the Election Assistance Commission, further known as (EAC), for the 2020 General Election and subsequent elections thereof, were not in compliance with the written policy of the **EAC voting System Test Laboratory Program Manual, version 2.0, (OMB-3265-0018)[2], Section 3.4, 3.6 and 3.8** which violate the federal standards for laboratory testing accreditation set forth in the **HELP AMERICA VOTE ACT 2022, (HAVA ACT)[3], Subtitle B §231 (a) (1) (2) (b) (1).**

7. This lack of compliance not only violates Federal codes and official policy of the EAC, but also violates **CALIFORNIA ELECTION CODE § 19006 (2019),** as well as the Secretary of State Administrative Code **CALIFORNIA ELECTION CODE § 19101(a) (2019) and CALIFORNIA VOTE CCR § 20700(a) (2020), and Cal. Elec. Code § 19210-19211 (2019).**

8. These VSTLs were used in testing and certification of the Voting System Machines further known as (VSM) used in the California 2020 General Elections and elections thereafter.

9. Per the (VSTL) Voting System Test Laboratory Program Manual ver. 2.0 effective May 31, 2015, page 38, Sec. 3.6.1.[4] Certificate of Accreditation: A Certificate of Accreditation

[2] https//www.eac.gov/sites/default/files/eac assets/1/28/VSTLManual %207%208%2015%20FINAL.pdf

[3] https://www.congress.gov/107/plaws/pub/252/PLAW-107publ252.pdf

[4] https://www.eac.gov/sites/default/files/eac assets/1/28/VSTLManual%207%208%2015%20FINAL.pdf

shall be issued to each laboratory by vote of the Commissioners. The Certificate shall be signed by the CHAIR of the Commission and state:

"3.6.1.3 The effective date of the certification, which shall not exceed a period of two (2) years."

So not just the date is important, but the signature on the Lab Certification of Accreditation is very crucial. The Commission Chairman only serves one (1) year, but their signature is good on those certificates for two (2) years.

10. The (VSTL) program requires certified laboratories to submit an application package to the Program Director, consistent with the procedures of Section 3.4, no earlier than 60 days before the accreditation expiration date, and no later than 30 days before their accreditation expires. Pro V&V and SLI Compliance did not submit an application prior to the expiration date in 2015 and 2017 respectfully. The EAC and in her own words:

> "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 2020. 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. (Exhibit A.), paragraph 60-63, page 110.

11. Maras covers in great detail how 2020 Election reporting demonstrated this algorithm in key swing states as examples and further demonstrates plaintiffs claims on lack of VSTL EAC

Accreditations, FAC violations of the HAVA Act, and the importance of robust testing of the SMs and EMS systems to help ensure fair elections. (Exhibit A.)

12. **CONCLUSION:** This affidavit (Exhibit A) presents unambiguous evidence of:

a. Foreign Interference

b. Complicit behavior by the previous administrations from 1999 to present to hinder the voice of the American People.

c. Knowingly and willingly colluding with foreign powers to manipulate the outcome of the 2020 election.

d. Foreign nationals, through investments and interests, assisted in the creation of the Dominion software.

e. Akamai Technologies merged with a Chinese company that makes and distributes the COTS components of election machines.

f. U.S. persons holding an office and private individuals knowingly and willingly oversaw fail safes to secure our elections.

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

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

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

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

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

l. AKAMAI Technologies and Hurricane Electric raised serious concerns for the NATSEC due to their ties with foreign hostile nations (Exhibit A.)

13. Based on pending and closed California Open Records Requests, Plaintiff believes that the Secretary of State require every California County to use an election night reporting program from SCYTL. This is the same company referenced in Exhibit L., which casts further doubt on election integrity. (Exhibit M.)

V. SUMMARY/CLOSING

1. There is an urgency to Plaintiff's petition with the upcoming election scheduled on November 8, 2022 using electronic voting equipment that has not been EAC certified and has "TRAPDOOR MECHANISMS" that allow the manipulation of the vote. The main violation of VSTL EAC accreditations render the EAC VSM certification invalid. The reason for such policy and law is to ensure that the SM and their software do not have vulnerabilities that could be exploited to undermine election integrity and are set forth by **EAC Voting System Test Laboratory Program Manual, version 2.0 (OMB-326-0018)[5], Section 3.4, 3.6 and 3.8** to meet the federal standard for laboratory testing accreditation set forth in the **HELP AMERICA**

[5] Https//www.each.gov/sites/default/files/eac assets/1/28/ VSTLManual%207%208%2015%20FINAL.pdf

VOTE ACT 2002, (HAVA ACT)[6] **Subtitle B § 231 (a) (1) (2) (b) (1).** Exhibit A., affidavit of Terpesehore Maras, filed under penalty of perjury on December 1, 2020 in ase #2-20-cv-01771-PP in the 2nd Judicial District of the Denver District Court in Denver, Colorado[7], explains the trapdoor mechanism in the encryption/decryption process. the conflict of interest with SCYTL, the foreign interests involved, the EAC violations, the importance of VSTLs, and testing of COTS. The approval by the Secretary of State for use in California with such gaps in EAC policy and potential vulnerabilities violates our State Constitutional rights and laws, **CALIFORNIA ELECTION CODE 19205, CALIFORNIA VOTING SYSTEM STANDARD 7.5 OPEN ENDED VUNERABiLITY TESTING**[8] as well as our U.S. Constitutional rights and laws, **U.S. Constitution 14th Amendment, 52 U.S. Code § 20971, and HAVA of 2002 § 231.** For all the reasons above a complete failure of duty to provide safe and just elections are observed.

2. Plaintiff sent two demand letters for the preservation of election evidence on August 29, 2022 ahead of the scheduled destruction date of September 3, 2022 for the November 2020 election data. CALIFORNIA ELECTIONS CODE § 17502 (Exhibit V)

VI. ELECTION SOFTWARE WHISTLEBLOWERS

1. **CLINTON E. CURTIS** - Creator, Vote Fraud Software Program in Florida, 2000 On

December 13, 2004, Clinton Eugene Curtis gave sworn testimony before the House of Representatives Democrats of the Judiciary Committee. The committee was convened to

[6] https://www.congress.gov/107/plaws/publ252/PLAW-107publ252.pdf

[7] https://storage.courtlistener.com/recap/gov.uscourts.wied.92717/gov.uscourts.wied 92717.9.13.pdf

[8] https://admin.cdn.sos.ca.gov/regulations/elections/califonria-voting-system-standards.pdf

determine if the vote counting process of the 2004 U.S. General Election could have been manipulated. Mr. Curtis explains to the committee his work at Yang Enterprises (YEI) and the vote fraud software program (VFSP) he built while working at YEI at the request of Tom Feeney (Florida House Speaker) to steer elections before the 2000 U.S. General Election. He explains how votes can be manipulated without any knowledge of election officers and vote system inspectors and also offers superficial clues to look for when considering electronic vote tampering. Curtis explains how the VFSP can move from machine to machine in virus-like manners and stresses the necessity of examining uncompiled source-code of vote systems before those systems are deployed, being a requirement to ensure election integrity. Attorney Cliff Arnebeck questions Mr. Curtis before the committee; Representatives Stephanie Tubbs Jones, Maxine Waters and Jerrold Nadler also question Curtis. A summary of facts given both during testimony at the Judiciary Committee [Exhibit C, page 23 – transcript of committee testimony] and in his sworn affidavit [Exhibit D, page 33] follows.

Curtis was the lead programmer for YEI in Orlando, Florida. YEI was working to contract with the Florida government with the assistance of lobbyist Tom Feeney. Curtis became Feeney's tech advisor for the proposed projects and Feeney would advise YEI on how best to procure the contracts.

In October of 2000, Feeney requested that YEI develop a prototype of a VFSP to alter vote tabulation during elections. Feeney was specific in the design and specification making sure that the VFSP was deployable on touch screens, hackers had the ability to trigger the VFSP without additional equipment, and that the VFSP remained hidden even if the election system was inspected. Curtis pointed out that if uncompiled source-code were inspected, the VFSP would be detected. HOWEVER, if the VFSP was compiled, inspection would NOT REVEAL its presence.

Curtis thought his VFSP was to be used to flush out potential election security deficiencies. He created the VFSP, proved functionality, AND created an automated version that required no user intervention. The VFSP was invisible to voters and election supervisors and could be deployed as many times as needed to achieve the desired result across a single race and/or multiple races. No amount of testing would reveal the vote fraud that had occurred as activation and processing of the VFSP was completely invisible to everyone, except the person deploying the VFSP.

Curtis also supplied a report to educate those examining vote machines how to 'see' the invisible fraud – by looking at uncompiled source-code. Curtis stated in his affidavit: "Conversely, if they allowed blind (already compiled) code to be used (no source-code provided) and there were no paper receipts, the votes could be flipped from one candidate to the other without any possible way for the deception to be detected. I explained that this could be done with a touch screen machine or automatically. She [YEI's CEO] immediately stated, 'You don't understand, in order to get the contract, we have to hide the manipulation in the source-code. This program is needed to control the vote in South Florida.' I was shocked that they were actually trying to steal the election and told her that neither I nor anyone else could produce any such program. She stated that she would hand in what I had produced to Feeney and left the room with the software." [Exhibit D, ¶ 9, page 35]

2. **J. ALEX HALDERMAN** – A Decade Spent Studying EVMS Hacking

J. Alex Halderman, Computer Science and Engineering Professor at University of Michigan has spent over a decade hacking electronic voting systems, studying their vulnerabilities, documenting the ease with which electronic vote systems are manipulatable, gave Congressional testimony on the matter, and regularly speaks about election hacking. Halderman has consistently presented the sheer ease with which he and his team gain remote electronic access into vote machine systems as well as the thin margins needed to steal general elections.

One of the most alarming facts Halderman points out is that comprehensive threat assessments and cybersecurity best practices are not employed when designing EVMS. Halderman's suggestions for defending election infrastructure from these inherent weaknesses are miniscule in cost comparison to present budgets allocated to vote security and elections. Halderman's suggestions rely on common sense quality control, tried and tested methods of paper ballots, risk limiting audits, comprehensive threat assessments and cybersecurity best practices. [Exhibit E, page 38 – Halderman's prepared congressional testimony July 21, 2017]

Halderman's studies, declarations, and testimony were incorporated into a key Georgia case (Curling v. Kemp, CIVIL ACTION NO. 1:17-CV-2989-AT, September 17, 2018 and Curling v. Raffensperger, et. al. CIVIL ACTION NO. 1:17-CV-2989-AT, filed September 28, 2020) revealing substantial election security issues. Halderman performed a 12-week intensive testing of the Dominion Ballot Marking Device (BMD) and identified multiple SEVERE SECURITY FLAWS which could be exploited to install malicious software either remotely or in person. He authored a 25,000-word report detailing how votes can be altered while escaping detection of procedural protections of acceptance testing, hash validation, logic and accuracy testing, external firmware validation, and risk limiting audits. The report was subsequently sealed by presiding Judge Amy Totenberg.

The public is deprived of the granular details Halderman's report outlines. However, two of Halderman's affidavits entered into the cases reveal several salient details. The first affidavit argues the nature of changes Pro V&V made to updated software fails a "de minimis" standard and explains why:

a. Pro V&V testing of Dominion BMD software 5.5.10.32 is inadequate. He states about the effort, "The report makes clear that Pro V&V performed only cursory testing of this new software. The company did not attempt to independently verify the cause of the ballot display problem, nor did it adequately verify that the changes were an effective solution. Pro V&V also appears to have made no effort to test whether the changes create new problems that impact the reliability, accuracy, or security of the BMD system." [Exhibit F, ¶ 2, page 47]

b. Changes made to 5.5.10.32 are NOT "de minimis" changes requiring one line of configuration code having no material impact of system configuration. Pro V&V directly stated, they made two different kinds of changes in five different lines of source-code. [Exhibit F, ¶ 3, page 48]

c. he nature of the changes was altering HOW the program operated in every instance the line of code was used. The resulting changes could cascade into multiple files, and he goes on to say that these types of changes often introduce new bugs. (Exhibit F, ¶ 4, page 48]

d. He further emphasizes the impossibility of evaluating changes of this nature by only examining source-code. [Exhibit F ¶ 5, page 49]

e. Zero regression testing (checking that a change to a system does not break existing functionality) was performed. [Exhibit F, ¶ 6, page 49]

f. New software was compiled for distribution and installation throughout Georgia. Compiled code is in a non-human readable format, and therefore unconfirmable, that what was distributed and installed was faithful to the original build. [Exhibit F, ¶ 11, page 52] The new software was distributed and installed into Georgia BMD AFTER the system had been certified. Pro V&V submitted a report seeking approval for a de minimis change, which if more than de minimis change, does not comport with lawful EAC certification protocols and would require recertification of the EVMS.

g. Curiously, Halderman takes the opportunity to note that Pro V&V, one of two labs certified by the EAC for EVMS accreditation, does NOT support HTTPS encryption on its website, and notes it as a sign (because it is the most basic of security) that other best practices of security are maintained. [Exhibit F, ¶ 12, page 53]

h. In the second Affidavit, Halderman rebuts expert witness disclosures used on behalf of the defense effort authored by Dr. Juan Gilbert and Dr. Benjamin Adida. Noteworthy points follow:

1. Neither of the defendant's expert witnesses, who were able to access Halderman's sealed report offered any rebuttal to the numerous, critical vulnerabilities described within. Neither witness claimed to have examined the EVMS used in Georgia, nor undertook such an inquiry to do so. [Exhibit G, ¶ 2, page 55]

2. Established cybersecurity protocol requires state defendants to subject Georgia's BMD to rigorous testing in response to Halderman's report to assess extent and significance of vulnerabilities identified in report. [Exhibit G, ¶ 3, page 56]

3. The report discloses SEVERE SECURITY FLAWS, which Halderman is prepared to demonstrate in court. [Exhibit G, ¶¶ 4 and 5, page 57]

4. Specific to Dr. Gilbert's testimony, the claims are vague generalities; Gilbert ignores the relative ease with which the EVMS can be hacked; Gilbert ignores the accepted standard of election security which compels reduction points of attack to EVMS immediately upon discovery; and Gilbert ignores the fact that Georgia requires less than adequate risk limiting audits (one RLA of statewide contests, every 2 years). [Exhibit G, ¶¶ 6, 7, 8, and 9, pages 58-59]

5. Halderman's report outlines several routes by which malicious hardware or software can manipulate QR codes causing recorded votes to differ from voters's elections, demonstrates Georgia's Ballot Marking Devices can be manipulated AND escape detection on recount or audit, election

officials and poll workers would likely NOT suspect a systemic problem with the BMD's, malicious malware could be programmed to remove all traces of its presence after manipulating ballots, said malware would not be detected by any of the defenses the defendants purport to practice, said malware would defeat QR code authentication, logic, and accuracy testing, on-screen hash validations and external APK validation. [Exhibit G, ¶¶ 10,11, 20, 24, pages 59-70]

6. Halderman points out Gilbert's statement of not being aware of any "provided equipment marred by 'undetectable' hacks to any other independent researcher" and also chooses NOT to evaluate Halderman's submitted report or examine voting equipment. [Exhibit G, ¶ 24, page 70]

7. Halderman draws attention to Gilbert equating BMD insecurity to hand-marked systems and that Gilbert has recently developed his own BMD system to address some of Georgia's reliability issues.

8. Specific to Adida, Halderman makes clear Adida's declarations predate his report. [Exhibit G, ¶ 29, page 75]

3. **RUSSELL RAMSLAND** – 18 Month Study of ES&S and Dominion EVMS

Ramsland holds multiple degrees (MBA, Harvard; Political Science, Duke), has worked with NASA and MIT, has run many businesses very highly technical in nature, and has served on government technical panels. He serves on the management team of Allied Security Operations Group, LLC (ASOG) which is comprised of former DoD, Secret Service, DHS, CIA and provides a range of security services with particular focus on cybersecurity, open source investigation, and penetration testing of networks. In 2018, ASOG analyzed audit logs for the central tabulation server of ES&S EVMS for the Dallas County Texas General Election. ASOG discovered thousands of error messages that should not have occurred, and an election operator ignored and overrode all error messages. The discovered irregularities resulted in an 18-month study conducted on ES&S and Dominion EVMS for both the states of Texas and Arizona, and led to legal challenges for the 2018 Texas General Election; findings are outlined in Russell Ramsland's declaration filed in Bowyer v. Ducey, 2:20-CV-02321-DJH. [See Exhibit H, page 79]

The investigation included ES&S and Dominion literature background research; confirmed evidence of Democratic and Republican stakeholders in vulnerability of ES&S and Dominion; Texas rejecting Dominion's certification for use in their state due to vulnerabilities; verified, major vote tampering using ES&S EVMS in Dallas County, TX 2020 General Election. Passive penetration testing provided a stunning finding: vulnerabilities previously identified were STILL LEFT OPEN TO EXPLOIT in the November 2020 election. Due to ES&S and Dominion's Common ancestry in Diebold EVMS, striking similarities exist in software, therefore striking similarities in vulnerabilities. [Exhibit H, ¶ 4, page 80]

Both ES&S and Dominion EVMS (collectively, SYSTEMS) contain a large number of hacking/tampering vulnerabilities either front-end with BMD or back-end in vote storage, tabulation, and reporting by election officials. Vulnerabilities have been well documented, well known, and experts have written extensively about these vulnerabilities. [Exhibit H, ¶ 6, page 81]

Key components of SYSTEMS offer paperless usage allowing for no permanent record of voters choice to be recorded and utilize unprotected logs allowing for hackers/external operators to arbitrarily add, modify, or remove log entries, causing the SYSTEMS to log erroneous election events. Creation and maintenance of various logs is voluntary, offering perfect opportunities to conceal actions. These deficiencies do not support the stated purpose of functional, transparent audit logs to the public or election officials. [Exhibit H, ¶¶ 7, 8, page 81]

Electronic vote switching in Antrim County Michigan was reported. First reports suggested a "glitch" because of an 'update to the system', which would have required EAC recertification by law. The initial report was recanted, and the 'error' was attributed to 'clerical error'. Based on acquired information surrounding the event, ASOG believes the 'glitch' was an update to the system (as originally reported). Glitches of this type cause votes to be misread or redirected to another candidate. [Exhibit H, ¶ 10, page 81]

During the time period of Oct. 7 – Oct. 30, 2020, 53,485 voter records had their unique hash identifier changed in Dallas County, TX. The tampering took the form of purging votes and reconstituting them in some form or fashion resulting in the hash total changing (meaning the legitimate vote was altered), and evidence shows that approximately 107,000 votes were hacked in Dallas County alone. Key to understanding the gravity of this, Ramsland explains: "In plain English, at the instant before a voter casts a ballot there is a one-to-one relationship between the voter and their ballot as well as a one-to-one association between the voter and their votes. At the instant that ballot is cast, the one-to-one relationship between the voter and the ballot still exist, but the relationship between the voter and their votes is gone. NO ONE can know how they voted. The key security check on voting integrity is the absolute match between the number of voters in the Vote Roster and the number of ballots counted. If these numbers do not match, either physical ballots were added or removed from the Ballot Counter or "voters" were added or removed from the Vote Roster. In either case, the election has been compromised and the election is nothing more than a lottery. Tens of thousands of Vote Roster entries undeniably purged and another tens of thousands of entries apparently created out of thin air, using the ES&S system." [Exhibit H, ¶ 11, page 82]

In the case of Dallas County, 92% of purged in person and absentee voters were over 65 Years of age, making it crystal clear that the ES&S EVMS contains the apparent ease of targeting specific groups within the voter base via an inside or outside actor(s) with access to the ES&S EVMS. [Exhibit H, ¶ 12, page 83].

Ramsland notes statistical red flags in Pima and Maricopa County Arizona voter turn-out above 80% of county voter records. And with statistical red flag voter turn-out, Pima county tabulated over 32,000 excess votes over the maximum expected and Maricopa County tabulated over 68,000 excess votes over the maximum expected. [Exhibit H, ¶ 13, 14, page 85]

Ramsland declares the data strongly suggests the use of an 'additive algorithm'. Dominion's user guide, Chapter 11 covers deploying Ranked Choice Voting Method (RCV), which allows election officials and workers to deploy weighted values for each vote. In other words, one vote could be tallied fractionally or in multiples based upon the set parameters of weighting and Dominion's EVMS provides for such features. Ramsland noted statistical impossibilities proving the use of algorithm(s) to tabulate votes. Additionally, operators are able to use completely blank ballots and block allocate those blank ballots to a specific candidate. [Exhibit H, ¶ 15, page 86] Any vote tally total reflecting decimals points in the total is evidence of 'additive algorithms' being used in that tally. Effort is made to remove the fractional decimals reflected in tallies before the results are released publicly, though, on rare occasions, uneven tallies are seen in public.

Another statistical red flag ASOG's team discovered was "improbable, and possibly impossible" voting spikes based upon the on hand EVMS available on site. In other words, a dump of 143,100 votes occurred at 8:08pm in Maricopa County Arizona on Nov. 3, 2020 COULD NOT HAVE legitimately occurred as physically processing that number of ballots in the given time frame was not possible using the on hand EVMS. The spike of votes cast almost exclusively for one candidate would be easily explained by the deployment of algorithm(s) or batch allocation of blank ballots. [Exhibit H, ¶ 16, page 86]

4. **TERPSEHORE MARAS:** EX-MILITARY AND INTELLIGENCE SUBCONTRACTOR

Terpsehore Maras served in the U.S. Navy and as a private contractor specializing in foreign intelligence. She functioned in the capacity of localizer during deployment of projects and operations within the contiguous 48 states and District of Columbia (CONUS), and outside the continental United States (OCONUS). She is a trained Cryptolinguist, holds a completed degree in molecular and cellular physiology and has formal training in other sciences such as computational linguistics, game theory, algorithmic aspects of machine learning, and predictive analytics. Maras has operational experience in U. S. intelligence sources and methods of implementing operations during elections both CONUS and OCONUS. Additionally, Maras is an amateur network tracer and cryptographer and has over two decades of mathematical modeling and pattern analysis. Maras is an expert witness regarding elections CONUS and OCONUS due to nearly two decades subcontracting for the U. S. Intelligence or 9 EYES.

Ms. Maras' sworn declaration, dated Nov. 29, 2020 and filed in case Feehan v. Wisconsin Elections Commission, et. al. Case No. 2:20-CV-01771-PP [Exhibit A], explains the inherent vulnerabilities in EVMS which provides for 'invisible' manipulation of votes. Her affidavit explicitly presents financial conflicts of interest, national security risks affecting vote integrity, lack of proper voter machine certification and the intrinsic inability of Voting System Test Laboratories (VSTL) to competently and accurately certify voting machines.

a. ELECTION ASSISTANCE COMMISSION AND VTSLs

Maras points out that the Election Assistance Commission (EAC) certification of Pro V&V expired on Feb. 24, 2017 and remains unaccredited since 2017, even though EVMS are being unlawfully 'certified' and deployed all over the United States since 2017. [Exhibit A, ¶ 8, page 90] Congressionally passed Help America Vote Act of 2002 (HAVA) dictates that the EAC provide accreditation of independent, non-federal laboratories qualified to test EVMS to federal standards (Section 231(b) of HAVA 42 U.S.C. §15371(b)). Only two companies are accredited VSTL's through the EAC. Procedures of the requirements to obtain EAC Accreditation are outlined in The EAC Voting System Test Laboratory Accreditation Program Manual (VSTLAPM) and the EAC Voting System Testing and Certification Program Manual (VSTPM). State participation in

HAVA is voluntary, any state that volunteers to participate must adhere to the requirements set forth by HAVA Federal Standards, which are realized through EAC function, administration, policies and procedures outlined in the aforementioned manuals. Pro V&V and SLI Gaming lack evidence of proper EAC Accreditation per the VSTLAPM. [Exhibit A, ¶¶ 8, 9, 10, 11, 12, 18, pages 90-97]

Maras establishes Pro V&V's conflicts of interest in that owner/operator Ryan Jackson Cobb formerly worked under the entity of Wyle Laboratories which is an aerospace defense contracting entity. Additionally, the address on file at EAC and NIST differ from the address Pro V&V publishes on its website. Wyle was a very early tester of EVMS in the 1990's, tested over 150 different EVMS, was the first company to obtain accreditation by the EAC as a VSTL, and received NVLAP accreditation to ISO/IEC 17025:2005 from NIST. [Exhibit A, ¶¶ 19, 21, page 98]

b. VSTLs and COMMERCIAL OFF THE SHELF COMPONENTSThe VSTLs are critical for election machine integrity as they examine commercial off the shelf components (COTS). COTS are used in most EVMS and preferred because they are tried and tested in the open market, most economical and readily available. However, use of these crucial components confer several fractures in election integrity:

i. COTS are sourced from foreign nations such as China and Germany.

ii. In science, computing and engineering, a "black box" is a system which can be viewed in terms of inputs and outputs, without any knowledge of its internal workings, and has an implementation that is opaque. COTS are the Black

Box" in U.S. EVMS which provide for completely undetectable fraud, misappropriation of votes and backdoor access to the voting machines.

iii. COTS are inherently "black box" components due to constant changes in specifications and hardware and support third party software that can be classed as proprietary and often undergoes updates.

iv. Because of constant changes in specs and hardware of COTS, these updates are/can be overlooked, therefore, causing a critical vulnerability ripe for election fraud.

v. Exporting system reporting using software like Crystal Reports or PDF software allows for vulnerabilities with constant updates.

vi. Cloud software companies providing networking services to U.S. elections are provided through companies in China and Germany. [Exhibit A, ¶¶ 20 – 26, pages 99-101]

c. NATIONAL SECURITY THREATS VIA OFFSHORE INTERNET SERVICE

Maras states the following national security flaws are affecting many sectors of government, military, and U.S. elections:

i. Akamai Technologies (AT), having offices in India, China, Japan, Singapore, Australia and New Zealand, working through Germany, is a Laos founded Chinese linked cloud service company. AT works with SCYTL, who provides election reporting services for Dominion.

ii. Level 3 (L 3) Communications is a federal contractor providing communications services for the Federal Government is partially owned by George Soros, the billionaire founder of liberal political infrastructure. L 3 develops, produces and integrates communication systems and support equipment for space, air, ground, and naval applications, including C41 systems and products, integrated Navy communications systems, integrated space communications and RF payloads, recording systems, secure communications and information security systems.

iii. Michigan's government website is thumped off AT servers which are housed on Telia A.B., a foreign server in GERMANY.

iv. SCYTL contracts with Associated Press to receive tallied election results from SCYTL on behalf of Dominion and was selected by the Federal Voting Assistance Program of U.S. Department of Defense to provide 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 also works with a large number of states, making SCYTL, a foreign company, the largest provider of election reporting results. All of these practices are serious threats to U.S. National Security and U.S. elections nationwide. [Exhibit A, ¶¶ 26 – 34, pages 100-105]

d. VSTLs AND NATIONAL SECURITY

The importance of VSTLs being accredited is to ensure that no foreign interference or "bad actors" can access tally data via backdoors in equipment software. SCYTL's core software used in election reporting and all related EVMS ensures "anonymity." Algorithms employed to shuffle data to maintain anonymity provides for the ability to set values to achieve a desired election outcome and masquerades under the guise of encryption in Trapdoors (also referred to as Trapdoor Commitment Keys and Commitment Keys; referred to TDCK hereafter, exclusive of quoted text). A TDCK is a cryptotech term describing a state of a program that knows the commitment parameters and therefore is able change the value of the commitments to predetermined values. Maras declares, "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 algorithms or manual scripts to fractionalize or distribute pooled votes to achieve the outcome you wish – you cannot prove they are doing it! See STUDY : 'The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiability of the Scytl- SwissPost Internet voting system.'" [Exhibit A, ¶¶ 37 - 39, page 105]

e. SCYTL'S ALGORITHMIC TREATMENT OF VOTES

i. Once cast, all votes are sent offshore to SCYTL for configuration of data.

ii. The vote is cleansed, categorized, and judged invalid or valid.

iii. Every vote is shuffled and mixed and then re-encrypted. This phase of electronic handling is the most vulnerable due to TDCK and the inability to determine whether the vote delivered from the shuffling/mixing phase matches the vote cast.

iv. Anyone having access to the TDCK can see the parameters of the algorithm deployed and how the algorithm redistributes the votes.

v. The TDCK is said to only be held by SCYTL and Dominion, offering unfettered access to determine who wins the election.

vi. Within the TDCK, algorithms behave to move the goal posts in elections without being detected. Algorithms being deployed can be seen in elections when one candidate has a spike while the other candidate drops or stays the same. Or if there are pauses in elections, this is when block allocations for the predetermined winner can be observed by those experienced in TDCK deployment, without detection by otherwise unsuspecting election officials, election workers and the public. [Exhibit A, ¶¶ 41 – 59, pages 105-110]

Among the most critical pieces of data contained in Maras' declaration is the fact that SCYTL's election reporting software, providing for anonymity, is founded upon zero-knowledge proofs which allow a prover to convince a verifier that he/she holds information that satisfies some desirable properties without revealing anything else. Therefore, one cannot prove any manipulation of data occurred. Our election 'integrity' is built upon "… the perfect Three Card Monty…" offering zero proof of integrity of the vote. If decryption is challenged, the TDCK holder can provide some proof that would pass blind verification. A case study by TheUniversity of Melbourne done in March of 2020, proved that alteration of vote by using TDCK was undetectable. In other words, one could not prove the outcome was altered; one could not prove the outcome was NOT altered. [Exhibit A, ¶¶ 60-63, page 110]

f. REAL LIFE EXPERIENCE ENGINEERING ELECTIONS USING SCYTL

Maras goes further to excellently outline reporting behavior patterns consistent with alteration of votes using TDCK, which manifests as "vote dumps" and "stalled election reporting." Having personally witnessed U.S. interference in Ukraine's 2014 Presidential Election and having personal knowledge of programs deployed by the Obama administration in 2013 to assist the Ukraine with U.S. Taxpayer Funded 'democratic elections', Maras personally observed the same vote irregularities in both 2016 and 2020 U.S. General Elections, as was observed in Ukraine's 2014 [compromised] Presidential Election. Important to note:

i. The Obama administration hired SCYTL to provide EVMS and software in the Ukraine;

ii. CyberBerkut was accused of infiltrating central election computers and deleting key files, however, the key files were TDCK utilized by SCYTL to tally the votes (as proven by disclosed emails outlining how their vote was rigged and that they attempted to avoid a fixed election);

iii. In the early AM hours of May 25, 2014 election results were blocked and the final tally delayed.

iv. In 2016, what was first thought to be Russellian hackers in Georgia's elections, was later found to match an IP address used by the Department of Homeland Security;

v. DDoS attacks were claimed to have been perpetrated, however what occurred was mitigation of deploying TDCK requiring Dominion, ES&S, Smartmatic, and Hart Intercivic representatives manually deploy the TDCK to reach the desired election outcomes;

vi. Maras further outlines key events occurring during the 2020 General Election that strongly indicate TDCK were utilized by SCYTL to engineer the results. [Exhibit A, ¶¶ 64 – 100, pages 111-117]

vii. Maras explicitly declares personal knowledge of using modems to deploy TDCK as the point of access to steer the compromised 2014 Presidential

Election in Ukraine. [Exhibit A, ¶ 112, page 119]

g. EAC VSTL CERTIFICATION FAILURES AFFECT HAVA COMPLIANT STATES

When the EAC VSTLs were allowed to fall out of compliance with lawful accreditation, every state tasked with Independent Verification and Validation of EVMS, all states electing to participate in HAVA failed to uphold their own states' standards, which remain federally regulated per HAVA. Any VSTL with a NIST certificate fails to comport with lawful edicts required by HAVA. NIST's role is clearly laid out in the EAC Voting System Test Laboratory Accreditation Program Manual (VSTLPM) Section 1.3 and the EAC Voting System Testing and Certification Program Manual (VSTCPM) Section 1.6.2.3. Both Pro V&V and SLI Gaming received NIST certification outside the 24-month scope outlined in HAVA, VSTLPM, and VSTCPM. Pro V&V NIST certification was granted for one year; SLI Gaming NIST certification was granted for 90 days, and granted 27 days before general election; none of which comports to EAC standards outlined in the referenced manuals above. Any state voluntarily participating in HAVA, claiming their state acquired lawful accreditation is false. [Exhibit A, ¶¶ 101 – 107, 113 - 115, pages 117-120] More detailed examination of EAC certifications follow below.

h. GEMS SOFTWARE (OWNED BY SCYTL), DOMINION AND ELECTIONS

Maras declares personal knowledge of high-level officials in the Obama/Biden administration and large private contracting firms meeting with software company GEMS. GEMS is software deployed on all EVMS running under the Dominion flag. GEMS was created by SOE software and purchased by SCYTL developers in conjunction with U.S. Federally Funded persons.[Exhibit A, ¶¶ 116, 117, page 120] John McCain's campaign assisted in funding the development of GEMS web monitoring via WEB Services with 3EDC and Dynology. [Exhibit A, ¶¶ 121, 122, page 120] GEMS only functions across all machines if all counties across the United States are housed on the same server. GEMS was fine tuned in Latvia, Belarus, Serbia and Spain to be localized for EU deployment as observed during the SwissPost election debacle. [Exhibit A, ¶¶ 118, 120, page 120]

i. AKAMAI TECHNOLOGY - GOVERNMENT INTERNET SERVICE PROVISION

AT services SCYTL, houses all foreign government sites, houses all .gov state sites, and AT is Edge Gateway based out of Germany. Using AT allows all .gov sites to obfuscate and mask their systems using Hurricane Electric (he.net) which then routes traffic anonymously to AT offshore servers. AT house all .gov information in Germany via Telia A.B. AT has worldwide locations including China and Iran. AT merged with Unicom (Chinese Telecom) in 2018. [Exhibit A, ¶¶ 122 – 135, pages 121-122]

j. MARAS CONCLUDES by enumerating gravely serious and illegal interferences to the conducting of fair and just elections and National Security of which elections are a critical part of

k. Foreign interference in the U.S. 2020 Presidential Election, chiefly foreign party interests, financing, and assistance for the creation of GEMS (software foundational to Dominion) and AT merging with a Chinese company to make COTS used in EVMS.

ii. EAC failing to abide by HAVA standards, lack of ensuring EAC conducts its duties as set forth by HAVA, and lacking required quorums authorized to issue EAC Certifications.

iii. Serious national security threats from use of AT and HE ties with foreign, hostile nations and U.S. Intelligence Community's direct and indirect procurement of services for the assistance, development, implementation, and promotion of GEMS.

iv. Military (Cyber Brigade) use of ShadowNet Platform deployment to 30 states (coincidentally, the same states using Dominion EVMS) under the guise of L-3).

5. CHRISTOPHER KREBS – Former Director, CISA

Senate Testimony, DEC. 12, 2020, while giving Senate testimony to Senator Ron Johnson, Krebs admits internet connections are present during elections. Transcript of pertinent Krebs testimony from 12/16/2020 hearing - [Exhibit I, page 127]:

a. Christopher Krebs: (01:10:56) "Yeah. There are a number of different systems and machines and computers involved in the entirety of the election process, from registration, through ballot design, through ballot printing, to actual voting, into the tabulation and post-election process. Throughout, you're going to, particularly where a vote is cast on Election Day, those machines tend to, and should not be connected to the internet, certainly as a best practice."

b. Chairman Ron Johnson: (01:11:22) "But some have the capability, don't they?"

c. Christopher Krebs: (01:11:24) "Some may have modems that are typically disabled, but in certain states, I believe in Wisconsin, some are temporarily activated to transmit some counts. But again, when you have paper and you can conduct a post-election.." [crosstalk 01:11:38].

d. Chairman Ron Johnson: (01:11:38) "Again, if there-"

e. Christopher Krebs: (01:11:39) "It's an important security control that-"

f. Chairman Ron Johnson: (01:11:42) "Oh, absolutely."

g. Christopher Krebs: (01:11:43) "That technology in elections are used to facilitate access and increase accuracy of the process. But election officials are very careful that technology is not a single point of failure and that there are security controls before, during, and after the vote process."

h. Chairman Ron Johnson: (01:12:01) "Yeah, finish just answering the computer thing, we'll come back, my time's already expired, but we'll come back to how many audits, the statistical sampling, that type of thing, to use those paper backups to the electronic voting. But finish this answer."

i. Christopher Krebs: (01:12:13) "Right. And as you move out from Election Day, there will be tabulators that may have internet connections to transmit the vote from the precinct, to the county level, to the state, again, security controls in place. And as long as you have the paper, can't hack paper-"

j. Chairman Ron Johnson: (01:12:29) "Right, right, right."

k. Christopher Krebs: (01:12:30) "You can run that process…" [crosstalk 01:12:32].

l. Chairman Ron Johnson: (01:12:31) "But those tabulators are connected on Election Day, because that's how they transmit the data to the counties and also into the unofficial-"

m. Christopher Krebs: (01:12:39) "In some cases, yes, sir."

n. Chairman Ron Johnson: (01:12:40) "Yeah."

o. Christopher Krebs: (01:12:40) "That's right."

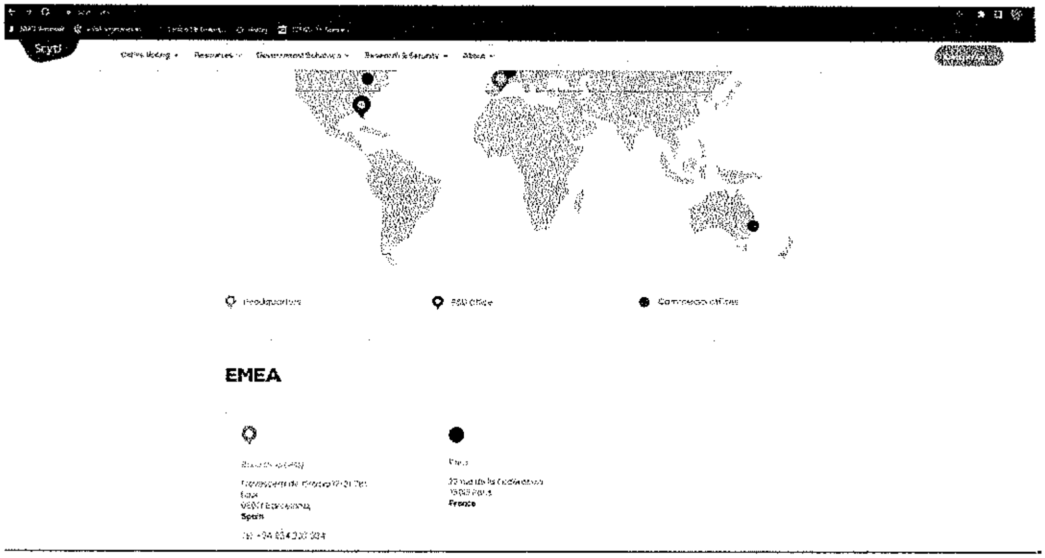
p. Chairman Ron Johnson: (01:12:40) "Okay."

6. CISA RELEASES SECURITY ADVISORY FOR DOMINION EVMS

On June 3, 2022, CISA finally admitted Dominion EVMS has security vulnerabilities in Report ICSA-22154A, outlining several exploitable points of attack and providing suggestions for mitigation. Many hazard CISA released this report as a pre-emptive strike to the release of the sealed Halderman Report. [Exhibit J, page 135 – CISA announcement and Security Advisory]

7. SCYTL – THE GHOST IN THE MACHINE AND THE THREAD THAT RUNS THROUGH IT

In addition to the declarations Maras makes about SCYTL (software that ensures anonymity and cannot provide verifiable proof of secure tallies; DoD selected to provide voting capabilities to the military and overseas voters; tallies votes for the largest number of states; works with AT; contracts with Associated Press to tally Dominion's election results for which Associated Press reports; was contracted to provide software and EVMS in Ukraine and was intended to be the point of deployment for TDCK; SCYTL owns GEMS via SOE; GEMS requires ALL county governmental networks across the country to be housed on the same server to deploy GEMS software on all EVMS), several other points must be noted. Not only is it quite obvious that all present EVMS are deficient for conducting free and fair elections, lack proper hardening and cybersecurity best practice protocols are not employed, specific **foreign companies** have been contracted to control the majority share of tabulation and reporting. [See scytl.com/contact]



EMEA

Spain

Paris
France

Targeting of EVMS is not even required if moving desired election outcomes through the use of TDCK during tabulation and reporting of election results is utilized. Companies providing tabulation and reporting are critically important to the infrastructure of elections, and have thus far, mostly remained out of the purview of examination, creating yet another grave election security concern. An obviously simple but key point to examine is how live election results are tabulated and reported if EVMS are purportedly NOT CONNECTED TO THE INTERNET. Reasonable common sense tells us that live, real-time results are not possible without internet connectivity. Christopher Krebs, former Dir., CISA recently admitted during testimony in a Congressional hearing that vote machines were connected to the internet for tabulation. Foundational to vote security are air-gapped voting systems. Many states, California included, codified law(s) barring all EVMS from any internet connectivity whatsoever.

On May 24, 2022, California Secretary of State, Shirley Weber, gave an on-camera video conference interview with San Diego Union Tribune Editorial Board. During the interview, Ms. Weber commented on internet connections and the voting machines (https://www.sandiegouniontribune.com/opinion/story/2022-05-26/secretary-of-state-shirley-weber-elections-reparations-voting-rights). At the 31:39 mark of the interview timeline, board member Kristy Totten, an Opinion editor and producer for The San Diego Union Tribune, questioned Ms. Weber:

a. KRISTI TOTTEN: (31:39 to 31:47): "Do you think we will ever be able to vote by phone or internet? I read a lot during the pandemic about why that's not necessarily a good idea, but is there any conversation around it?"

b. SECRETARY OF STATE WEBER (31:48 to 32:58): "There has always been a lot of conversation around it, and it always ends up in the same place, that we can't secure it. And so therefore, and **that's why there is a law that says we cannot have any internet voting. None of our machines can be connected to the internet because it's not secure enough** and, uh, people believe that it will increase the amount of fraud even more. And I think, uh, ideally we would say 'great, we should be able to do that' but.. um.. every.. all the evidence says that, that we haven't gotten to that level yet. In terms of being able to secure.. we.. it can happen but we can't guarantee that it would be secure, yeah….So all the stuff you've been reading is the stuff we've been reading as well. When it's came

> before the committee, when I was on… when I was Chair of the Elections Committee, uh.. much of **the conclusions ended up the same way**, you know **it's not secure, we can't secure it** and so therefore, with all the ... and I think if people saw all of the, the cyber stuff that comes through our office, from our whole, our office of cyber security, we have a couple offices of cyber security, I think they would probably conclude that, it's probably not worth it at this point."

SCYTL's own election night reporting .pdf reads, "• Secure cloud service platform built on sound network infrastructure; • Adheres to extensive global security standards; • Content delivery network distributes load & provides 24/7 availability." They claim secure cloud service while it is hosted in foreign nations. Details provided by Maras clearly demonstrate SCYTL's service and security standards only serve to erode U.S. National Security. [Exhibit K, page 194] The words, "Powered by SCYTL" with the word 'SCYTL' hyperlinked back to SCYTL's home page appears on many state and local government web pages, election report webpages, etc., in the footer of these pages. Web searches produce results too numerous to elaborate in full detail here, however, several examples are included in Exhibit L to highlight the saturation of state and local government pages hosted by SCYTL, therefore AT. This begins to confirm Maras' claim of all county servers being housed on the same system in order to use GEMS. Webpages with the following URL string included: https://results.enr.clarityelections.com/CO/113964/web.285569/#/summary run through SCYTL servers. ClarityElections.com resolves to or navigates to www.SCYTL.us. Most interesting is Nebraska's Sarpy County election results page; link: (https://results.enr.clarityelections.com/NE/Sarpy/64652/182419/en/summary.html), which returns a 404-error page which is hosted by SCYTL. A screenshot of the archived webpage was taken from the Wayback Machine on Archive.org at 4:42pm PT on July 3, 2022. By 11:05 pm PT on the same day, the archived page was curiously scrubbed from the internet. [Exhibit L, page 197]

The County of San Diego contracted with SOE Corporation for SCYTL Election Training Software between January 29, 2016 and November 4, 2020. [Exhibit M] All SCYTL Online Training includes standardized training modules addressing cyber security awareness [Exhibit N]. SCYTL was formed in Barcelona Spain, marking yet another large tech firm having enormous impact upon U.S. elections being domiciled in a foreign country, defying best practices for National Security. Not only are several key companies with involvement in U.S. elections FOREIGN, but many of the EVMS companies have very incestuous company and executive ancestry. [Exhibit O] is a small but vital collection of news articles outlining some of the very surface details of the corporate and executive histories of the brands used in the United States. In order to be fully informed on the matter, forensic research should be conducted on the corporate filings of these companies to explore any potential common corporate shells that further obfuscate deeper financial ties of common ownership, executive leadership, executive/ staff revolving doors between governmental oversight or elected offices and EVMS companies. Examples of this is Ramsland pointing out that both Dominion and ES&S shared common ancestry in Diebold. In 2013, Smartmatic and Dominion had a legal battle over which company would hold the worldwide rights to common software both companies employed in their EVMS. The case was tried in chancery court in Delaware, case number C.A. 7844-VCP.

8. SAN DIEGO COUNTY VOTING CENTERS IDENTIFIED AS WI-FI-ENABLED ON JUNE 7, 2022, DURING THE PRIMARY ELECTION.

a. Stanley Recreation Center 3585 Governor Dr, San Diego, CA 92122 around 7:20 pm [Exhibit P]

9. SIX LOS ANGELES COUNTY VOTING CENTERS IDENTIFIED AS WI-FI-ENABLED ON JUNE 4, 2022 AND JUNE 7, 2022, DURING THE PRIMARY ELECTION UNDER THE NETWORK ID VSAPRRCC.

The following public six voting centers in Los Angeles County were identified as having the active and publicly available WI-FI-enabled network ID, VSAPRRCC [See Exhibit Q]:

a. Coolidge school San Gabriel CA [See *Exhibit Q - mobile phone screenshot A*].

b. San Gabriel high school [See Exhibit Q - mobile phone screenshot B].

c. Armenian center Pasadena [See mobile phone screenshot C, Exhibit Q].

d. Victory Park Pasadena [See Exhibit Q - mobile phone screenshot D,].

e. Carver school San Marino [See Exhibit Q - mobile phone screenshot E].

f. School San Gabriel Blvd. at Duarte Rd. [See Exhibit Q - mobile phone screenshot F].

10. EIGHT ORANGE COUNTY VOTING CENTERS IDENTIFIED AS WI-FI-ENABLED ON JUNE 4, 2022 UNDER NETWORK ID CP(#). [Exhibit R]

On June 4th, 2022 in Orange County, California voter Matt Hamilton observed eight polling stations and found each site indicating a designated Wi-Fi network ID of 'CP' and a corresponding site number. Each of the Civic Center, Library, City Hall, and Sports Park locations were equipped with its own free and publicly available Wi-Fi connection, despite California law barring them from being connected to the internet or even having the capability of being connected to the internet. The designated Wi-Fi addresses for each location are reflected below, while the mobile screenshot images captured by Mr. Hamilton at the time of his observations are attached as Exhibit R. The following is formatted as Wi-Fi Address - Network ID - Physical Address – Date – Time:

a. FE:22:32:41:5A:5F **CP94** - El Toro Library, 24672 Raymond Way, Lake Forest, CA 6.4.22. 13:21 PT

b. EA:AC:A1:5B:2D:DD **CP93** - Lake Forest Senior Center, 100 Civic Center Drive, Lake Forest, CA 6.4.22 13:42 PT

c. DA:C5:81:A9:69:75 **CP95** - Foothill Ranch Library, 27002 Cabriole, Lake Forest, CA 6.4.22 13:52 PT

d. FA:7D:2E:3F:5C:51 **CP96** - Lake Forest Sports Park, 28000 Rancho Way, Lake Forest, CA 6.4.22. 14:07 PT

e. 2A:3F:89:F5:42:30 **CP138** - Shepherd of the Hills RSM, 30605 Avenida De Las Flores, Rancho Santa Margarita, CA 6.4.22. 14:22 PT

f. FA:DD:1A:90:8E:5B **CP137** - Bell Tower Regional Community Center / RSM City Hall, 22232 El Paseo, Rancho Santa Margarita, CA 6.4.22. 14:28 PT

g. DA:7B:4D:BA:1B:EA **CP136** - Rancho Santa Margarita Library, 30903 La Promesa, Rancho Santa Margarita, CA 6.4.22. 14:33 PT

h. 62:A8:B5:EE:ED:A9 **CP139** - Trabuco Canyon Water District, 32003 Dove Canyon Drive, Trabuco Canyon, CA 6.4.22. 14:39 PT

11. EAC CERTIFICATIONS EXAMINED

Per the EAC website, only two companies are presently VSTLs – Pro V&V and SLI Gaming. [Exhibit S] The final, valid EAC certification for Pro V&V expired in 2017. The certification signed by Executive Director, Mona Harrington, dated Feb. 2, 2021 is invalid as Harrington is NOT lawfully allowed to sign EAC certifications (see law cite, next ¶). Additionally, this certification asserts that accreditation is "effective until revoked by a vote of the EAC pursuant to 52 U.S.C 20971(c)(2) (see law cite, next ¶)."

Certifications for SLI do not comport with lawful EAC Certification. The EAC certificate signed By Brian Newby in 2018 reflects certification lasting three years, which is out of compliance with VSTLPM stating EAC certifications may only be issued for 2 years maximum, EAC VSTLPM 3.6.1.3. Newby is an Executive Director; VSTLPM rules dictate that only the EAC Chair is authorized to sign EAC certifications, VSTLPM 3.6.1,

thus further rendering both Pro V&V and SLI certifications issued after 2017 invalid. [Exhibit T – EAC certifications, etc.] Additionally, as pressure mounted for EAC VSTL lack of compliance, the EAC attempted to assert unlawful authority on two occasions. On Jan. 27, 2021, Jerome Lovato asserts that CV-19 is the outstanding circumstance upon which the renewal of certification was not conducted and additionally asserts that Pro V&V still retains its VSTL accreditation. CV-19 WAS NOT present prior to 2020, so this excuse only made the EAC look foolish for claiming valid certifications were not issued in 2017 and 2019 due to CV-19; every other sector of government and businesses continued to work remotely. Sometime after Jan. 27, 2021, in an undated statement, the EAC then claimed an administrative error during 2017-2019 - the failure of the EAC to issue updated certificates and asserted Pro V&V and SLI remained in good standing. [Exhibit T – EAC certifications, etc.]

The entire process of recertification is quite lengthy occurring over several months, requiring voluminous reporting, applications, etc. on a specific schedule – there is no data which suggests these rigorous processes occurred AND the certifications issued during the 2018 timeframe, as outlined above, do not comport with lawful standards. Congressionally passed HAVA, EAC VSTLPM and VSTCPM manuals do not outline exceptions for proper certification due to national emergencies and pandemics; stating the VSTL's maintained compliance because the certification was never revoked also does not comport with HAVA, VSTLPM and VSTCPM.

The EAC has failed to post the required public data about each VSTL

publicly on its website as outlined in VSTLPM 3.6.2 and has accrued an extraordinary number of failures to meet the requirements of public disclosure over several years. This can be proven by looking at archived versions of the pages that now display information that falls far below the standard outlined in VSTLPM 3.6.2. The EAC has failed EAC quorum standards required to issue EAC certifications more times than succeeding to EAC quorum standards since its inception [Exhibit T]. This fact is easy to establish simply by looking at the years when the EAC actually had less than 4 commissioners. When sending a FOIA request to the EAC for current certifications issued to VSTLs, the response received has been that no EAC certifications are available [Exhibit T – EAC certifications, etc.] or the request for information goes unanswered beyond the lawfully permitted response time from confirmation date of receipt of the request. EAC Certification of VSTLs is a matter of public record and the lack of compliance by the EAC falls negligibly short of the lawful standards by which the EAC is required to comply. The government agency tasked with the job of securing EVMS reliability, transparency and standards of function has a history of repeatedly disregarding its own required standards, per HAVA §20926, Dissemination of information, VSTCPM Section 1.15, and VSTCPM, Sec. 10.2. The federal executive and legislative branches continue to ignore these shortcomings, despite being repeatedly made aware of such willful disregard of compliance. [Exhibit A, ¶ 8, page 9] Of importance to note: the EAC's VSTCPM, Section 3.2.3 states in very certain terms, "Significance of an EAC Certification. An EAC certification is an official recognition that a voting system (in a specific configuration or configurations) has been tested by a VSTL to be in conformance with an identified set of Federal voting standards. An EAC certification is not: (VTSCPM Section 3.2.3.2) A Federal warranty of the voting system or any of its components." Basically, the EAC is released for any liability for its certification(s) of VSTLs testing of EVMS.

Concluding on EAC certifications: any state participating in HAVA, whether federally or optionally state accredited, asserting they obtained lawful EAC certification is either woefully mis or malfeasant in conduction of the duties of their office. All states have selected an executive office to manage the integrity of elections which includes the oversight of certification and accreditation of all EVMS used in their state and that public officials (appointed or elected) are duty bound to perform due diligence on these matters as well as duty bound to act within the parameters of the State Election Code for EVERY ELECTION and for EVERY ASPECT OF THE VOTING PROCESS.

VII. STATEMENT OF CONCLUDING FACTS

12. CYBERSECURITY AND SYSTEMIC INFILTRATION OF EVMS

a. UNDENIABLE EVMS VULNERABILITIES & LACK OF EVMS HARDENING

The last two decades have provided an abundance of cyber professionals undeniably demonstrating EVMS insecurities, vulnerabilities, attack points. The evidence is clear – any presently used EVMS is far too soft a target to prevent vote fraud. We should be asking: "WHY?" Governmental bodies have consistently avoided any serious, consequential hardening of EVMS through egregious inaction, expert rebuttals of stated cyber vulnerabilities and sealing crucial evidence and documentation from public scrutiny. It is important to note that many of EVMS systems, tabulation and reporting services used in the United States are born and headquartered in foreign countries. This is a threat to national security. Is any investigator or body examining reporting and tabulation within the scope of election security? Again, we should be asking: "WHY?"

b. Governmental bodies have consistently avoided any serious, consequential hardening of EVMS through egregious inaction, expert rebuttals of stated cyber vulnerabilities and sealing crucial evidence and documentation from public scrutiny. It is important to note that many of EVMS systems, tabulation and reporting services used in the United States are born and headquartered in foreign countries. This is a threat to national security. Is any investigator or body examining reporting and tabulation within the scope of election security? Again, we should be asking: "WHY?" reached many of the same or similar conclusions. Those conclusions are further aired by the insight of Maras:

i. confirms zero-knowledge proofs (no way to prove fraud exists; no way to prove fraud DOESN'T exist)

ii. confirms TDCK are responsible for vote dumps occurring when election reporting stalls

iii. confirms EVMS have internet connection

iv. confirms observed election reporting patterns of vote dumps and paused reporting/counting

v. confirms cybersecurity best practices are avoided It is critical to extrapolate from the 'Statement of Facts' section: the conclusions reached by non-governmental professionals identifying the security weaknesses in EVMS literally further PROVE THE ACCURACY of the declarations of government whistleblowers Curtis and Maras. There are several common factors in their declarations. Both Curtis and Maras state the inability to prove fraud once EVFS and TDCK are deployed. Both EVFS and TDCK, while materially different, function in apparent virus-like spreads that can move or 'seem to move' throughout EVMS. Both Curtis and Maras give sworn testimony of government officials colluding in the engineering and steering of elections. The testimony of Curtis and Maras allow examiners of that testimony to see the weight and gravity of one simple fact: governmental actors have been the chief architects of systemic vote fraud over two decades across several continents. Both Curtis and Maras observed additional crime perpetrated by federal and local government officials beyond the scope of voting, details which are included in their sworn declarations.

c. EVMS, SCYTL AND GEMS

An additional extrapolation should also be noted: the broad use of EVMS, SCYTL equipment and services, and the use of GEMS offers deep enough penetration in the U.S. election EVMS market, to thoroughly engineer any election, whether local, county, state or federal. The only areas not a target of vote fraud are those refraining from use of EVMS and tabulation and reporting services.

13. CISA AND EAC

Christopher Krebs, former CISA Director, admitted during Senate testimony that EVMS had internet connections during voting, tabulating, and reporting. This is a damning admission that is counter to ANY election security. And Krebs' confirmation of this also underlines that all America's votes are tallied and reported using FOREIGN SERVICES AND SERVERS. The EAC, simply put, does not consistently comport with CRITICAL, FOUNDATIONAL Operational duties. Having a legal quorum that can properly execute EAC accreditation and certification of VSLTs is the most basic foundation that the EAC has repeatedly failed to maintain. Additionally, HAVA specifically states that accredited labs be non-federally affiliated, and NIST recommended, per 20971(b)(1). Therefore, why is CISA examining the EAC/VSTL related matters regarding the recent report from ICSA regarding Dominion EVMS?

14. PERTINENT CALIFORNIA ELECTION CODES, HAVA FUNDS, BROKEN LAWS

a. HAVA STANDARDS

HAVA outlines minimal standards for both federal AND state testing and certification of EVMS in 52 U.S.C. § 20971 Certification and testing of voting systems. Section (a)(1) states, "The Commission shall provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories." Sections (a)(2) states, "At the option of a State, the State may provide for the testing, certification, decertification, or recertification of its voting system hardware and software by the laboratories accredited by the Commission under this section."

HAVA clearly states optional state testing and certification MUST use EAC accredited labs for all EVMS employed in the state. If the EAC failed to lawfully certify VSTLs, then optional state testing and certification also FAILS LAWFUL testing and certification. For any years that EAC failed to supply lawfully accredited VSTLs, the HAVA participating states also fell short of lawful testing and certification.

b. CALIFORNIA'S PARTICIPATION IN HAVA

From 2009 – early 2020, the state of California volunteered to adhere to the standard of federal certification directly through the EAC. The pertinent California Election Codes governing this status are: **"The Secretary of State shall establish the specifications for and the regulations governing voting machines, voting devices, vote tabulating devices, and any software used for each, including the programs and procedures for vote tabulating and testing. The criteria for establishing the specifications and regulations shall include, but not be limited to, the following: (a) the machine or device and its software shall be suitable for the purpose for which it is intended, (b) the system shall preserve the secrecy of the ballot, (c) the system shall be safe**

from fraud or manipulation." CA ELEC CODE § 19205 (West 2009). On and after January 1, 2005, the Secretary of State shall not approve a direct recording electronic voting system unless the system has received federal qualification and includes an accessible voter verified paper audit trail. CA ELEC CODE § 19250 (West 2009). [Exhibit U]

In early 2020, the state of California changed the voluntary participation in HAVA to Baseline HAVA standards. HAVA's state requirement handbooks dictates the following for Baseline Requirements:

"State statutes and/or regulations do not explicitly state that voting systems must be tested to federal standards or be certified by a federal agency or federally accredited laboratory. However, voting systems must, at a minimum, meet standards for voting equipment set forth by the 2002 Help America Vote Act (HAVA)." [Exhibit U]

The EAC kindly provides a list of all Federal HAVA Funds (HAVA$) dispersed to each state for HAVA participation. For many years in which the state of California received HAVA to conduct HAVA compliant elections and failed to do so, the State of California has misappropriated U.S. Taxpayer Dollars. Since the State of California has been voluntarily participating in HAVA since its inception, the state has collected $490,956,981.00 in HAVA$ for participation. Nearly $110,000,000.00 has been received by the state of California since 2018. The receipt of HAVA$ requires the state to comply with HAVA standards. IF the state of California was receiving HAVA$ and not lawfully supporting HAVA standards, that is, minimally, misuse of funds. [Exhibit U]

15. CALIFORNIA ELECTION CODE

a. California Election Code (CEC) § 18500 states, "Any person who commits fraud or attempts to commit fraud, and any person who aids or abets fraud or attempts to aid or abet fraud, in connection with any vote cast, to be cast, or attempted to be cast, is guilty of a f felony, punishable by imprisonment for 16 months or two or three years."

b. CEC § 19001 clearly states, "This division shall be liberally construed so that the real will of the electors will not be defeated by any informality or failure to comply with all of the provisions of the law." Defined in CEC § 10500 as "Voter" means a voter or elector as respectively defined in the principal act of each district or agency. It will be Interesting to discover the number of counts of violations of the above two codes. The state of California is duty bound by CEC §19001 to respect the will of the people as it relates to elections.

c. CEC § 19006.b clearly states the state will adopt and publish testing standards that meet or exceed HAVA standards. And yet, the state is presently failing HAVA standards. CEC § 19006.c clearly states,

"encourage development of EVMS that makes use of nonproprietary source code." This is a fantastic idea, however EVMS are riddled with proprietary source code and COTS which are black box inclusions in EVMS that can and do escape adequate testing.

d, CEC § 19105 requires the SECRETARY OF STATE to investigate any alleged violation of CEC, SOS regulations with the power to s subpoena all necessary records. The SOS is bound by her Oath of

Office and the California and United States Constitutions to do so. To date, she has merely stood by.

f. CEC § 19205 states: A voting system shall comply with all of the following:

i. No part of the voting system shall be connected to the Internet at any time.

ii. No part of the voting system shall electronically receive or transmit election data through an exterior communication network, including the public telephone system, if the communication originates from or terminates at a polling place, satellite location, or counting center.

iii. No part of the voting system shall receive or transmit wireless communications or wireless data transfers.

g. California Elections do not comport with any point in this codification. All points of CEC § 19283 (referenced above in HAVA section) were violated.

16. CALIFORNIA VOTER ROLLS

In 2018, Judicial Watch sued the state of California for inflated voter rolls (Judicial Watch, Inc.et al. v. Dean C. Logan, et al. (No. 2:17-cv-08948)); eleven of fifty-eight counties reported registration rates that exceeded 100% of the age-eligible persons. The case was eventually settled with the state of California agreeing to remove 1.5 MILLION names from the inflated voter rolls without admission of guilt. States are expected to remove invalid names from voter rolls and federal law makes the removal mandatory, so it is a wonder why the state of California allows its voter rolls to exceed, by approximately 25%, the legitimate number of eligible voters.

17. SYSTEMIC EVMS INSECURITY WARRANTS IMMEDIATE INJUNCTION

Eligible and active voters have NO METHOD of obtaining proof that votes were counted as they were cast. Because of the likelihood that votes were manipulated or changed, any eligible voter desiring vote accuracy, transparency, and free and fair elections is aggrieved. Any eligible voter who cannot prove their vote was counted as cast, is an aggrieved party. Every eligible voter is owed proper due process under California Constitutional law, Article 1, Section 3 guaranteeing the people the right to instruct their representatives, petition for redress of grievances, and is additionally enshrined in the United States Constitution's 14th Amendment. Voting Americans have ZERO assurance their inalienable Constitutional rights are not eroded and that every voting American can exercise the rights set forth in the United States and California Constitutions. Because

American voters are "more likely to be injured if injunctive relief is erroneously denied than Defendants would be if injunctive relief were erroneously granted," this factor tips in favor of granting an injunction. NuScience Corp. v. Henkel, No. CV 08-2661GAF (FFMX), 2009 WL 10700220, at *11 (C.D. Cal. Apr. 14, 2009). The rendering of a fully informed determination, one that factors in the critical facts contained herein regarding the 2020 election results, will require time. However, as the court is aware, the window of opportunity to make those determinations ends with the scheduled purge of 2020 election results on September 3, 2022, per 52 U.S.C. § 20701. All California 2020 election results data, including but not limited to any digital records ranging from all processes related to voting through election vote tallies, any physical ballots, and any and all election EVMS, EVMS data, machines, hardware and software must be protected and any and all officials responsible for its care and maintenance must be enjoined from the destruction or purge of the 2020 election results and related data and material upon the end of the 20-month retention period until such time that proper investigation can be legitimately and transparently carried out and proper, reasonable and fair remedies sought. The 2022 midterm elections are near and stand to be conducted using the same critically unsecure Electronic Voting Machine Systems that are completely void of integrity and reliable cybersecurity. The reality is stark:

All states participating in HAVA are using EVMS that fail compliance standards REQUIRED by Congressionally passed HAVA. THEREFORE, any election conducted using EVMS by any state participating in HAVA is illegally and unlawfully conducted, therefore rendering any election results tallied using unlawfully accredited EVMS null and void.

The affidavits of Maras and Curtis demonstrate that engineered election fraud has been organized since the use of EVMS, meaning the will and voice of all Americans has been defrauded for at least two decades. The only means of truly recording free and fair elections is by old technology - hand marked paper ballots. Therefore, an Immediate Injunction enjoining the deployment and use of any Electronic Voting Machine Systems tabulation and election reporting software and/or hardware be forthwith banned, and conduction of future elections restricted to old technology of tried and true, common-sense methods of conducting in-person voting and hand-marked ballots until all security vulnerabilities inherent with EVMS tabulation and reporting. "Fraud vitiates everything, and a judgment equally with a contract; that is, a judgment obtained directly by fraud, and not merely a judgment founded on a fraudulent instrument; for, in general, the court will not go again into the merits of an action for the purpose of detecting and annulling the fraud" United States v. Throckmorton, 98 U.S. 61.

The United States of America was foundationally constructed upon the power resting with the people. ***Our vote is our preeminent civic expression of freedom of speech, guaranteed by the United States Constitution, 1st Amendment.*** Any election conducted using the present EVMS tabulation and reporting services, i.e., engineered election results, usurps the entire system of the people's government, the power of the people, and the Constitutions of every state in the nation

.

I. COUNT I

Denial of Equal Protection: 14th Amendment of U.S. Constitution; 42 USC (1983)

18. Plaintiffs repeat and reallege every allegation contained in the foregoing paragraphs as if fully plead herein.

19. The 14th Amendment of the U.S. Constitution provides "nor shall any state… deny to any person within its jurisdiction equal protection of the laws."

20. The Supreme Court of the United States has recognized that the right to vote consists of not only casting a ballot, but having that vote counted accurately, as it was cast;

21. "We regard it as equally unquestionable that the right to have one's vote counted is as open to protection by Congress as the right to put a ballot in a box." See *United States v. Mosley, 238 U.S. 386 (1915);*

22. "No right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined." *See Wesberry v. Sanders, 376 U.S. 17 (1964);*

23. "No one would deny that the equal protection clause would . . . prohibit a law that would expressly give certain citizens a half-vote and others a full vote . . . .[T]he constitutionally guaranteed right to vote and the right to have one's vote counted clearly imply the policy that state election systems, no matter what their form, should be designed to give approximately equal weight to each vote cast . . . . [A] state legislature cannot deny eligible voters the right to vote for Congressmen and the right to have their vote counted." *See Reynolds v. Sims, 377 U.S. 563 (1964), citing Colegrove v. Green, 328 U.S. 549, 328 U.S. 569-571*

24. By utilizing voting machines that are in fact subject to the Trapdoor mechanism described in Exhibit A, the County of San Diego has deprived its voters the capability of knowing that their vote was accurately counted. As long as the voting machines are used, no citizen can be assured their vote was free from being modified by a person(s) working with the Trapdoor mechanism, and therefore citizens of California were denied equal protection under the election laws.

25. Plaintiffs are entitled to temporary, preliminary, and permanent injunctive relief by:

1. Restraining Defendant from destroying the November 2020 election data as permitted 22 months after the election, until a thorough investigation of the software and its Trapdoor functions and vulnerabilities can be undertaken.

2. Ordering Defendant to de-certify the November 2020 election results.

3. Ordering Defendant to stop the use of election machines and to reconfigure elections to be held exclusively with hand-counted paper ballots.

4. Ordering Defendant to place a record retention hold as it relates to the November 2020 state and federal elections.

a. All voter data collected by an electronic poll book and/or a local election management system

b. Precinct register pages with signatures and button text

c. All voting machine tapes AVC and ICX

d. All results reports including the worksheet, the ICC result printout, the ICX result report, and the challenge removal reports.

e. All public and protective count sheets for early voting.

f. All election verification forms for early voting.

g. All records of elections submitted after the election reflecting ALL machines used in the election even if delivered on election day.

h. All notation of irregularities reports.

i. The list of early voters checked during preparation and verification.

j. The reports printed from the California Secretary of State's Online Voting Registration system reflect everyone given credit for voting on election day, early voting and absentee by mail.

k. The updated turnout report for each county district.

l. AVC layout sheets showing lockout information in each precinct.

m. Alex Padilla's Notice of Withdrawal of Certification and Conditional Approval of Voting systems – Effective August 27, 2019

5. Ordering Defendant to stop the implementation or use of print your own ballot programs in the County of San Diego

(See https://www.sos.ca.gov/administration/regulations/current-regulations/elections/ballot-printing).

II. COUNT II

Denial of Due Process: 14th Amendment of U.S. Constitution; 42 USC 1983

26. Plaintiffs repeat and reallege every allegation contained in the foregoing paragraphs as if fully plead herein.

27. The Supreme Court of the United States has recognized that the right to vote consists of not only casting a ballot, but having that vote counted accurately, as it was cast.

28. "We regard it as equally unquestionable that the right to have one's vote counted is as open to protection by Congress as the right to put a ballot in a box." *See United States v. Mosley,*

238 U.S. 386 (1915)

29. "No right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined." *See Wesberry v.*

Sanders, 376 U.S. 17 (1964)

30. "No one would deny that the equal protection clause would . . . prohibit a law that would expressly give certain citizens a half-vote and others a full vote . . . .[T]he constitutionally guaranteed right to vote and the right to have one's vote counted clearly imply the policy that state election systems, no matter what their form, should be designed to give approximately equal weight to each vote cast . . . . [A] state legislature cannot deny eligible voters the right to vote for Congressmen and the right to have their vote counted." *See Reynolds v. Sims, 377 U.S. 563 (1964), citing Colegrove v. Green, 328 U.S. 549, 328 U.S. 569-571*

31. By utilizing voting machines subject to the Trapdoor mechanism described in Exhibit A, the County of San Diego has deprived its voters of the ability to know with certainty that their vote was accurately counted.

32. Plaintiffs are entitled to temporary, preliminary, and permanent injunctive relief by:

> 1. Restraining Defendant from destroying the November 2020 election data as permitted 22 months after the election, until a thorough investigation of the software and its Trapdoor functions and vulnerabilities can be undertaken.
>
> 2. Ordering Defendant to de-certify the November 2020 election results.
>
> 3. Ordering Defendant to stop the use of election machines and to reconfigure elections to be held exclusively with hand-counted paper ballots.
>
> 4. Ordering Defendant to place a record retention hold as it relates to the November 2020 state and federal elections.
>
> > a. All voter data collected by an electronic poll book and/or a local election management system

b. Precinct register pages with signatures and button text

c. All voting machine tapes AVC and ICX

d. All results reports including the worksheet, the ICC result printout, the ICX result report, and the challenge removal reports.

e. All public and protective count sheets for early voting.

f. All election verification forms for early voting.

g. All records of elections submitted after the election reflecting ALL machines used in the election even if delivered on election day.

h. All notation of irregularities reports.

i. The list of early voters checked during preparation and verification.

j. The reports printed from the California Secretary of State's Online Voting Registration system reflect everyone given credit for voting on election day, early voting and absentee by mail.

k. The updated turnout report for each county district.

l. AVC layout sheets showing lockout information in each precinct.

m. Alex Padilla's Notice of Withdrawal of Certification and Conditional Approval of Voting systems – Effective August 27, 2019

5. Ordering Defendant to stop the implementation or use of print your own ballot programs in the County of San Diego (See https://www.sos.ca.gov/administration/regulations/current-regulations/elections/ballot-printing).

COUNT III

33. Plaintiffs repeat and reallege every allegation contained in the foregoing paragraphs as if fully plead herein.

34. The Guarantee Clause of the U.S. Constitution states that "The United States shall guarantee to every State in the Union a Republican Form of Government…" (Art. IV, §4)

35. By utilizing voting machines subject to the Trapdoor mechanism described in Exhibit A, the County of San Diego has deprived its voters of the capability of knowing that their vote was accurately counted and did not ensure that the guaranteed republican form of government was in fact provided in the November 2020 elections.

36. Plaintiffs are entitled to temporary, preliminary, and permanent injunctive relief by:

1. Restraining Defendant from destroying the November 2020 election data as permitted 22 months after the election, until a thorough investigation of the software and its Trapdoor functions and vulnerabilities can be undertaken.

2. Ordering Defendant to de-certify the November 2020 election results.

3. Ordering Defendant to stop the use of election machines and to reconfigure elections to be held exclusively with hand-counted paper ballots.

4. Ordering Defendant to place a record retention hold as it relates to the November 2020 state and

federal elections.

a. All voter data collected by an electronic poll book and/or a local election management system

b. Precinct register pages with signatures and button text

c. All voting machine tapes AVC and ICX

d. All results reports including the worksheet, the ICC result printout, the ICX result report, and the challenge removal reports.

e. All public and protective count sheets for early voting.

f. All election verification forms for early voting.

g. All records of elections submitted after the election reflecting ALL machines used in the election even if delivered on election day.

h. All notation of irregularities reports.

i. The list of early voters checked during preparation and verification.

j. The reports printed from the California Secretary of State's Online Voting Registration system reflect everyone given credit for voting on election day, early voting and absentee by mail.

k. The updated turnout report for each county district.

l. AVC layout sheets showing lockout information in each precinct.

m. Alex Padilla's Notice of Withdrawal of Certification and Conditional Approval of Voting systems – Effective August 27, 2019

5. Ordering Defendant to stop the implementation or use of print your own ballot programs in the County of San Diego (See https://www.sos.ca.gov/administration/regulations/current-regulations/elections/ballot-printing).

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff pray for judgment against Defendant(s) as follows:

A. That the Court assumes jurisdiction of this Action;

B. Until Defendant can prove beyond a reasonable doubt that the voting machines, as configured in 2020 for the 2020 elections, and as configured in 2022 for the 2022 elections in California, absolutely comply with every legal requirement as articulated in state and federal laws, CALIFORNIA ELECTION CODE 19205, CALIFORNIA VOTING SYSTEM STANDARD 7.5 OPEN ENDED VULNERABILITY TESTING, and HAVA of 2002 § 231, and prove beyond reasonable doubt that the voting machine and election management system software does not contain code to execute, nor connect to any 3rd party computer networks that can execute or enable "trap door" features as described in Exhibit A:

1. Temporarily restrain, as well as preliminarily and permanently enjoin Defendant from destroying, altering, or otherwise changing all voting machines, software, peripherals, and other data and equipment used to cast, examine, count, tabulate, modify, store, or transmit votes or voting data in the November 2020 elections

held in California and which are planned to be used in the same manner in the upcoming November 2022 elections to be held in California:

2. Order Defendant to preserve in their current state all voting machines, software, peripherals, and other data and equipment used to cast, sequester, count, tabulate, modify, store, or transmit votes or voting data in the November 2020 elections held in California and which are planned to be used in the same manner in the upcoming November 2022 elections to be held in California.

3. Order the State of California and the County of San Diego, to immediately stop the use of any electronic election machines and to configure elections to be held exclusively with same day in person voting, and same day reporting of election results where only voters who are pre-registered US citizens may vote one time each on hand-counted paper ballots, and sign in on paper poll books, and

C. Such other relief as it is just and proper.

Date Signed: October 23, 2022

____

Kristin Vent, Plaintiff, Pro se
2017 Sonett Street
El Cajon, CA 92019
(619) 729-6202
kristinvent17@gmail.com

CERTIFICATION AND CLOSING

Under Federal Rule of Civil Procedure 11, by signing below, we certify to the best of our knowledge, information, and belief that this complaint: (1) is not being presented for an improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; (2) is supported by existing law or by a non-frivolous argument for extending, modifying, or reversing existing law; (3) the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery; and (4) the complaint otherwise complies with the requirements of Rule 11. We agree to provide the Clerk's Office with any changes to my address where related papers may be served. We understand that my failure to keep a current address on file with the Clerk's Office may result in the dismissal of our case.

Date Signed: October 15, 2022

____

Kristin Vent, Plaintiff, Pro se
2017 Sonett Street
El Cajon, CA 92019
(619) 729-6202
kristinvent17@gmail.com

held in California and which are planned to be used in the same manner in the upcoming November 2022 elections to be held in California:

2. Order Defendant to preserve in their current state all voting machines, software, peripherals, and other data and equipment used to cast, sequester, count, tabulate, modify, store, or transmit votes or voting data in the November 2020 elections held in California and which are planned to be used in the same manner in the upcoming November 2022 elections to be held in California.

3. Order the State of California and the County of San Diego, to immediately stop the use of any electronic election machines and to configure elections to be held exclusively with same day in person voting, and same day reporting of election results where only voters who are pre-registered US citizens may vote one time each on hand-counted paper ballots, and sign in on paper poll books, and

C. Such other relief as it is just and proper.

Date Signed: October 23, 2022

Kristi Vent . 10/23/22

Kristin Vent, Plaintiff, Pro se
2017 Sonett Street
El Cajon, CA 92019
(619) 729-6202
kristinvent17@gmail.com

CERTIFICATION AND CLOSING

Under Federal Rule of Civil Procedure 11, by signing below, we certify to the best of our knowledge, information, and belief that this complaint: (1) is not being presented for an improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; (2) is supported by existing law or by a non-frivolous argument for extending, modifying, or reversing existing law; (3) the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery; and (4) the complaint otherwise complies with the requirements of Rule 11. We agree to provide the Clerk's Office with any changes to my address where related papers may be served. We understand that my failure to keep a current address on file with the Clerk's Office may result in the dismissal of our case.

Date Signed: October 23, 2022

Kristin Vent 10/23/22

Kristin Vent, Plaintiff, Pro se
2017 Sonett Street
El Cajon, CA 92019
(619) 729-6202
kristinvent17@gmail.com