

“operates safely, efficiently, and accurately and complies with the voting system standards adopted by the Election Assistance Commission”.

- a. The Denton County Elections Administrator, Frank Phillips, recommended and the County Commissioners Court approved canvassing of the 2020 General Election on Nov 17, 2020.<sup>332</sup>
- b. An assistant District Attorney (John Feldt) informed the Elections Administrator (Frank Phillips) in June 2021 of allegations that county voting machines were not certified<sup>333</sup>.
- c. A county resident (Alana Phillips, a Plaintiff) publicly informed the Commissioners Court on September 28, 2021, that the Hart Inter-Civic voting machine systems were not certified.<sup>334</sup>
- d. Denton County initially stated it used Hart InterCivic Verity 2.4 voting machine systems for the November 2020 election, as shown by an October 6, 2021, email statement from the county<sup>335</sup>.<sup>336</sup> SLI Compliance was the

---

<sup>332</sup> [https://dentoncounty.granicus.com/MediaPlayer.php?view\\_id=26&clip\\_id=1787&meta\\_id=197132](https://dentoncounty.granicus.com/MediaPlayer.php?view_id=26&clip_id=1787&meta_id=197132) Last visited 06/06/22

<sup>333</sup> [https://files.tttexas.com/case/TX\\_SOS\\_Election\\_Violation\\_References](https://files.tttexas.com/case/TX_SOS_Election_Violation_References) See Exhibit 1

<sup>334</sup> <https://rumble.com/vn679l-denton-county-commissioners-meeting-92821-crowdstrike-purchase.html> Last visited 06/07/22

<sup>335</sup> [https://files.tttexas.com/case/TX\\_SOS\\_Election\\_Violation\\_References](https://files.tttexas.com/case/TX_SOS_Election_Violation_References) See Exhibit 2

<sup>336</sup> [https://www.eac.gov/sites/default/files/voting\\_system/files/](https://www.eac.gov/sites/default/files/voting_system/files/)

App.262a

Voting System Test Laboratory (VSTL) for version 2.4 of that voting system, per the EAC website.<sup>337</sup> SLI Compliance has a three-year accreditation certificate on the EAC website from Jan 10, 2018, through Jan 10, 2021<sup>338</sup>. Accreditation, per the EAC Voting System Test Laboratory Program Manual 2 “is valid for a period not to exceed two years.”<sup>339</sup> Therefore, this is an invalid accreditation certificate.

- e. On October 8, 2021, two county commissioners (Edmondson and Williams), the elections administrator (Frank Phillips), and IT and elections personnel met with county residents to discuss election issues. During the discussion about voting machine certification, the elections administrator (Frank Phillips) read aloud the EAC letter claiming Covid-19 was the reason for VSTLs not being certified.<sup>340</sup> A county resident (Alana Phillips)

---

HRT-VERITY-2.4%20Certificate%20and%20Scope%2002-21-2020.pdf Last visited 06/06/22

<sup>337</sup> <https://www.eac.gov/voting-equipment/voting-system-test-laboratories-vstl/sli-compliance-division-gaming-laboratories> Last visited 06/06/22

<sup>338</sup> [https://www.eac.gov/sites/default/files/voting\\_system\\_test\\_lab/files/SLI\\_Compliance\\_Certificate\\_of\\_Accreditation011018.pdf](https://www.eac.gov/sites/default/files/voting_system_test_lab/files/SLI_Compliance_Certificate_of_Accreditation011018.pdf) Last visited 06/06/22

<sup>339</sup> [https://www.eac.gov/sites/default/files/eac\\_assets/1/28/VSTLManual%207%208%2015%20FINAL.pdf](https://www.eac.gov/sites/default/files/eac_assets/1/28/VSTLManual%207%208%2015%20FINAL.pdf) See 3.8 – page 40

<sup>340</sup> [https://www.eac.gov/sites/default/files/voting\\_system\\_test\\_lab/files/VSTL%20Certificates%20and%20Accreditation.pdf](https://www.eac.gov/sites/default/files/voting_system_test_lab/files/VSTL%20Certificates%20and%20Accreditation.pdf) Last visited 06/07/22

explained that the state of emergency was declared after the VSTL accreditation had already lapsed. Both the IT representative (Todd Landrum) and the elections administrator (Frank Phillips) received a copy of Terpsehore Maras's affidavit.

- f. A county resident (Alana Phillips) publicly explained the accreditation and certification issue to the county commissioners on February 1, 2022<sup>341</sup>, and again on April 5, 2022<sup>342</sup>. The commissioners court and elections administrator (Frank Phillips) continued to deny that the voting machines lacked certification.
- g. During the canvas of the Republican Primary election results on March 10, 2022, a precinct chair (Alana Phillips) informed the county chair (Jayne Howell) that voting machines were not certified. The elections administrator (Frank Phillips) continued to state that they are certified.
- h. Denton County later stated in a May 2022 email that it had instead used Hart Inter-Civic Verity 2.4.2 for the November 2020 general election.<sup>343</sup> Neither the EAC nor the

---

<sup>341</sup> <https://rumble.com/vucli7-county-commissioners-meeting-feb-1-2022.html> Last visited 06/07/22

<sup>342</sup> <https://rumble.com/v106quo-commissioners-court-april-5-2022.html> Last visited 06/07/22

<sup>343</sup> [https://files.tttexas.com/case/TX\\_SOS\\_Election\\_Violation\\_References](https://files.tttexas.com/case/TX_SOS_Election_Violation_References) See Exhibit 3

SoS website show certification or approval of that version.

563. Tex. Elec Code states a “voting system may not be used in an election unless the system” . . . “prevents counting a vote on the same office or measure more than once . . . ”<sup>344</sup>. The list of November 2020 voters the county provided shows 49 people voted twice<sup>345</sup>

564. Tex. Elec Code states a “voting system may not be used in an election unless the system” . . . “is safe from fraudulent or unauthorized manipulation”.<sup>346</sup>

565. The list of November 2020 registered voters from the county indicates the registered voters from ages 60 and over exceeded the 2020 Census estimate for those ages. The actual voters exceeded the 2020 Census estimate from ages 70-85<sup>347</sup>.

566. The linear forecast of presidential election voter turnout in Denton County since 1992 indicates 56,967 more ballots than expected were received in November 2020<sup>348</sup>.

567. Voters have standing and are not barred by sovereign immunity claims to challenge an uncon-

---

<sup>344</sup> See TX Election Code § 122.001(a)(8)

<sup>345</sup> [https://files.tttexas.com/case/TX\\_SOS\\_Election\\_Violation\\_References](https://files.tttexas.com/case/TX_SOS_Election_Violation_References) See Exhibit 4

<sup>346</sup> See Tex. Elec Code § 122.001(a)(4)

<sup>347</sup> [https://files.tttexas.com/case/TX\\_SOS\\_Election\\_Violation\\_References](https://files.tttexas.com/case/TX_SOS_Election_Violation_References) See Denton County Exhibit 5

<sup>348</sup> [https://files.tttexas.com/case/TX\\_SOS\\_Election\\_Violation\\_References](https://files.tttexas.com/case/TX_SOS_Election_Violation_References) See Denton County Exhibit 6

stitutional voting system, in spite of what the SoS or other government officials might claim. As stated in *Andrade v. NAACP of Austin*, 345 S.W.3d 1, 8 (Tex. 2011),

“The Secretary urges a blanket rule that would ensure no voter ever has standing to challenge a voting system. We think the Secretary overreaches in that respect. The voters assert a denial of equal protection — a claim voters often have standing to bring. *See Baker v. Carr*, 369 U.S. 186, 206, 82 S.Ct. 691, 7 L.Ed.2d 663 (1962) (noting that voters have standing to bring equal protection challenges to complain of vote dilution, and observing that “[m]any of the cases have assumed rather than articulated the premise in deciding the merits of similar claims”). For example, the Supreme Court has permitted Virginia residents to sue for a declaration that Virginia’s poll tax was unconstitutional. *Harper v. Va. State Bd. of Elections*, 383 U.S. 663, 666, 86 S.Ct. 1079, 16 L.Ed.2d 169 (1966) (holding that poll tax violated the equal protection clause).”

### HARRIS COUNTY

568. Harris County Commissioners, in addition to election officials, have failed to confirm if the voting equipment in Hays County is properly certified. The Harris County elections office has been unresponsive to numerous Public Information Requests. Harris County utilized Hart InterCivic 6.2.1 according to the SoS website “Voting Systems by County” dated 2/11/2020. On July 10, 2020, Peter Lichtenheld Senior

App.266a

VP of Customer Success contacted the SoS's to inform the states that Hart was working with the below counties to upgrade them from their current Verity voting system version to the latest Texas certified version of 2.4 including Harris County.

**Hart InterCivic**

Christine Worrell Adkins  
Legal Director, Texas Secretary  
of State Elections Division  
1019 Brazos Street  
Austin, Texas 78701

July 10, 2020

Dear Christina,

This letter is to inform the Texas Secretary of State Elections Division that Hart InterCivic is working with the following Hart customers in Texas to upgrade them from their current Verity voting system version (noted in the table below) to the latest Texas certified version, Verity version 2.4 certified by the State of Texas on June 26, 2020. There are 31 customers who are currently planning on upgrading after the July 14, 2020 election and before the November 3, 2020 election.

We will update you if there are any changes to this list.

{ dense illegible data table omitted }

App.267a

569. Hart InterCivic with non-subsequent ballot numbers violated several Texas Election codes<sup>349</sup>. April 30, 2009, the SoS's office certified Hart eSlate Voting System Version 6.2.1. for use in Texas elections without the required EAC certification<sup>350</sup>. The Hart InterCivic 6.2.1 was notated to have many security issues during examination as stated in Montgomery County section of this complaint on pages 87-95. The Election Code specifically assigns the SoS duties<sup>351</sup> to ensure uniform compliance but does NOT provide the SoS with "discretion" to advise any jurisdictions to ignore or refuse to comply with the Election Code<sup>352</sup>. The SoS Defendants and County Officials disregard for Tex. Elec Code in their guidance to jurisdictions violates the Separation of Powers clause of Art. 2 Sec. 1 of the Texas Constitution.

570. The Texas Constitution provides that only the Legislature can suspend laws – not the SoS whom is a member of the Executive Branch. Currently, Isabel Longoria has admitted she knew about 10,000 extra ballots having not been counted but states she was too exhausted to count them. In an email from Alan Vera, Chairman, HCRP Ballot Security Committee-President/CEO to Defendant Jose "Joe" Esparza and Keith Ingram of the SoS office the following issue are reported: The iPads were not giving confirmation of

---

<sup>349</sup> See Tex. Elec Code § 52.062, § 52.006, § 51.007, § 51.008, § 51.10, § 62.007 and § 62.009

<sup>350</sup> <https://www.sos.state.tx.us/elections/forms/sysexam/hart621cert.pdf>

<sup>351</sup> See Elec. Code § 31.003

<sup>352</sup> See Elec. Code § 52.062, § 51.010(c), § 51.007(b), 51.008 (d)

cancelled mail in ballots. Vera goes on to state, “. . . stack of mail ballots siting in every early voting location. There is apparently no record in the system that these ballots have been cancelled . . . county clerk is . . . picking up these mail ballots in an inappropriate way . . . with no apparent record in the system that THE BALLOTS HAVE BEEN CANCELLED, they are still “live” ballots that could be filled out and voted . . . This mess needs immediate attention.”

From: Alan Vera [REDACTED] >  
Sent: Sunday, October 18, 2020 8:06 AM  
To: Sonya Aston [REDACTED]; Josh Helton [REDACTED]; Joe Esparza <JEsparza@sos.texas.gov>; Keith Nielsen [REDACTED]; Keith Ingram <kingram@sos.texas.gov>; Mitch Carney [REDACTED]  
Cc: Kevin Fulton [REDACTED]; Sarah Singleton [REDACTED]; KEN RENBERT [REDACTED]; Colleen M. Vera [REDACTED]; Mano DeAyala - [REDACTED]  
Subject: RE: Chaos in BBM Processing & Chain of Custody  
Importance: High

CAUTION: This email and any files transmitted with it have originated from the ANS Office and may be confidential in nature. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. If you are not the named addressee you should not disseminate, distribute or copy this e-mail.

In follow-up to the note below from last night, I asked Republican At Deborah Carr some important follow up questions. Her answers are attached.

The most alarming element in her attached answers is the following:

In the last election she worked, when she had to cancel a mail ballot on the iPad she received a confirmation on the iPad that the mail ballot “has been successfully cancelled.” Per her attached comment, they are NOT getting that message this year.

So we have a stack of mail ballots sitting in every early voting location. There apparently is no record in the system that these ballots have been cancelled. The county clerk is apparently picking up these mail ballots in an inappropriate way. And with no apparent record in the system that THE BALLOTS HAVE BEENCANCELLED, these are still “live” ballots that could be filled out and voted.

This mess needs immediate attention.

Regards,  
Alan O. Vera  
Chairman, HCRP Ballot Security Committee  
President/CEO

### Transcription

From: Alan Vera xxxxxxxx>  
Sent: Sunday, October 18, 2020 8:06 AM  
To: Sonya Aston xxxxxxxx>; Josh Helton



App.269a

xxxxxxx>; Joe Esparza  
<JEsparza@sos.texas.gov>; Mitch Carney  
xxxxxxx  
Cc: 'kevin Fulton' xxxxxxxx; Sarah Singleton  
<xxxxxxx>; KEN xxxxxxxxxxxx; Coileen M. Vera  
xxxxx  
Subject: RE: Chaos in BBM Processing & Chain  
of Custody  
Importance: High

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

In follow-up to the note below from last night, I asked Republican AJ Deborah Carr some important follow up questions. Her answers are attached.

The most alarming element in her attached answers is the following:

In the last election she worked, when she had to cancel a mail ballot on the iPad she received a confirmation on the I Pad that the mail ballot "has been successfully cancelled," Per her attached comments, they are NOT getting that message this year.

So we have stack of mail ballots sitting in every early voting location. There apparently is no record in the system that these ballots have been cancelled. The county clerk is apparently picking up these mail ballots in an inappropriate way. And with no apparent record in the system that **THE BALLOTS HAVE**

BEENCANCELLED, these are still “live” ballots that could be filled out and voted.

This mess needs immediate attention.

Regards,

Alan D. Vera  
Chairman, HCRP Ballot Security Committee  
President/CEO

571. How many of these cancelled ballots that were not recorded correctly and still considered “live” were voted and counted? How does the SoS or the Harris County election officials or County Commissioner’s Court account for this massive security breach? The Harris County Defendants certified the general election of November 3, 2020 with numerous issues regarding the security of the voting system and possibly numerous cancelled ballots voted and counted. August 4, 2021, National File reported voter fraud in Harris County<sup>353</sup>. This information from this report was provided to the SoS office and the Texas Attorney General Ken Paxton’s office in formal investigations.

572. Audio Clips reveal:

- a. Charles Marler, FBI Special Surveillance Group, contacted Sylvia Thomas, whom shows voted in Harris County election of 2020, but has not lived in Harris County for years. Sylvia Thomas says “I’ve been away from Harris County” and confirmed that she has not voted in Harris County in recent years even though someone has been obtaining

---

<sup>353</sup> <https://nationalfile.com/watch-black-democrat-operative-blows-the-lid-off-democrat-voter-fraud-in-texas/>

App.271a

absentee ballots on her behalf. A Tomar Bishop, who obtained the absentee ballots is associated with Thomas's identity, or Gloria Palmer, the recent Sheila Jackson-Lee campaign PAC vender who oversaw Tomar Bishop. Sylvia Thomas does not recognize or know a Tomar Bishop.

- b. Charles Marler confirms with a woman in Harris County that a man who applied to "vote" in the election named Jesse Burks passed away on November 4, 2015. The woman confirms this death. The dead Burks' address matches the address of the "voter." The woman does not recognize Tomar Bishop, who obtained the absentee ballot, or Gloria Palmer, who mailed the dead man's ballot application in.
- c. Charles Marler confirms with a woman in Harris County that her mother Gloria Chambers, born in 1946, voted in the election despite dying in 2010. The daughter of the deceased voter does not know Tomar Bishop, who obtained the absentee ballot, or Gloria Palmer, who mailed the dead woman's vote in. "That's fine, because we don't know either one of those people," said the daughter of the dead voter, consenting to cooperate with Marler's investigation.
- d. There are numerous counts of voter fraud cited within this one article with affidavits from a veteran Texas Peace Officer, a retired Houston Police Officer, and Former FBI Agent Charles Marler.

**XI. FAILURES, NEGLECT  
AND OFFENSIVE VIOLATIONS**

UNDER 42 U.S.C. § 1983, 42 U.S.C. § 1985, 42 U.S.C.  
§ 1986, GUARANTEE CLAUSE, 28 U.S.C § 1367

573. Defendant Ruth R. Hughs, as Texas Secretary of State, Defendant Jose “Joe” Esparza as Texas Deputy of State and Defendant Keith Ingram as Texas Director of Elections have violated state and federal law. Defendants’ violations include failing to:

- a. Under the guise of ‘protecting the vote’, Defendants with undisputed knowledge of HAVA2002 have nefariously sought to suppress the violations of federal and state law from Plaintiffs. After multiple attempts in the form of PIA(s), county and state actors have attempted to conceal public information regarding the voting equipment and software utilized in the election process.
- b. Defendants and employees, under the directive of the SoS Office, certified the election results of the 2020 election through present elections with the knowledge that voting equipment and software had defective issues prior to the day of the election. Defendants did not issue public statements and solely relied on the “vendor” to contact affected counties with software malfunctions and perform “testing” of said software malfunctions.
- c. Defendants and employees under the directive of the SoS Office under her direction certified the election results of the November 3, 2020, election with the knowledge that voting

App.273a

equipment and software were not properly certified in accordance with Tex. Elec. code § 122.032, § 50.062, Tex. Admin. Code § 81.60 and § 81.61, which are apparent violations of Tex. Const. Art. 6, § (2) and Art. 6 § 4.

- d. Defendants and employees under the directive of the SoS Office withheld from the public that the malfunctions of the voting equipment/software were not resolved but were in fact affecting multiple counties during the 2020 and 2021 elections.
- e. Defendants and employees under the directive of the SoS Office certified the election results with the knowledge that voting equipment and software were not certified as the Voting System Test Laboratories were not accredited in accordance with HAVA and Tex. Elec. Code § 122.032, § 50.062, Tex. Admin. Code § 81.60 and § 81.61, which are apparent violations of Tex. Const. Art. 6, § 2(c) and Art. 6 § 4.
- f. Failed to seek an injunction and or restraining order from the attorney general on the voting equipment/software to prevent the use of any part of the voting system/software.
- g. Failed to revoke any voting system/software from being used in any of the counties and or the state.
- h. Defendants, acting under the color of law, certified non HAVA complaint voting system equipment, software, and modifications for the state of Texas to be used in state and

App.274a

federal elections in 2020 to present with the knowledge in violating Tex. Elec. code § 122.032, § 50.062, Tex. Admin. Code § 81.60 and § 81.61, which are apparent violations of Tex. Const. Art. 6, § 2(c) and Art. 6 § 4.

- i. Defendants and employees under the directive of the SoS Office withheld from the public that the malfunctions of the ES&S voting equipment/software were not resolved but was in fact affecting multiply counties during the 2020 election.
- j. Defendants and employees under the directive of the SoS Office to violate Tex. Elec Code § 52.062 in manner that Defendants advised to counties to ignore election laws, violating Art. 1 § 28 of the Texas Constitution.
- k. SoS Defendants violated Tex. Const. Art. 6 § 4; by “providing for numbering of tickets” specifically reserved for the Legislative Branch.
- l. SoS Defendants impeded CO’s ability to “detect and punish fraud and preserve the purity of the ballot box” as randomized ballot numbers prevented recording, violating, and tracking the official ballot serial number ranges in possession of, personally distributed, and retained at polling locations violating Tex. Const. Art. 6 § 4.
- m. Defendants initiated confusion and uncertainty to the COs and caused a chain reaction of violations of several ballot numbering statues that are not only illegal but punishable criminally in the election code. Tex. Elec.

App.275a

Code § 51.010(c), 51.007(b), 51.008(d), and 13 TAC § 7.125(a)(10), and Tex. Penal Code § 37.10(3)

- n. By Defendants' own admission via the State of Texas' Secretary of State website regarding education of the HAVA 2002; knowingly certified voting system equipment, software, and modification without a valid VSTL accreditation via the EAC.
- o. Defendants' duplicitous activity and arrangement seem to only exist for a singular self-serving purpose of covering misdeeds and offenses.
- p. Defendant John Scott, as Texas Secretary of State, Jose "Joe" Esparza as Texas Deputy of State and Keith Ingram as Texas Director of Elections has violated state and federal law. Defendants' violations include failing to:
  - q. Under the guise of 'protecting the vote', Defendants with undisputed knowledge of HAVA have nefariously sought to suppress the violations of federal and state law from Plaintiffs. After multiple attempts in the form of PIA(s), the county and state actors have attempted to conceal public information regarding the voting equipment and software utilized in the election process.
- r. Defendants and employees under the directive of The SoS Office certified the 2021-2022 election results with the knowledge that voting equipment and software were not certified as the Voting System Test Laboratories were not accredited in accord-

App.276a

ance with HAVA and Tex. Elec. Code § 122.032, § 50.062, Tex. Admin. Code § 81.60 and § 81.61, which are apparent violations of Tex. Const. Art. 6, § 2 and Art. 6 § 4 and federal 52 U.S.C. § 20971.

- s. Defendants were knowingly remiss in their duties acting under the color of law and are in violation of Texas statute in not acknowledging the expiration of certifications of accreditation of VSTLs or the lack of legal signature per HAVA thereby allowing voting machines to be used in statewide elections since 2020 violating Tex. Elec. code § 122.032, § 50.062, Tex. Admin. Code § 81.60 and § 81.61, which are apparent violations of Tex. Const. Art. 6, § 2 and Art. 6 § 4 and federal 52 U.S.C. 20971.
- t. Defendants acting under the color of law certified non HAVA complaint voting system equipment, software, and modifications for the state of Texas to be used in state and federal elections in 2021 and 2022 violating Tex. Elec. Code § 122.032, § 50.062, Tex. Admin. Code § 81.60 and § 81.61, which are apparent violations of Tex. Const. Art. 6, § 2 and Art. 6 § 4 and federal 52 U.S.C. 20971.
- u. Defendants and employees under the directive of The SoS Office withheld from the public that the malfunctions of the ES&S voting equipment/software were not resolved but were in fact affecting multiple counties during the election.



App.277a

- v. Defendants and employees under the directive of The SoS Office to violate Tex. Elec Code § 52.062 in manner that Defendants advised to counties to ignore election laws, violating Art. 1 § 28 of the Texas Constitution.
- w. Defendants violated Tex. Const. Art. 6 § 4; by “providing for numbering of tickets” specifically reserved for the Legislative Branch.
- x. Defendants impeded CO’s ability to “detect and punish fraud and preserve the purity of the ballot box” as randomized ballot numbers prevented recording, violating, and tracking the official ballot serial number ranges in possession of, personally distributed, and retained at polling locations violating Tex. Const. Art. 6 § 4.
- y. Defendants initiated confusion and uncertainty to the COs and caused a chain reaction of violations of several ballot numbering statues that are not only illegal but punishable criminally in the election code. Tex. Elec. Code § 51.010(c), 51.007(b), 51.008(d), and 13 TAC § 7.125(a)(10), and Tex. Penal Code § 37.10(3)
- z. By Defendants’ own admission via the State of Texas’ Secretary of State website regarding education of the HAVA; knowingly certified voting system equipment, software, and modification without a valid VSTL accreditation via the EAC.
- aa. Failed to seek an injunction and or restraining order from the attorney general on the

App.278a

voting equipment/software to prevent the use of any part of the voting system/software.

- bb. Defendants' duplicitous activity and arrangement seem to only exist for a singular self-serving purpose of covering misdeeds and offenses.

574. Defendant County Officials, Jacquelyn Callanen, Nelson Wolff, Bobbie Koepf, Cynthia Jaqua, Frank Phillips, Jennifer Doinoff, Ron Massingill, Michele Carew, Pat Deen, Cricket Miller, George Conley, Craig Peacock, Larry Walden, Steve Dugan, Heider Garcia, Roy Charles Brooks, Devan Allen, Gary Fickes, J.D. Johnson, Dana Debeauvoir, Rebecca Guerrero, Bill Gravell, Christopher Davis, Terry Cook, Cynthia Long, Valerie Covey, Russ Boles, Suzie Harvey, Robert C. Walker, Charlie Riley, James Noack, James Metts, R. Jack Cagle, Andrew Steven Brown, Sarah Eckhardt, Rebecca Clay-Flores, Justin Rodriguez, Marialyn Barnard, Tommy Calvert, Andy Eads, Ryan Williams, Ron Marchant, Bobbie J. Mitchell, Dianne Edmondson, Lina Hidalgo, Rodney Ellis, Adrian Garcia, Tom Ramsey, Isabel Longoria, Ruben Becerra, Debbie Ingalsbe, Mark Jones, Lon Shell, Walt Smith, B. Glen Whitley, Robert Walker, Suzie Harvey has violated state and federal law. Defendants' violations include failing to:

- a. Operating systems lacking proper certifications.
- b. Unmonitored network communications.
- c. Restricting access to public information.
- d. Concealing and refusing to release voting system software versions.

App.279a

- e. CO once informed of any problematic issues with voting systems/software proceeded with elections without informing the public nor issued any public statement as the malfunction continued to affect casting of ballots during the election.
- f. CO Defendants under the advice of SoS violated Tex. Elec Code § 52.062 requiring numbering ballots producing violation Art. 1 § 28.
- g. CO Defendants under the advice of SoS Defendants violated Tex. Const. Art. 6 § 4; by providing for numbering of tickets specifically reserved for the Legislative Branch.
- h. CO Defendants impeded election workers and staff from “detect and punish fraud and preserve the purity of the ballot box” as randomized ballot numbers prevented recording, violating, and tracking the official ballot serial number ranges in possession of, personally distributed, and retained at polling locations violating Tex. Const. Art. 6 § 4.
- i. CO Defendants set off a chain reaction of violations of several ballot numbering statues that are not only illegal but punishable criminally in the election code. Tex. Elec. Code § 51.010(c), 51.007(b), 51.008(d), and 13 TAC § 7.125(a)(10), and Tex. Penal Code § 37.10(3)
- j. CO Defendants certified not only the November 3, 2020, election results but every election since after receiving evidence from

Plaintiffs that cast doubt on integrity of the ballot.

- k. CO Defendants were knowingly remiss in their duties acting under the color of law and are in violation of Texas statute in not acknowledging the expiration of certification of accreditations of VSTLs or the lack of legal signature per HAVA thereby allowing voting machines to be used in county elections since 2020. What is confirmed is that Pro V& V and SLI Compliance were Not Accredited VSTL. (*Emphasis added*)
- l. Under the guise of 'protecting the vote', CO Defendants with undisputed knowledge of HAVA have nefariously sought to suppress the violations of federal and state law from Plaintiffs. After multiply attempts in the form of PIA(s), the county actors have attempted to conceal public information regarding the voting equipment and software utilized in the election process.
- m. CO Defendants and employees under the directive of The SoS Office withheld from the public that the malfunctions of the voting equipment/software were not resolved but was in fact affecting multiply counties during the elections.
- n. CO Defendants acting under the color of law administered elections with non HAVA complaint voting system equipment, software, and modifications for the state of Texas to be used in state and federal elections in 2020 through 2022 violating Tex. Elec. Code

§ 122.032, § 50.062, Tex. Admin. Code § 81.60 and § 81.61, which are apparent violations of Tex. Const. Art. 6, § 2 and Art. 6 § 4 and federal 52 U.S.C. 20971.

- o. By Defendants' own admission via the State of Texas' Secretary of State website regarding education of the HAVA; knowingly certified voting system equipment, software, and modification without a valid VSTL accreditation via the EAC.
- p. Defendants' duplicitous activity and arrangement seem to only exist for a singular self-serving purpose of covering misdeeds and offenses.

## **XII. PLAINTIFF(S) FACE DIFFICULT CIRCUMSTANCES**

575. Plaintiff(s) are entitled to free and fair elections of our representatives. This is affirmed in the U.S. Constitution, Article 1. The government provides the means by which we exercise that Right. Plaintiffs do not have an alternate means of ensuring our election process. Therefore, we are burdened by the system put in place through our elected officials. In *Rice v. Cayetano*, the Court ruled the Fifteenth Amendment, "... reaffirms the equality of races at the most basic level of the democratic process, the exercise of the voting franchise." The Court did not specify the 15th Amendment applies only to a protected class, but rather it applies to everyone.<sup>354</sup>

---

<sup>354</sup> <http://cdn.loc.gov/service/11/usrep/usrep528/usrep528495/usrep528495.pdf>

576. As part of their sworn duty, it is imperative our elected officials guarantee the election process is protected from any form of fraud or profiteering as this could lead to discrimination of voters regardless of classification. Additionally, when elected officials fail to provide the level of protection necessary to secure the election franchise, it is the Right and Duty of the American people to correct this deficiency. The Court cannot deny this Right to the people when the injury is widespread. It is infeasible to imagine an entire population advancing on the Court for relief.

577. Failure to perform their sworn duty has allowed discrimination to occur across the equality of races in the State of Texas. This violates the Right to Vote Clause of the Fifteenth Amendment. Furthermore, by failing to protect against private interference (i.e.: vendor voting systems, Scytl, et al) of the election process by not adhering to Federal election/ voting system certification standards (HAVA 2002), and the most basic cyber security defense and hardening frameworks, Defendants failed to comply with 18 USC Section 245(1)(a). Therefore, Defendants do not comply with the Enforcement clause of the Fifteenth Amendment.<sup>355</sup>

578. Each day Plaintiff(s) has suffered irreparable harm living under a government that no longer represents we the people and deprives us, the Plaintiffs and all voters of the state of Texas, of the Republic that the Constitution of the State of Texas and United States Constitution outline as protection from a

---

<sup>355</sup> [https://uscode.house.gov/view.xhtml?req=\(title:18%20section:245%20edition:prelim\)%20OR%20\(granuleid:USC-prelim-title18-section245\)&f=treesort&num=0&edition=prelim](https://uscode.house.gov/view.xhtml?req=(title:18%20section:245%20edition:prelim)%20OR%20(granuleid:USC-prelim-title18-section245)&f=treesort&num=0&edition=prelim)

tyrannical government. The general public benefits from the remedy against the constitutional infringements where any citizen can bring a case before the court as long as it impacts the public interest, and benefits the general public, not just the Plaintiff. *Assoc. Indus. of New York v. Ickes*, 134 F.2d 694, 704 (2d Cir. 1943).

579. It is our constitutional duty to invoke our authority as free persons to petition and address this court regardless of the outcome of this complaint, it serves as notice to all acting officials and non-officials within our government that we demand justice for any and all criminal behavior and fraud. 'When a State exercises power wholly within the domain of state interest, it is insulated from federal judicial review. But such insulation is not carried over when state power is used as an instrument for circumventing a federally protected right.' *Baker v. Carr* 369 US 186, 208 (1962) citing 364 U.S. at 347, 81 S.Ct. at 130.57.

580. *Sherar v. Cullen*, 481 F 946 (1973), "There can be no sanction or penalty imposed upon one because of this exercise of constitutional rights." "No state legislator or executive or judicial officer can war against the Constitution without violating his undertaking to support it." *Cooper v. Aaron*, 358 U.S. 1, 78 S. Ct. 1401 (1958). Although defendants may assert immunity against these claims, the constitution theory is that we the people are the sovereigns, the state and federal officials only our agents. As Judge P. Higginbotham dissented, "the 11th Amendment does not bar these claims under the 14th Amendment . . . The role of the Court in protecting the most vital right of a democratic government: the right to vote; should not be denying the right to vote." *Texas Alliance for*

*Retired Americans; Sylvia Bruni; DSCC; DCCC v. Scott Secretary of State 20-40643 March 16, 2022. United States Court of Appeals, Fifth Circuit.*

581. The immediate injury continues as Texas officials continue to allow us to vote in another election conducted on uncertified and networked machines is a violation of our 1st 14th and 15th amendment rights and in violation of Tex. Elec. Code § 52.062, § 122.01(3)(4), § 129.054(a) (b)(c), § 122.031(c) and United State Code 52 U.S.C. § 20511 (2)(a)(b), which is criminal. The Plaintiff(s) stand to lose more of our freedoms as each day passes without resolution.

582. However, knowing what we, the Plaintiffs, now recognize as the illegality of the certifications. Did the Plaintiffs cast an illegal ballot unknowingly at the time? Since 2020, we have been Forced to continue this illegal practice by our own government due to their reckless disregard for the law and constitution. Our only remedy thus far has been:

583. Notify the proper authorities in our respective counties and our state government in pursuant with Tex. Elec. Code § 273 in which the Plaintiffs have made many attempts for over a year.

584. Not to participate in unlawful elections and thereby denied our right to vote as our last alternative.

585. Seek legal means via the Peoples' court.

586. Which brings us here today seeking redress of our 1st, 4th, 14th, and 15th amendment rights under 42 U.S.C. § 1983 "taking on the mantel of the sovereign,' guarding for all of us the individual liberties enunciated in the Constitution. Section 1983 represents a balancing feature in our governmental



structure whereby individual citizens are encouraged to police those who are charged with policing us all. Thus, it is of special import that suits brought under this statute be resolved by a determination of the truth rather than by a determination that the truth shall remain hidden." *Frankenhauser v. Rizzo*, 59 F.R.D. 339 (E.D. Pa. 1973).

587. We, the people, have the Right to elect our representatives. The government provides the means by which we exercise that Right. The Framers couldn't foresee the day computerized touch screens or FROG ciphers would be used any more than they could an AR-15. But we the people have the Right to ensure elections are free and fair. It's not just the Right to CAST the vote. It is the Right to ELECT our government. The entire process must be guaranteed. Anything that circumvents that process is inherently infringing upon the Right we have to pursue life, liberty, and happiness.

588. We have a Right to defend ourselves and others from attack. We have the same Right to defend our election process when it is subject to profiteering by actors who would seek to abolish our sovereignty in favor of a dictatorship. We the people carry this Right, and every Right, in the same manner we would a physical firearm. Every single Right we enjoy, as affirmed in the Constitution, is a weapon against tyranny. A violation of one Right, is a violation of all Rights. We exercise our free will and choose, through our Rights, to remain free. As Justice Oliver Wendell Holmes put it: "We do not inquire what the legislature meant; we ask only what the statute means."

### XIII. COUNTS

**COUNT I - Violation of Procedural Due Process  
UNDER 42 U.S.C. § 1983, 28 U.S.C. § 1331dp  
(1st, 14th, and 15th Amendments)**

(Seeking declaratory and injunctive relief against  
All Defendants)

589. Plaintiffs incorporate the foregoing paragraphs as if set forth in full herein.

590. In order establish a claim under section 1983 of the Civil Rights Act, a plaintiff must prove a Defendant: (a) acted under the color of state law; (b) proximately causing; (c) the Plaintiff to be deprived of a federally protected right. *42 U.S.C. § 1983*.

591. For this matter, Defendants violated the federally protected rights of voting.

592. In the instant case, Defendants unquestionably acted under the color of state and federal law.

593. Each Individual Defendant is an appointed official with the authority of duties pursuant to Texas Statutes for the State of Texas.

594. Under the First Amendment to the Constitution, no abridging the freedom of speech.

595. The Fourteenth Amendment applies the protections of the First and Fifteenth Amendment to state actors. U.S. Const. Ann., Amendment XIV.

596. Under the Fifteenth Amendment to the Constitution, no citizen of the United States the right to vote shall not be denied or abridged by any state on account of servitude by those in power without due process of law. U.S. Const. Ann., Amendment XV.

597. Plaintiffs have constitutionally protected interests in the benefits that come from the right to vote and not being subject to the illegal voting systems/equipment, software, and modifications, including the ability to pursue our First Amendment right to legal elections without being subjected to casting an illegal vote that violates federal and state laws.

598. Defendants' knowingly certified voting system/equipment, software and modifications unlawfully deprives Plaintiffs of these and other constitutionally protected interests without due process of law. Such deprivation occurred after Defendants had open communications with voting vendors and the EAC in which Defendants did not disclose to the public and gave no notice or meaningful opportunity for open public discussion regarding defects of voting equipment /software to the Plaintiffs prior to certifications. Such deprivation was arbitrary, capricious, based on ignorance without inquiry into facts, and in violation of the Texas and Federal laws and other applicable laws. Such deprivation violates the First, Fourteenth, and Fifteenth Amendments of the Unites States Constitution thereby depriving Plaintiffs civil rights in regard to casting a "legal" vote.

599. Despite Defendant's knowledge of voting systems noncompliance with state and federal law, Defendants intend to continue to utilize these non-compliance systems in future elections.

600. Plaintiffs were harmed and continue to be irreparably harmed by these unlawful acts, including by suffering forced contracts with representatives through deceptive practices and fraudulent certifications. 52 USC 20105 and 52 USC 20510.

**COUNT II - Violation of Substantive Due Process  
UNDER 42 U.S.C. § 1983, 52 U.S.C 20105, 52  
U.S.C. 20510 (Fourteenth Amendment, Equal  
Rights)**

(Seeking declaratory and injunctive relief against  
All Defendants)

601. Plaintiffs incorporate the foregoing paragraphs as if set forth in full herein.

602. In order establish a claim under section 1983 of the Civil Rights Act, a plaintiff must prove a Defendant: (a) acted under the color of state law; (b) proximately causing; (c) the Plaintiff to be deprived of a federally protected right. 42 U.S.C. § 1983.

603. For this matter, Defendants violated the federally protected rights of voting. *52 U.S.C. 20105, 52 U.S.C. 20510.*

604. In the instant case, Defendants unquestionably acted under the color of state law.

605. Each Individual Defendant is an appointed official with the authority of duties pursuant to Texas Statutes for the State of Texas.

606. Under the Fourteenth Amendment of the Constitution, and as established by state law, including the state created Accardi doctrine, Plaintiffs have a fundamental right to cast a ballot and vote in a legal and fair election.

607. Plaintiffs were harmed and continue to be irreparably harmed by these unlawful acts, including by suffering forced contract with representatives through deceptive practices and fraudulent certifications. *TEX. ELEC. CODE § 276.013(a)(4)*

**COUNT III – Deprivation of Civil Rights UNDER  
42 U.S.C § 1983vp, 28 U.S.C. 1985 (TX Const.  
Art. I, § 13 and Art. I, § 19)**

(Seeking declaratory and injunctive relief against  
All Defendants)

608. Plaintiffs incorporate the foregoing paragraphs as if set forth in full herein.

609. Article 1, § 13 of the Texas Constitution provides, “All courts shall be open, and every person, for an injury done him, in his land, goods, person, or reputation, shall have remedy by due course of law.”

610. Article 1, § 19 of the Texas Constitution affords the people of Texas with the right to be free from violations of the procedural due process rights, and no person may be deprived of life, liberty, or property without due process of law.

611. Plaintiffs have constitutionally protected interests in the benefits that come from the right to vote and not being subject to the illegal voting systems/equipment, software, and modifications, including the ability to pursue our First Amendment right to legal elections without being subjected to casting illegal votes in violation of both state and federal laws.

612. Defendants’ knowingly certified voting system /equipment, software and modifications unlawfully deprives Plaintiffs of these and other constitutionally protected interests without due process of law. Such deprivation occurred after Defendants had open communications with voting vendors and the EAC in which Defendants did not disclose to the public and gave no notice or meaningful opportunity for open

public discussion regarding defects of voting equipment /software to the Plaintiffs prior to certifications. Such deprivation was arbitrary, capricious, based on ignorance without inquiry into facts, and in violation of the Texas and Federal laws and other applicable laws. Such deprivation violates Article 1, § 13 and Article 1, § 19 of the Texas Constitution thereby depriving Plaintiffs civil rights regarding casting a “legal” vote. *TEX. PEN. CODE § 37.03, § 37.10.*

613. Plaintiffs were harmed and continue to be irreparably harmed by these unlawful acts, including by suffering forced contracts with representatives through deceptive practices and fraudulent certifications.

**COUNT IV – Deprivation of Constitutional Rights UNDER 28 U.S.C. 1331vc (TX Const. Art. I, § 13 and TX Const. Art. I, § 19)**

(Seeking declaratory and injunctive relief against All Defendants)

614. Plaintiffs incorporate the foregoing paragraphs as if set forth in full herein.

615. Article 1, § 13 of the Texas Constitution provides, “All courts shall be open, and every person, for an injury done him in his land, goods, person, or reputation, shall have remedy by due course of law.”

616. Article 1, § 19 of the Texas Constitution affords the people of Texas with the right to be free from violations of the substantive due process rights, and no person may be deprived of life, liberty, or property without due process of law.

617. Under Article 1, § 19 of the Texas Constitution, and as established by state law including the state created Accardi doctrine, Plaintiffs have a fundamental right to cast a ballots and vote in a legal and fair election.

618. Plaintiffs were harmed and continue to be irreparably harmed by these unlawful acts, including by suffering forced contracts with representatives through deceptive practices and fraudulent certifications. *TEX. PEN. CODE § 39.03(2)*.

**COUNT V – Voting Rights Violation UNDER 52 U.S.C § 20510, 52 U.S.C. § 10101, 28 U.S.C. 13943 (First and Fourteenth Amendment)**

(Seeking declaratory and injunctive relief against All Defendants)

619. Plaintiffs incorporate the foregoing paragraphs as if set forth in full herein.

620. In order establish a claim under section 20510 of Title 52-Voting and Elections, a plaintiff must prove a Defendant: (a) acted under the color of state law; (b) proximately causing; (c) the Plaintiff to be deprived of a federally protected right. *42 U.S.C. § 1983*.

621. In the instant case, Defendants unquestionably acted under the color of state and federal law.

622. Each Individual Defendant is an appointed official with the authority of duties pursuant to Texas Statues for the State of Texas.

623 Under the First and Fourteenth Amendment to the Constitution, and as established by state law including the state created Accardi doctrine, Plaintiffs

have a fundamental right to cast a ballot and vote in a legal and fair election.

624. Plaintiffs were harmed and continue to be irreparably harmed by these unlawful acts, including by suffering forced contract with representatives through deceptive practices and fraudulent certifications. *TEX. PEN. CODE § 39.02.*

**COUNT VI – DECLARATORY JUDGMENT  
UNDER 28 U.S.C. § 2201**

(Seeking declaratory and injunctive relief against all Defendants)

625. Plaintiffs incorporate the foregoing paragraphs as set forth in full herein.

626. Defendants' conduct has and will continue to violate the rights of citizens of Texas, as set forth above.

627. The Court has the authority pursuant to 28 U.S.C. § 2201 to issue an Order enjoining the State from conducting an election in which the votes are not accurately or securely tabulated.

628. If the State of Texas proceeds with the forthcoming election as described above, it will violate the rights of Texans by conducting an unsecure, vulnerable electronic voting systems which is susceptible to manipulation and intrusion.

629. If the State of Texas proceeds with the forthcoming election as described above, it will violate the rights of Texans by conducting an election on illegally certified voting systems in violation of both the State of Texas and Federal election laws.



630. The Court should issue an Order enjoining the State from using any electronic voting system and respective devices to include but not limited to poll pads, tabulators, printers, etc.

#### **XIV. PRAYER FOR RELIEF**

WHEREFORE, "For there is no authority except from God, and the authorities that exist are appointed by God." *Romans 13:1* (NKJV). Plaintiffs request that the Court grant the following relief:

- a. Assume jurisdiction of this action in the interest of justice.
- b. Vacate and set aside all uncertified and illegal voting systems/equipment, software, and modifications and implement a precinct level hand marked paper ballot and hand counting system as permissible by Tex. Elec. Code Chp 65.
- c. Enter a preliminary and permanent injunction prohibiting Defendants from requiring or permitting voters to have votes cast or tabulated using any electronic voting systems.
- d. Enter a preliminary and permanent injunction prohibiting Defendants from destruction/deletion of any and all election records created under Title 8 of the Tex. Elec Code to include all paper ballots created by voting systems, mail in ballots, tabulation tapes, USB final counts from precincts and all other election records not specifically stated.
- e. Declare that the Defendants' certifications of all voting system/equipment, software, and

modifications are void and without legal force or effect;

- f. Declare that the institution of the certification policies are arbitrary, capricious, and based on negligence and disregard in accordance with law, and without observance of required procedure, Accardi doctrine; Declare that the certifications and the actions taken by Defendants are in violation of the Constitution and contrary to the laws of the United States and the State of Texas;
- g. Temporarily restrain, as well as preliminarily and permanently enjoin Defendants, their agents, servants, employees, attorneys, and all persons in active concert or participation with any of them, from implementing and/or enforcing the certifications of all voting systems/equipment, software and modifications that is not in compliance with the applicable law, and

Grant such other and further relief as may be just, equitable, and proper including without limitation, an award of any attorneys' fees and costs to Plaintiffs.

Respectfully submitted this 3rd day of October, 2022.

**Pro se Counsel for Plaintiffs**

/s/ Kyle Strongin  
253 Martin Dr.  
Granbury, TX 76049  
979.492.0023  
kstrongin04@gmail.com>  
Hood County

App.295a

/s/ Lindsey Gremont  
4502 Deepwoods Drive  
Austin, TX 78731  
512.879.7069  
linny2777@protonmail.com  
Travis County

/s/ Christine Koepke  
19509 Encino Crown  
San Antonio, Texas 78259  
210.845.9448  
stina4kids@protonmail.com  
Bexar County

/s/ Travis Wayne Eubanks  
1823 Lookout Forest  
San Antonio, TX 78260  
505.506.1050  
travis.eubanks@gmail.com  
Bexar County

/s/ Amanda Eubanks  
1823 Lookout Forest  
San Antonio, TX 78260  
505.818.8824  
amanda.eubanks710@gmail.com  
Bexar County

/s/ Kristen Plaisance  
22355 Log Orchard Lane  
Porter, TX 77365  
713.724.0474  
robbiekristenp@gmail.com  
Montgomery County

/s/ Karen Rene 'Towell  
1015 Teresa Court  
Granbury, TX 76048

App.296a

817.300.0827  
renetowell6165@gmail.com  
Hood County

/s/ Jason S. Buster  
2003 Mulberry Tree  
San Antonio, TX 78251  
210.265.7914  
jason.s.buster@gmail.com  
Bexar County

/s/ Alexandra Campo  
PO Box 40  
Weir, Texas 78674  
512.790.8774  
acampo0312@gmail.com  
Williamson County

/s/ James L Clark  
1750 Loop 165  
Dripping Springs, TX 78620  
512.808.6734  
rccpd715@protonmail.com  
Hays County

/s/ Jose Christine Silvester  
8055 Garden Oaks Drive  
San Antonio TX, 78266  
830.515.3212  
lousilvester@msn.com  
Comal County

/s/ Tommie Dickinson  
1231 W Goodwin  
Pleasanton, TX 78064  
830.570.1366  
tommie.dickinson@yahoo.com  
Atascosa County

App.297a

/s/ Robert James Brooks Jr

3414 Zebecca Creek Drive  
Austin, TX 78732  
512.550.8688  
brooks@mindsetatx.com  
Travis County

/s/ Alana S. Phillips

3461 Highway 8 E,  
Mena, AR 71953  
940.437.0049  
Phillipsar@yahoo.com  
Denton County

/s/ Jennifer B. Edwards

422 WW Lane  
Millsap, TX 76066  
940.682.5214  
Jenn@jennz.com  
Parker County

/s/ Aubrey Brandon Rhymes

3522 Turkey Pen Branch Road  
Maryville, TN 37083  
469.714.1157  
brandon.rhymes@protonmail.com  
Collin County

/s/ Lester Rand

515 Oakwood Drive  
Allen, TX 75013  
214.437.6780  
lrando1tv@gmail.com  
Collin County

/s/ Amber Cloy

421 Palisades Trail  
Keller, TX 76248

App.298a

817.522.2732  
Amberb2222@yahoo.com  
Tarrant County

/s/ Sheron Jennifer Lipper  
11700 Preston Road, Ste.660-275  
Dallas, TX 75230  
214.679.5760  
Theburgundyacademy@gmail.com  
Dallas County

/s/ Jennifer Williams  
1613 Sandle Wood Drive  
Weatherford, TX 76087  
817.565.9137  
Jennifer.Williams2236@yahoo.com  
Parker County

/s/ Sonja Zielsdorf  
400 County Road 369  
Taylor, TX 76574  
512.667.1746  
Sonjaz22@yahoo.com  
Williamson County

/s/ Juan Carlos Arias  
9415 Pagewood Lane  
Houston, TX 77063  
713.204.0981  
Altcode1969@proton.me  
Harris County

/s/ Lynn Christine Davenport  
9627 Windy Hill Road  
Dallas, TX 75238  
214-673-4018  
Ldaven@me.com  
Dallas County

App.299a

/s/ Beverly Foley  
8 Oak Village Ct  
Trophy Club TX 76266  
214.415.7154  
Beverlyfoley@gmail.com  
Denton County

**PLAINTIFFS' BRIEF IN SUPPORT OF  
MOTION TO SUPPLEMENT SECOND  
AMENDED COMPLAINT  
(OCTOBER 3, 2022)**

---

IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS  
FORT WORTH DIVISION

---

STRONGIN ET AL.,

*Plaintiff(s),*

v.

SCOTT, ET AL.,

*Defendant(s).*

---

No. 4:22-cv-00576-BJ

Before: Hon. Mark T. PITTMAN,  
United States District Judge.

---

**TO THE HONORABLE JUDGES JEFFERY  
CURETON AND MARK PITTMAN:**

The Plaintiffs file this Brief in support of Supplemental and respectfully show unto the Court as follows:

[TOC and TOA, Omitted]



**I. Adoption of Second Amended Complaint**

1. Plaintiffs bring this Supplemental cause of action under original jurisdiction pleaded in Second Amended Complaint. Plaintiffs additional cause of action 52:552pa, Right to Privacy.

2. Plaintiffs bring this Supplemental with the adaptation of standing under the Second Amended Complaint.

3. Plaintiffs bring this Supplemental to the Second Amended Complaint with the additional federal questions.

- a. What is the Constitutional remedy for the usurpation of the Texas Legislature as the underlying governmental authority for forcing Plaintiffs to participate in a “federalized” election? Art. 1 Sec. 4 cl. 1.
- b. The Department of Homeland Security has installed “monitoring” sensors on state and local voting systems/rolls; does this impede on Plaintiffs’ private and personal information? Privacy Act of 1974
- c. If Art. 1 Sec. 4 cl. 1 of the United States Constitution grant sole authority of elections to the Texas Legislature, does the Secretary of State and local county officials have the authority to “federalize” Texas elections by contract with the Department of Homeland Security via Center for Internet Security and third-party partners after the U.S. Congress rejected H.R. 1 (For the People Act of 2021)?

## II. Federalization of Texas Elections

### 2017 The Pilot Program

1. In January 2017, Department of Homeland Security (DHS) designated election systems as critical infrastructure.<sup>1 2</sup>

2. In 2017, the Election Infrastructure Subsector Government Coordinating Council (EIS-GCC) was established and consisted of representatives from Department of Homeland Security (DHS), the U.S. Election Assistance Commission (EAC), the National Association of Secretaries of State (NASS), and the National Association of State Election Directors (NASED). Texas participated in the pilot program which began in March of 2018.<sup>3</sup>

“The EIS-GCC and MS-ISAC first began their formal collaboration in October 2017 with a pilot that included representatives from seven states (Colorado, Indiana, New Jersey, Texas, Utah, Virginia, Washington) and two local election organizations (Travis County, Texas; Weber County, Utah).”<sup>4</sup>

“The DHS Election Task Force (ETF), EAC, and NASED worked alongside the MS-ISAC

---

<sup>1</sup> USA Patriot Act of 2001 (42 U.S.C. 519c(e))

<sup>2</sup> [https://www.cisa.gov/sites/default/files/publications/19\\_0531\\_cisa\\_election-security-resources-guide-may-2019.pdf](https://www.cisa.gov/sites/default/files/publications/19_0531_cisa_election-security-resources-guide-may-2019.pdf)  
pg. 2

<sup>3</sup> <https://www.cisecurity.org/insights/white-papers/2018-year-in-review> pg. 2

<sup>4</sup> *Id.* pg. 3

to develop a program that could serve as an ISAC for the Election Infrastructure Sub-sector. The MS-ISAC quickly formed an elections team to leverage their existing suite of products and services, as well as their relationships with state and local government IT staff, to address the vision of the pilot participants.”<sup>5</sup>

3. In October, the newly formed EIS-GCC determined that an Information Sharing and Analysis Center (ISAC), focusing on election infrastructure, was needed and recommended its creation.<sup>6</sup>

4. The next step was implementing a pilot program to develop a framework for the new ISAC. The EIS-GCC turned to CIS and MS-ISAC® (the Multi-State Information Sharing & Analysis Center®) to support these efforts, as the MS-ISAC was designated by DHS as their key cybersecurity resource for all U.S. State, Local, Tribal, and Territorial (SLTT) governments.<sup>7</sup>

5. The Pilot program ran from October 2017-February 2018.<sup>8</sup>

6. In 2018, EIS-GCC held a vote on February 15 to formally launch the ISAC (Information Sharing and

---

<sup>5</sup> *Id.*

<sup>6</sup> *Id.* pg. 2

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

Analysis Center) Elections Infrastructure ISAC which began on March 7, 2018.<sup>9</sup>

### **2018 In Review**

7. In early 2018, former Secretary Kirstjen Nielsen established a Countering Foreign Influence Task Force (CFITF) within DHS. The “Task Force” is currently part of CISA.

“During the 2018 midterm Election cycle, DHS established the Election Task Force (ETF) and the Countering Foreign Influence Task Force (CFITF) to coordinate federal support to the election community. ETF and CFITF have now been institutionalized as the Election Security Initiative (ESI) within CISA. CISA works in coordination with various federal partners, such as DHS’ Office of Intelligence and Analysis (I&A) and the Federal Bureau of Investigation (FBI), as well as non-federal election stakeholders.”<sup>10</sup>

8. The CFITF works in close coordination with the FBI Foreign Influence Task Force, the government lead on foreign interference. CFITF is charged with helping CISA’s leadership by “identifying the policy options available to government and working with social media companies, academia, international

---

<sup>9</sup> *Id.* pg. 3

<sup>10</sup> See pg. 4 [https://www.cisa.gov/sites/default/files/publications/ESI%20Strategic%20Plan FINAL%202.7.20%20508.pdf](https://www.cisa.gov/sites/default/files/publications/ESI%20Strategic%20Plan%20FINAL%202.7.20%20508.pdf)

partners”. Both the CFITF and the FBI Foreign Influence Task Force work closely with social media.<sup>11</sup>

9. The EI-ISAC has continued to evolve since its creation and offered DHS (via CISA and CIS Security) products and services including the following:<sup>12</sup>

- a. Access to a 24/7/365 SOC (Security Operations Center)
- b. Cyber incident response and remediation
- c. Threat and vulnerability monitoring
- d. Election-specific threat intelligence
- e. Training sessions and webinars
- f. A NCSAR (Nation Cyber Situational Awareness Room)
- g. Security best practice recommendations and tools
- h. Access to a Members-Only Discussion board
- i. Malicious code Analysis Platform (MCAP)
- j. Digital forensics and log analysis

“The EI-ISAC has positioned itself at the forefront of our nation’s effort to secure our election systems, and will continue to operate in partnership with members and stakeholders nationwide to ensure the integrity of elections in the United States.”

10. The Pilot program called for the deployment of “Albert,” the MS-ISAC’s Intrusion Detection System

---

<sup>11</sup> *Id.* pg. 16

<sup>12</sup> *See* pg. 2 <https://www.cisecurity.org/ms-isac>

(IDS), on every pilot state's elections network to the voter registration database if it was not covered by an existing Albert sensor. DHS acquired the funding and approval, deciphering whether each state was covered, working with the states to execute agreements, identifying and educating stakeholders from various departments and vendors, ordering and configuring the hardware along with assisting the pilot members with installation.<sup>13</sup>

11. On February 15 the EIS-GCC formal created the EI-ISAC, operated by CIS alongside the MS-ISAC. "The following weeks were filled with collaboration across CIS to create the permanent infrastructure necessary to formalize the EI-ISAC's efforts. This infrastructure included legal agreements, a webpage and a way for members to join, staff training, and further collaboration with the partners and leadership that had supported them thus far. The Elections Infrastructure Information Sharing & Analysis Center was formally launched on March 7, 2018."<sup>14</sup>

---

<sup>13</sup> *Id.* pg. 3

<sup>14</sup> *Id.*



provide incident response and forensic services.

- Cyber Intelligence Team to provide forward-leaning analysis, written products, and presentations.
- Engineering Team to provide sensor deployment and technical assistance.
- Stakeholder Engagement Team to provide member support and engagement.



The EI-ISAC was conceived as a means of leveraging the many capabilities and the infatuates of the MS-ISAC. The integration if the two continued after the EI-ISAC's formal launch in March. Both the MS-ISAC and EI-ISAC benefit by operating under the auspices if CIS. This allows them to work together to educate and protects SLTT government from the myriad cyber threats that are aimed at both the traditional government IT systems and those specific to elections.

Both ISACs continued to utilize centralized, and in many cases shared, resources to enable a greater level of visibility and information sharing across the elections and the SLTT government sector to benefit the constituencies of both organizations. Furthermore, everything from webcasts to workgroups to in-person meetings integrate the needs of both ISACs, offering efficiency and consistency for the Membership. The support structure behind the ISACs includes:

- Security Operations Center (SOC) to provide 24/7/365 incident triage and immediate response.

- Computer Emergency Response Team (CERT) to provide incident response and forensic services.
- Cyber Intelligence Team to provide forward-leaning analysis, written products, and presentations.
- Engineering Team to provide sensor deployment and technical assistance
- Stakeholder Engagement Team to provide member support and engagement.

MS-ISAC  
Multi-State Information  
Sharing & Analysis Center®

12. To streamline the membership process, ISAC staff, along with teams from across CIS, made a change, replacing the Membership Agreement (which required handwritten signatures of both parties) with a checkbox on the online registration form for potential members to agree to a set of terms and conditions. This led membership growth in both the EI-ISAC and MS-ISAC; in fact, MS-ISAC membership grew by over 150 percent in 2018. This change now precluded the possibility of no formal agreement at the local level or public oversight.<sup>15</sup>

13. Partnerships: Partnership expertise of NASS and NASED at the state level, to iGO (International Association of Government Officials) and the Election

---

<sup>15</sup> *Id.* pg. 5



Center's provided the insight into local government election organizations.<sup>16</sup>

14. Albert: Elections-Focused Cyber Defense Suite created by the EI-ISAC<sup>17</sup>

- a. A focus of the EI-ISAC's efforts throughout 2018 was a federally funded initiative to deploy its IDS, known as Albert, on elections networks throughout the United States.<sup>18</sup>
- b. Under the MS-ISAC, sensors had already been funded for each state and territorial network and were developed to be specific to the SLTT government environment. The EI-ISAC expanded this initiative to cover the voter registration databases of any state or territory where the voter registration database was not already covered by an existing sensor, as well as to place sensors in 42 of the most populous local election jurisdictions in which voter registration data were hosted on local hardware.<sup>19</sup>

15. "A combination of logistical expediting, a Membership that was incredibly supportive of the efforts, and extensive outreach and technical support efforts by EI-ISAC staff and partners paid off with DHS Secretary Kirstjen Nielsen sharing that on Election Day, approximately 90 percent of all voters

---

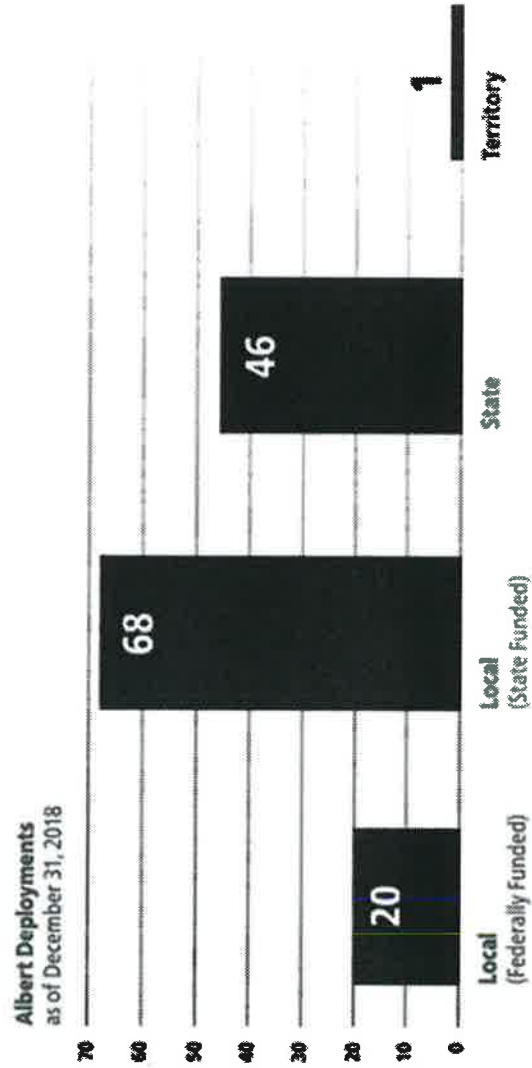
<sup>16</sup> *Id.*

<sup>17</sup> *Id.* pg. 7

<sup>18</sup> *Id.*

<sup>19</sup> *Id.*

in the United States would cast a ballot in a jurisdiction or state monitored by Albert.”<sup>20</sup>



“Using a multi-pronged approach to achieve

---

<sup>20</sup> *Id.* pg. 8

these goals, the EI-ISAC and DHS embedded a DHS Intelligence & Analysis representative at the EI-ISAC headquarters for more than a month prior to the election, heightened reporting through fusion centers to improve accuracy, and developed new, internal reporting streams for information-sharing. At the end of October, an elections focused Intelligence Analyst from the EI-ISAC was detailed at NCCIC in Washington, D.C., to assist with federal communication with EI-ISAC headquarters.”<sup>21</sup>

16. National Cyber Situational Awareness Room (NCSAR) The NCSAR HSIN room was opened to EI-ISAC members and partners on October 31 for 12 hours each day and transitioned to a 24-hour resource on November 4 for the duration of the week of the general election. Over the two-week election span, particularly on November 6. “. . . representatives from 40 states, two territories, 120 local government elections offices across 30 states, 15 federally recognized fusion centers, NASS, NASED, vetted vendors of election infrastructure, the Information Technology-ISAC, and the MS-ISAC coordinated activity and shared information. DHS Cybersecurity Advisors, representatives from the ETF, and federal representatives designated by EI-ISAC members also accessed the NCSAR.”<sup>22</sup>

---

<sup>21</sup> *Id.* pg. 11

<sup>22</sup> *Id.*

### **2019-2020 Expansion**

17. The expansive reach of the DHS, federal and private partners continued under the guise of “security” and enters the public sector through social media regarding “disinformation” of security of elections.

18. CISA’s Cybersecurity Advisors (CSAs) are trained CISA personnel based throughout the United States in the private sector entities and state, local, territorial, and tribal (SLTT) governments under the guise to prepare for—and protect themselves against—cybersecurity threats.<sup>23</sup>

19. By 2019, through CIS Security, CISA, and DHS there are now 73 districts in 50 states and Puerto Rico, Protective Security Advisors (PSAs) are linked to CISA infrastructure and the Federal Emergency Management Agency (FEMA).<sup>24</sup>

20. “Election infrastructure security is a priority for the Cybersecurity and Infrastructure Security Agency (CISA), based in the Department of Homeland Security (DHS). As the lead agency for securing the Nation’s homeland, DHS, through CISA, is responsible for maintaining public trust and confidence in America’s election system. CISA works directly with election officials throughout the United States to help them protect election systems by sharing timely and actionable threat information and offering cybersecurity services to safeguard their election systems.”<sup>25</sup>

---

<sup>23</sup> See pg. 2 [https://www.cisa.gov/sites/default/files/publications/19\\_0531\\_cisa\\_election-security-resources-guide-may-2019.pdf](https://www.cisa.gov/sites/default/files/publications/19_0531_cisa_election-security-resources-guide-may-2019.pdf)

<sup>24</sup> *Id.* pg. 3

<sup>25</sup> *Id.* pg. 1

21. Through CIS, DHS has infiltrated all aspects of the State of Texas' election processes. EI-ISAC (Election Infrastructure Information Sharing and Analysis Center), created by DHS, currently develops and oversees the following:

- a. "The EI-ISAC is a voluntary, collaborative effort between its parent organization, the Center for Internet Security . . . , CISA, and the EIS GCC. Funded through DHS grants, the EI-ISAC addresses the cybersecurity needs of state and local election offices. The EI-ISAC offers state and local election officials a suite of elections-focused cyber defense tools, including threat intelligence products, incident response and forensics, threat and vulnerability monitoring, cybersecurity awareness and training products, and best practices."
- b. Alignment to the NIST Cybersecurity Framework . . . "facilitate an CRR (Cyber Resilience Review) to test if it aligns closely with Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST)."26
- c. Data Privacy The CRR report is created exclusively for an organization's internal use. All data collected and analysis performed during a CRR is protected under the DHS Protected Critical Infrastructure Information (PCII) Program (dhs.gov/pcii). PCII Program protection means CISA employees are trained in the safeguarding and handling of PCII;

---

<sup>26</sup> *Id.* pg. 5

CISA cannot publicly disclose PCII; and PCII cannot be used for regulatory purposes.<sup>27</sup>

22. “The External Dependencies Management (EDM) Assessment is an interview-based assessment evaluating an organization’s management of external dependencies. This assessment focuses on the relationship between an organization’s high-value services and assets, such as people, technology, facilities, and information, and evaluates how the organization manages risks derived from its use of the Information and Communications Technology (ICT) Supply Chain in the delivery of services. The EDM Assessment evaluates the maturity and capacity of an organization’s external dependencies risk management across the three areas: • Relationship formation, • Relationship management and governance, and • Service protection and sustainment.”<sup>28</sup> The #Protect2020 Strategic Plan posted in February of 2020 by CISA and DHS outlines the federal government’s campaign for the general election of 2020. (State and Local Election Authorities, Election Technology Vendors, Campaigns and Political Infrastructure, American Electorate)<sup>29</sup>

23. This “campaign” is a guide on the implantation of the federal government’s continued assault on U.S. Const. Art. 1 Sec 4 and privacy rights of the

---

<sup>27</sup> *Id.*

<sup>28</sup> *Id.* pg. 6

<sup>29</sup> [https://www.cisa.gov/sites/default/files/publications/ESI%20Strategic%20Plan FINAL%202.7.20%20508.pdf](https://www.cisa.gov/sites/default/files/publications/ESI%20Strategic%20Plan%20FINAL%202.7.20%20508.pdf)

Plaintiffs with involvement in Texas' election at the local level.

24. CISA's partners have now expanded to a number of federal agencies some with a direct election-related mandate while other adapting from traditional roles to election security.<sup>30</sup>

25. Under former Secretary Kirstjen Nielsen of DHS, the established Countering Foreign Influence Task Force (CFITF) now formally part of CISA, is charged with helping CISA's leadership to identify policy options available to the government, working with social media companies, academia, international partners, and across the executive branch on a variety of projects. The FBI Foreign Influence Task Force and CFITF coordinate "closely" on public outreach and education efforts.<sup>31</sup>

26. CISA's campaign is a marketing effort to introduces the federal government's "idea" of education on election infrastructure by promoting government funded "election security" via influencer organizations to build public "awareness" about disinformation threats and engaging "trusted voices" such as the American Association of Retired Persons (AARP) and the National Association for the Advancement of Colored People (NAACP). CISA's intent is to amplify resilience messaging and reach a broader "stakeholder" (citizens of the United States). There is no mistake that the people of the State of Texas and the citizens of the United States of American are the "stakeholders"

---

<sup>30</sup> *Id.* pg. 7

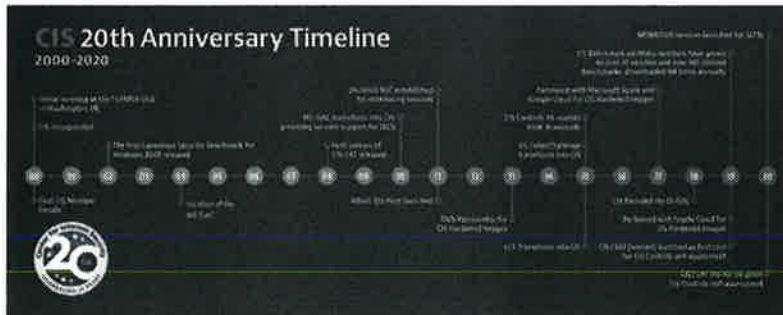
<sup>31</sup> *Id.* pg. 16

CISA is targeting for the Department of Homeland Security.<sup>32</sup>

27. “Following its success in the 2018 U.S. midterm elections, CISA again plans to operate as a switchboard for routing disinformation concerns of state and local elections officials to appropriate social media platforms and law enforcement agencies.”<sup>33</sup>

### Center for Internet Security and Partners (CIS)

28. CIS website claims to be a community-driven nonprofit. Founded in August of 2000. “CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.”<sup>34</sup>



<sup>32</sup> *Id.* pg. 19

<sup>33</sup> *Id.* pg. 20

<sup>34</sup> <https://www.cisecurity.org/about-us>



**Transcription:**

**CIS 20th Anniversary Timeline 2000-2020**

- 2000 Initial meeting at the COSMOS Club in Washington DC; CIS Incorporated
- 2002 The first Consensus Security Benchmark for Windows 2000 released
- 2004 Creation of the MS-ISAC
- 2008 First version of CIS-CAT released
- 2010 MS-ISAC transitions into CIS, providing no-cost support for SLLTs
- 2011 24x7x365 SOC established for monitoring services
- 2013 AWS Partnership for CIS Hardened images
- 2015 CIS Controls V6 reaches 100k downloads; US CyberChallenge transitions into CIS; CCS Transitions into CIS
- 2017 Partnered with Microsoft Azure and Google Cloud for CIS Hardened Images
- 2018 CIS founded the EI-ISAC
- 2019 CIS Benchmark portfolio numbers have grown to over 25 vendors and over 100 distinct Benchmarks, downloaded 1M times annually; Partnered with Oracle Cloud for CIS Hardened images; CIS CSAT [hosted] launched as first tool for CIS Controls self-assessment
- 2020 MDBR/EDR services launched for SLTTs; CIS CSAT Pro for on-prem CIS Controls self-assessment

29. Akamai-In 2015; Akamai Technologies, Inc. announced a strategic partnership agreement with China Telecom Corporation Limited's cloud division, CT Cloud.<sup>35</sup> As discussed previously in "Foreign Companies In Texas Infrastructure"; Akamai Technologies is merged with a Chinese company and is "involved in" Texas' election infrastructure in more than one junction.

30. Malicious Domain Block and Reporting (MDBR)<sup>36</sup> service initiative was announced by CIS on September 2, 2020; a year-long project funded by DHS to make state and local government networks and systems providing federal authorities "more insight into how the nation's smaller governments are being attacked." The initiative is the result of a partnership among the DHS's Cybersecurity and Infrastructure Agency (CISA), the Center for Internet Security (CIS), and Akamai. MDBR as of this posting serves 346 of the approximately 40,000 SLTT governments in the United States.

31. CIS further confirms the partnership with Akamai in an August 1, 2022 post stating;

"Akamai Enterprise Threat Protector (ETP) is a cloud-base secure web gateway (SWG) designed to help security teams ensure that users and devices can securely connect to the internet wherever they happen to be, without

---

<sup>35</sup> <https://www.prnewswire.com/news-releases/akamai-and-china-unicom-establish-strategic-cloud-services-partnership-300088898.html>

<sup>36</sup> <https://www.cisecurity.org/about-us/media/media-mention/dhs-partners-with-industry-to-offer-state-local-govts-cybersecurity-aid>

the intricacy and management overheads associated with other legacy security solutions. Enterprise Threat Protector is powered by real-time threat intelligence based on Akamai's unrivaled global insights into internet and domain name system (DNS) traffic, as well as multiple malware-detection engines.”<sup>37</sup>

32. Akamai's involvement highlights this growing dominance of Chinese/foreign suppliers and infiltration of US elections which adds further weight to Plaintiffs' arguments of “Foreign Companies in Texas Election Infrastructure”. See Decl. of Terpshore Maras, Lines 129-135.<sup>38</sup>

33. CrowdStrike — CIS and Cybersecurity firm CrowdStrike announced on November 5, 2021 it's partnering to provide a slate of security services to U.S. State, Local, Tribal and Territorial (SLTT) governments. “The new CIS Endpoint Security Services (ESS) platform, which is backed by CrowdStrike's tools, is built to identify, detect, and respond to security alerts from local governments.”<sup>39</sup>

34. CrowdStrike's Falcon system will offer ESS users deployments onto endpoint devices to include USB device monitoring and host-based firewall management. CrowdStrike has previously worked with

---

<sup>37</sup> <https://www.cisecurity.org/services/cis-cybermarket/software/akamai-enterprise-threat-protector>

<sup>38</sup> <https://files.tttexas.com/case/TX SOS Election Violation References>

<sup>39</sup> <https://www.zdnet.com/article/cis-partners-with-crowdstrike-on-cybersecurity-platform-protecting-local-governments/>

CIS on Elections Infrastructure and this partnership will see them provide a fully managed 24/7/365 next-generation cybersecurity offering tailored to SLTT to include more than 12,000 Multi-State Information and Analysis Center members across the US, with more than 14 million endpoints in total.<sup>40</sup>

### **Department of Homeland Security/CISA/CIS Security Agreements**

#### **Local Government**

35. Dallas and Denton Counties are one of many of the jurisdictions in Texas that entered into a “Memorandum of Agreement for Cybersecurity Services” with CIC operating in the capacity of the EI-ISAC. Dallas County Judge, Clay Jenkins signed on October 19, 2018 and Denton County Judge, Andy Eads signed on August 6, 2019.

36. In this same “Memorandum” between Dallas and Denton County, Texas, we learn that the EI-ISAC is contracted by the Department of Homeland Security to provide “Cybersecurity Services” for the state election entities.

---

<sup>40</sup> *Id.*

**MEMORANDUM OF AGREEMENT  
BETWEEN THE CENTER FOR INTERNET  
SECURITY/ELECTION INFRASTRUCTURE  
INFORMATION SHARING AND ANALYSIS  
CENTER AND FOR CYBERSECURITY SERVICES**

Dallas County, Texas

---

(Federally Funded Election Services)

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

37. Not only is this a bold step to “federalized” Texas elections in violation of U.S. Const. Art. 1 Sec. 4 but is evidentiary of 4th Amendment rights violations.

**Whereas**, CIS entered into an agreement with the U.S. Department of Homeland Security (“DHS”) to provide Cybersecurity Services for state election; and

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

38. The “cybersecurity services” and any “associated service devices” are at no cost to the entity. This DHS and EI-ISAC among other three letter agencies entering into an agreement to federalize elections at a

App.322a

county level by incentivizing compliance in exchange for “free” services.

III. Consideration

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

39. Ironically, this is “contingent on the availability and allocation of federal funds for this purpose”.

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

40. In return for the incentive of “no cost” for Albert sensor devices, CIS Security and DHS receive access to all of the following:

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

1. Current network diagrams to facilitate analysis of security events on the portion(s) of Entity’s network being monitored. Network diagrams will need to be revised whenever there is a substantial network change;
2. In-band access via a secure Internet channel to manage the device(s).
3. Outbound access via a secure Internet channel for log transmission.

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

41. The county also acknowledges that it may receive from CIS trade secrets and confidential and proprietary information "Confidential Information however both parties agree to "hold each other's Confidential Information" in confidence. Except the inclusion of CIS shall be permitted to disclose "relevant aspects" of such Confidential Information to its officers, employees, agents and CIS's cybersecurity partners,

including federal partners. Federal partners such as DHS, FEMA, LISA, FBI . . .

42. Along with unfiltered access to the county's ("entity") data of constitutes, the county shall also provide at the county's expense, logistic support in the form of rack space, electricity, Internet connectivity, and any other infrastructure necessary to support communications at the county's expense.

43. Travis County also entered into an agreement with CIS Security in which the Commissioners Court via the Purchasing agent submitted an Affidavit of Single Source to include additional network security monitoring sensors and analysis services (Albert) to both primary and secondary data center locations.<sup>41</sup>

44. The Center for Internet Security, Inc. (CIS Security) posted on their website MS-ISAC local county elections which include but are not limited to the following: Anderson, Andrews, Aransas, Arlington, Atascosa, Austin, Bandera, Bastrop, Baylor, Bee, Bell, Belton, Bexar, Borden, Brackett, Brazoria, Brazos, Brewster, Brown, Buna, Burleson, Burnet, Callahan, Cameron, Camp, Canton, Cherokee, Clay, Collin, Comal, Dallas, Denton, Eastland, Ector, Ellis, Falls, Fayette, Fort Bend, Franklin, Gaines, Galveston, Gillespie, Harris, Hays, Hood, Hidalgo, Hockley, Houston, Jack, Jim Wells, Johnson, Kendall, Kleberg, La Salle, Lee, Liberty, Lavaca, Lamar, Llano, Medina, McLennan, McCulloch, Lubbock, Midland, Montgomery, Moore, Nacogdoches, Navarro, Parker, Palo Pinto, Nueces, Rains, Randall, Reeves, Refugio, Rockwall, Runnels, Rusk, Smith, San Patrick), San

---

<sup>41</sup> See Appendix



Jacinto, San Augustine, Tarrant, Taylor, Terrell, Tom Green, Throckmorton, Uvalde, Trinity, Victoria, Williamson, and<sup>42</sup> . . . . .

45. DHS has entered into agreements with multiple SLTT government entities throughout Texas which include more than just “election” infrastructure but all aspects of governmental databases. (College Districts, Local Independent School Districts, County Offices, County Tax Assessor-Collector, Police Departments, Medical Services and Centers, 911 Districts, Power and Light, Water Authority, Health Network, Hospitals, City and Council Governments, Navigation & Port Districts, Regional Education Service Centers, Work Force Solutions, and . . . ).

**State Government/Secretary of State**

46. In 2015, Texas Governor Greg Abbott laid out the “Texas Homeland Security Strategic Plan 2015-2020” which “sets out a long-term vision for homeland security, providing guidance on how Texas will build on our previous successes and address emerging challenges and requirements”.

47. This “Strategic Plan” identified the following areas that fell under the scope of the plan:

Homeland Security Risk, Critical Infrastructure, Threats and Hazards and Texas in 2020.

**2018**

48. In February of 2018 Texas Director of Elections, Keith Ingram, testified to the Texas Senate

---

<sup>42</sup> *Id.*

on election security.<sup>43</sup> Ingram confirmed that Texas was included in attempts to scan election systems in 2016 from foreign nation IP addresses contrary to SOS office stance today. Ingram continues by confirming “We also have working relationship with the Department of Homeland Security as well as the MSI-ISAC multi-state information sharing and analysis center and have since 2016 . . . as well as the fact that we’ve got an Albert sensor on our registration database.” Ingram, on behalf of the SOS Office, believes that including DHS, a federal organization, in Texas elections is “taking measures that we deem to be reasonable and necessary to make sure that personally identifiable information of Texas voters stay safe”.<sup>44</sup>

49. On November 30, 2018, the Texas Secretary of State’s office provided a report outlining Texas Cybersecurity Preparedness to the Texas legislature in which SOS conducting this study upon visiting several counties in central Texas.<sup>45</sup> The report makes “A final recommendation regarding security of the voter registration database is to pass legislation enabling the SOS to require cyber training for all of the users of its systems. Our Office has made “Securing the Human” training available to county users at no cost. However, Our Office has no ability to require them to take the course, only the ability to encourage them to take advantage of this free useful resource.”

---

<sup>43</sup> <https://www.sos.texas.gov/elections/conducting/security-update.shtml> (last visited 9/7/2022)

<sup>44</sup> <https://www.youtube.com/watch?v=fwA89bv8UhE&t=2463s>

<sup>45</sup> Report to the Texas Legislature on Election Cybersecurity Preparedness (state.tx.us)

**2020**

50. The SOS Office released “Election Security Best Practices Guide”<sup>46</sup> in April 2020 as developed by Election Security Assessments (ESAs) of county election offices that were conducted as required by HB 1421.<sup>47</sup> Practices and Policies are as follows:

**2. MONITOR CONTINUOUSLY FOR THREATS**

***PRIORITY BEST PRACTICES***

- a. Contract an external security service provider to monitor the network and remote systems 24 hours every day and analyze events for indicators of cyberattack. Available services include:
  - i. Albert Sensor from the Center for Internet Security (CIS)
  - ii. Monitoring services available through the Texas Department of Information Resources (DIR)
- b. Ensure the service provider uses effective threat monitoring software and hardware products, particularly a Security Incident and Event Management (SIEM) solution.

**6. CONDUCT ELECTION SECURITY ASSESSMENTS REGULARLY**

***PRIORITY BEST PRACTICES***

---

<sup>46</sup> <https://www.sos.texas.gov/elections/forms/election-security-best-practices.pdf>Usearch=election%20security%20best%20practices%20guide

<sup>47</sup> See Tex. Elec. Code § 279

App.328a

- a. Participate in the Election Security Assessment provided by the Texas SOS Office as required by Section 279.003, Texas Election Code.
- b. Conduct subsequent security assessments at least once every two to four years or more often if the political subdivision has a significant change in structure or circumstance such as purchasing new equipment, moving to a new office, or 10 changing personnel. Certain political subdivisions may be eligible for assessments provided by DHS. Election authorities may also contract with private entities to conduct security assessments.
- c. Use the ESA results and the results from any subsequent assessment to establish a roadmap defining how and when the required improvements will be made.

**7. PARTICIPATE IN THE DHS MS-ISAC AND EI-ISAC INFO SHARING PROGRAM**

- a. Election Officials should join the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) information services and IT officials should join the Multi-State Information Sharing and Analysis Center (MS-ISAC) and provided by the Department of Homeland Security (DHS).
- b. Review communications and develop a process for monitoring the cyber threats tracked and reported by the MS-ISAC/EI-ISAC Security Operations Center (SOC)

51. Appendix A of the guide provides a list of "Election Data Classifications System". This list contains personal data as defined by Tex. Elec Code 13.004

(c) such as social security number, driver's license, residence address of federal or state judges and their spouses, residence address of applicants if the applicant or another person in the applicant's household is a victim of family violence, sexual assault, or abuse, stalking or trafficking, residence address of peace officers and other protected individuals under Texas Law, criminal history, and etc.

## **2022**

52. The Secretary of State's 2022 Election Security update outlines current practices as well as legislation associated with election security including the participation of "most Texas counties" in EI-ISAC.

### **Working with Federal and Local Partners**

- The SOS along with our county election officials have participated in numerous tabletop exercises on election security provided by the Department of Homeland Security.
- The SOS has provided on-going training opportunities for county election officials at our annual seminars, and on an individual basis, as needed, to county election officials.
- Most Texas counties participate in the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) to ensure that the elections community is effectively sharing relevant information with respect to safeguarding our elections and being aware of potential cyber threats.

### **Protecting Election Infrastructure**

- The Texas Secretary of State's office has also taken the following steps to further strengthen

App.330a

election infrastructure security in the State of Texas:

- Established effective communication protocols with the Department of Homeland Security (DHS), the Federal Bureau of Investigations (FBI), the Department of Public Safety (DPS), and the Department of Information Resources (DIR) to coordinate cybersecurity monitoring and response.
- Engaged in a pilot program with DHS and the Multi-State Information Sharing & Analysis Center (MS-ISAC), which helped develop and improve information sharing protocols between the federal government and the states in the realm of election security.
- Instituted multi-factor authentication for election officials to ensure that only those who are authorized to do so can gain access to the statewide voter registration database.
- Installed an active Albert sensor on our voter registration database that alerts our agency when any suspicious cyber-activity occurs.
- Submitted Texas' proposal to the U.S. Election Assistance Commission (EAC) (PDF) for implementing new cybersecurity and election security measures – both at the state and local levels – using funds from the 2018 HAVA disbursement to states for election security.
- Informed and encouraged Texas counties to take advantage of free cybersecurity services and physical security assessments available from DHS, MS-ISAC, and EI-ISAC.

- Removed legal roadblocks that prevented counties from upgrading to newer, more secure systems.

53. DHS may claim “extraordinary circumstances” or necessary to [the U.S. government’s] safety however the fact remains that only Congress would likely involve itself in congressional elections. To state concern over the ability of Congress to legislate how states would hold congressional elections, Alexander Hamilton, in *The Federalist No. 59*, reasoned that unless Congress had authority to regulate Senate and House elections, state legislatures might “at any moment annihilate [the U. S. government], by neglecting to provide for the choice of persons to administer its affairs” Noting that the Elections Clause gave state legislatures primary power over Senate and House Elections.

54. DHS cannot nor by Presidential executive order; impose election laws or enforce a “federal” authority on the states regarding elections.

“Who are to pass the laws for regulating elections? The congress of the United States, composed of a senate chosen by the state legislatures, and of representatives chosen by the people of the states. Can it be imagined, that these persons will combine to defraud

---

<sup>48</sup> <https://www.sos.texas.gov/elections/conducting/security-update.shtml> (last visited 9/7/2022)

their constituents of their rights, or to overthrow the state authorities, or the state influence?" Joseph Story, Commentaries on the Constitution of the United States § 826 (1833)

55. Judge Story's commentary echoes Hamilton's expectation as representatives of states and their people, Members of Congress would be reluctant to impose election laws on objecting states. This theory has been tested as recently as last year in H.R. 1: For the People Act of 2021.

56. H.R. 1 was to expand voter registration (*e.g.* automatic and same-day registration), and voting access (*e.g.*, vote-by-mail and early voting). It also limits removing voters from voter rolls. Additionally, the bill set forth provisions related to election security, including sharing intelligence information with state election officials, supporting states in securing their election systems, developing a national strategy to protect U.S. democratic institutions, establishing in the legislative branch the "National Commission to Protect United States Democratic Institutions", and other provisions to improve the cybersecurity of election systems.

57. Congress rejected this encroachment of federalization of elections. If Congress did not enact election cybersecurity law, then the federal government by way of DHS invading Texas' elections is unconstitutional and Defendants that have imposed such intrusion are derelict in their duty violating Plaintiffs' privacy and voting rights.

58. Art. I Sec. 4 of the Constitution makes clear that only the legislatures of the States have authority



to amend or nullify election statutes. *Bush II*, 531 U.S. at 104 (quoted supra). Non-legislative changes to State election law by SoS or County election officials are in violation of Art. 1 Sec. 4 of the U.S. Constitution.

59. Texas requires a voter to register in order to participate in state and federal elections within the state. Tex. Elec. Code § 11.002(a)(6).

60. The Texas voter registration form instructs prospective voters to provide at least the following information: name, residence and postal address, any previous voter registration address in Texas, county of residence, date of birth, previous name, driver's license number, or last four digits of social security number, and date of application. The applicant is further required to affirm that they: reside in the stated county and are a citizen of the United States, have not been convicted of a felony, or if a felony-have completed all punishment; and have not been determined by court to be mentally incapacitated.

61. The private information acquired by CIS via DHS is not widely available in Texas, but instead may be released only under certain circumstances and conditions imposed by Texas' voting laws. Tex. Elec. Code § 18.066. Seeking large scale voter information are only permitted to access certain data contained in Texas' computerized voter registration files and only upon certain conditions. Tex. Elec. Code § 18.066(d).

62. Requesting individuals or entities may obtain the limited, redacted information from the voter files only after (i) they pay a fee and (ii) they execute a notarized affidavit with the Elections Division of the Secretary of State's office stating that they will not use the data in certain enumerated, proscribed ways.

Tex. Elec. Code § 18.066. The affidavit from the requesting party must state “that the person will not use the information obtained in connection with advertising or promoting commercial products or services.” Tex. Elec. Code § 18.066(d). CIS Security currently has posted all SLT governments currently utilizing services and products.

63. The SoS offices may not furnish (i) any voter’s social security number; or (ii) certain residential addresses. Tex. Elec. Code § 18.066(b).

64. All Defendants have provided CIS Security, DHS, federal and third-party partners access to computerized voter file fields, including full names of all registrants, addresses, dates of birth, voting history from at least 2017 onward, active/inactive status and whether a voter’s registration has been cancelled, voting record (absentee, provisional, early, in-person), the party primaries for state and federal elections that the voter participated in, and the registration effective date.

65. Even if cabined to information generally available to candidates or other organizations who are entitled to request voter information under Texas law, would undermine, and run afoul of, the State’s carefully-crafted regulation of the use of voter data.

66. Firstly, the disclosure of private voter data under federal transparency requirements would enable widespread abuse of that information to the detriment of Plaintiffs. Neither the SoS Defendants nor the County Defendants can possibly provide assurances as to the voter data’s use once it is collected by federal agencies and their third-party vendors.

67. Secondly, voter birthdates threatens the privacy interest of Plaintiffs as Texas courts have acknowledged, a citizen has an inherent privacy interest in his or her birthdate, given that such date, in combination with other information that all Defendants have made available, can result in identity theft. It is for that reason that Texas courts have held that the disclosure of birth information constitutes a “clearly unwarranted invasion of personal privacy.”

68. Texas courts have recognized a “nontrivial privacy interest” in birth dates. *See Paxton v. City of Dallas*, No. 03-13-00546-CV, 2015 WAL3394061 at \*3 (Tex. App. May 22, 2015) (concluding that “public citizens have a privacy interest in their birth dates”), reviewed denied (Sept. 4, 2015); *Tex. Comptroller of Pub. Accounts v. Att’y Gen. of Tex.*, 354 S.W.3d 336, 34648 (Tex. 2010)(holding that disclosure of state employee birth dates constituted a “clearly unwarranted invasion of personal privacy”), *See also* Tex. Att’y Gen. Op. OR2017-06026 (2017) (“Based on *Texas Comptroller*, the court of appeals [in *City of Dallas*] concluded the privacy rights of public employees apply equally to public citizens, and thus, public citizens’ dates of birth are also protected by common-law privacy . . . ”)

69. Under the common-law right of privacy, an individual has a right to be free from the publicizing of private affairs in which the public has not legitimate concern. *Industrial Found.*, 540 S.W. 2d at 682; *see also Abbott v. Dallas Area Rapid Transit*, 410 S.W.3d 876, 880 (Tex. App.—Austin 2013, no pet.). Plaintiffs have an expectation of privacy when registering to vote.

70. The Texas Supreme Court acknowledged in *Texas Comptroller* that the disclosure of “[birth] dates,

when combined with name and place of birth, can reveal social security numbers.” 354 S.W.3d at 345.

71. All Defendants acknowledge by DHS/CIS participation provided certain information including voter names, addresses, date of birth and registration, voting methods, voter status, and the elections (including primaries) in which specific voters have participated.

72. The disclosure of birth dates included in the access provided have and will continue to violate Texas and Federal law and the rights of Plaintiffs. Furthermore, the combination of the identifying information, combination of birth dates and physical address, creates a greater risk of harassment and intimidation. Once Plaintiffs information becomes publicly available, the uses and purposes other entities have for it will be beyond the control of Defendants.

73. Thus, by providing unilateral unlimited access to Texas’ voter rolls or its information over to CIS Security, DHS and federal and third-party partners, all the Defendants would be sanctioning the disclosure of information regarding Plaintiffs’ to private firms and federal agencies, who could use such data without limitation and to the detriment of the privacy and associational rights of Texas voters, including Plaintiffs.

74. Why has DHS, CISA, FEMA, FBI,-the Federal Government in our election infrastructure?

75. Plaintiffs do not consent to DHS and affiliated federal agencies (CISA, NSA, FBI, FEMA) in our election infrastructure. This overreach of power provides access to private information, including voting records.

76. The expectation of privacy held by voters, is that private personal information will provide voters the right to vote within their local counties. Defendants have actively marketed and promoted the federalization of Texas elections without the consent of legislators or Plaintiffs. Under *Heckler v. Chaney*, 470 U.S. 821, 833 n.4 (1985), conscious action of executive policies to nullify statutes or to ignore statutory responsibilities are “reviewable” as if the policy had been written. Thus, the awareness of actions by State or local officials to nullify or ignore election and constitutional statutes violates the Election Clause and Right to Privacy.

77. Plaintiffs have not consented and do not consent to allow the federal government by way of DHS to violate our voting rights by the “federalization” of our elections or to have access to Plaintiffs’ personal and private information.

78. The contracts agreed to by both state and local officials have allowed for private voters data to be shared with federal entities. All Defendants cannot sidestep Texas law or U.S. Constitution simply because the CIS Security and DHS request it to be so in the name of security.

79. Plaintiffs do not and did not consent to have our private and personal information shared with federal entities or have federal entities dictating guidelines for how local and state elections are to be run.

80. The Texas State Election Code does not provide or authorize any election official either at the local or executive government level to “federal” state elections.

81. All Defendants have significantly overreached their authority and violated Plaintiffs' rights to vote in a free and fair election by knowingly providing access to Plaintiffs' personal data via the State of Texas' voter registration database to the federal government via DHS and affiliated federal agency "partners".

82. This blatant disregard for the rule of law renders all voting constitutionally tainted.

83. By allowing for the inclusion of federal agencies in Texas elections, all Defendants are currently in violation of U.S. Const. Art. 1 Sec. 4, 4th Amendment of the U.S. Const., Privacy Act of 1974.

### **III. Failures, Neglect and Offensive Violations**

84. All Defendants', non-legislative actors, actively marketed and promoted the federalization of Texas elections via DHS and affiliated federal agency "partners" to our local and state governments.

85. All Defendants', non-legislative actors, illegally authorized the monitored and provided access to personal and private information to federal agencies via DHS.

86. All Defendants', non-legislative actors, illegally authorized the monitored and provided access to personal and private information to federal agencies via DHS.

87. All Defendants' duplicitous activity and arrangement seem to only exist for a singular self-serving purpose of covering misdeeds and offenses.

#### **IV. Conclusions**

88. The SoS Defendants' and County Officials' defiance of Election Code knowingly caused the Plaintiff(s), registered voters of Texas; to cast a vote

- a. Under false pretense<sup>49</sup>
- b. Prevent a cast of a legal vote in which Plaintiff(s) are eligible to vote<sup>50</sup>
- c. Cause the ballot not to reflect the intent of the Plaintiff(s)/voter<sup>51</sup>
- d. Defendants committed the offense while acting in the capacity of an elected official<sup>52</sup>

**COUNT VI Civil Action  
for Deprivation of Rights**

**UNDER 5 U.S.C. 552pa,  
42 U.S.C. 1983vp,  
42 U.S.C. 1986**

**Election Clause — Right to Privacy**

**(U.S. Const. Art. 1 Sec. 4  
and Fourth Amendment)**

89. (Seeking declaratory and injunctive relief against All Defendants)

90. Plaintiffs incorporate the foregoing paragraphs as set forth in full herein.

---

<sup>49</sup> See Tex. Elec Code 276.013(1)

<sup>50</sup> See Tex. Elec Code 276.013(2)

<sup>51</sup> See Tex. Elec Code 276.013(6)

<sup>52</sup> See Tex. Elec Code 276.013(b)(1)

91. The foregoing violations have occurred as a consequence of Defendants acting under color of state and U.S. Constitutional law. Accordingly, Plaintiffs bring this cause of action for prospective equitable relief against Defendants pursuant to 5 U.S.C. 552pa, 42 U.S.C. 1983 and 42 U.S.C. 1986.

92. Art. 1 Sec. 4 of U.S. Const. provides, the authority of states to establish and regulate the times, places, and manners and laws of holding elections; state legislatures hold ultimate power over federal encroachment in regards to elections.

93. 4th Amendment of the U.S. Constitution is the right of a person's reasonable expectation of privacy.

94. Non-legislative actors lack authority to amend or nullify election statutes. *Bush II*, 531 U.S. at 104 (quoted *supra*)

95. The conscious and express actions by State and local election officials to nullify or ignore election statutes violates the Election Clause and Privacy.

96. By requiring Plaintiffs to "register" to vote on a system that is monitored unlawfully by federal agencies and "partners" providing access to private and personal information as defined by Tex. Elec. Code § 13.004, Defendants have and will continue to violated the rights of Plaintiffs under the Constitution of the United States.

97. By requiring Plaintiffs to vote on systems that are being monitored by the federal government, Defendants have and will violate the rights of Plaintiffs under the Constitution of the United States.



98. This Court has jurisdiction to grant injunctive relief base on 28 U.S.C. 1343 authority.

99. Unless Defendants are enjoined by this Court, then Plaintiffs will have no adequate legal, administrative, or other remedy by which to prevent or minimize the irreparable, imminent injury that is threatened by Defendants' intended conduct. Accordingly, appropriate damage and injunctive relief against these Defendants is warranted.

#### **IV. Prayer for Relief**

100. WHEREFORE, "For there is no authority except from God, and the authorities that exist are appointed by God." *Romans 13:1* (NKJV). Plaintiffs request that the Court grant the following relief:

101. Enter a preliminary and permanent injunction prohibiting Defendants from permitting the Center for Internet Security, Inc. in contract by the Department of Homeland Security from operating in any aspect of Texas election infrastructure.

102. Declare that the Defendants' Memorandums of Understanding/Agreements with Center for Internet Security, Inc. operating in contract by the Department of Homeland Security void and without legal force or effect.

103. Declare that the Center for Internet Security, Inc. in connection with the Department of Homeland Security are arbitrary, capricious and based on negligence and disregard in accordance with law.

104. Declare that the certifications and the actions taken by Defendants are in violation of the Constitution and contrary to the laws of the United States and the

State of Texas violating of the Election Clause (U.S. Constitution Art. 1 Sec. 4).

105. Temporarily restrain, as well as preliminarily and permanently enjoin Defendants, their agents, servants, employees, attorneys, and all persons in active concert or participation with any of them, from implementing and/or enforcing the MOU/Contracts with CIS/DHS of monitoring of election infrastructure and removal of all “Albert Sensors” or any other monitoring products that is not in compliance with the applicable law, and

106. Grant such other and further relief as may be just, equitable, and proper including without limitation, an award of any attorneys’ fees and costs to Plaintiffs.

Respectfully submitted this 1st day of October 3, 2022.

/s/ Kyle Strongin  
253 Martin Dr.  
Granbury, TX 76049  
979.492.0023  
kstrongin04@gmail.com  
Hood County

/s/ Lindsey Gremont  
4502 Deepwoods Drive  
Austin, TX 78731  
512.879.7069  
linny2777@protonmail.com  
Travis County

/s/ Christine Koepke  
19509 Encino Crown  
San Antonio, Texas 78259

App.343a

210.845.9448  
stina4kids@protonmail.com  
Bexar County

/s/ Travis Wayne Eubanks  
1823 Lookout Forest  
San Antonio, TX 78260  
505.506.1050  
travis.eubanks@gmail.com  
Bexar County

/s/ Amanda Eubanks  
1823 Lookout Forest  
San Antonio, TX 78260  
505.818.8824  
amanda.eubanks710@gmail.com  
Bexar County

/s/ Kristen Plaisance  
22355 Log Orchard Lane  
Porter, TX 77365  
713.724.0474  
robbiekristenp@gmail.com  
Montgomery County

/s/ Karen Rene "Towell"  
1015 Teresa Court  
Granbury, TX 76048  
817.300.0827  
renetowe116165@gmail.com  
Hood County

/s/ Jason S. Buster  
2003 Mulberry Tree  
San Antonio, TX 78251  
210.265.7914  
jason.s.buster@gmail.com  
Bexar County

App.344a

/s/ Alexandra Campo

---

PO Box40

Weir, Texas 78674

512.790.8774

acampo0312@gmail.com

Williamson County

App.345a

/s/ James L Clark

1750 Loop 165  
Dripping Springs, TX 78620  
512.808.6734  
rccpd715@protonmail.com  
Hays County

/s/ Jose Christine Silvester

8055 Garden Oaks Drive  
San Antonio TX, 78266  
830.515.3212  
lousilvester@msn.com  
Comal County

/s/ Tommie Dickinson

1231 W Goodwin  
Pleasanton, TX 78064  
830.570.1366  
tommie.dickinson@yahoo.com  
Atascosa County

/s/ Robert James Brooks Jr

3414 Zebecca Creek Drive  
Austin, TX 78732  
512.550.8688  
brooks@mindsetatx.com  
Travis County

/s/ Alana S. Phillips

3461 Highway 8 E,  
Mena, AR 71953  
940.437.0049  
Phillipsar@yahoo.com  
Denton County

App.346a

/s/ Jennifer B. Edwards

422 WW Lane  
Millsap, TX 76066  
940.682.5214  
Jenn@jennz.com  
Parker County

/s/ Aubrey Brandon Rhymes

3522 Turkey Pen Branch Road  
Maryville, TN 3 7083  
469.714.1157  
brandon.rhymes@protonmail.com  
Collin County

/s/ Lester Rand

515 Oakwood Drive  
Allen, TX 75013  
214.437.6780  
lrland01tv@gmail.com  
Collin County

/s/ Amber Cloy

421 Palisades Trail  
Keller, TX 76248  
817.522.2732  
Amberb2222@yahoo.com  
Tarrant County

/s/ Sheron Jennifer Lipper

11700 Preston Road, Ste.660-275  
Dallas, TX 75230  
214.679.5760  
Theburgundyacademy@gmail.com  
Dallas County

App.347a

/s/ Jennifer Williams

1613 Sandle Wood Drive  
Weatherford, TX 76087  
817.565.9137  
Jennifer.Williams2236@yahoo.com  
Parker County

/s/ Sonja Zielsdorf

400 County Road 369  
Taylor, TX 76574  
512.667.1746  
Sonjaz22@yahoo.com  
Williamson County

/s/ Juan Carlos Arias

9415 Pagewood Lane  
Houston, TX 77063  
713.204.0981  
Altcode1969@proton.me  
Harris County

/s/ Lynn Christine Davenport

9627 Windy Hill Road  
Dallas, TX 75238  
214-673-4018  
Ldaven@me.com  
Dallas County

/s/ Beverly Foley

8 Oak Village Ct  
Trophy Club TX 7 6266  
214.415.7154  
Beverlyfoley@gmail.com  
Denton County

**DECLARATION OF TERPSEHORE P. MARAS  
(NOVEMBER 29, 2020)**

---

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

1. I am over the age of 21 years and I am under no legal disability, which would prevent me from giving this declaration.

2. I have been a private contractor with experience gathering and analyzing foreign intelligence and acted as a LOCALIZER during the deployment of projects and operations both OCONUS and CONUS. I am a trained Cryptolinguist, hold a completed degree in Molecular and Cellular Physiology and have FORMAL training in other sciences such as Computational Linguistics, Game Theory, Algorithmic Aspects of Machine Learning, Predictive Analytics among others.

3. I have operational experience in sources and methods of implementing operations during elections both CONUS and OCONUS

4. I am an amateur network tracer and cryptographer and have over two decades of mathematical modeling and pattern analysis.

5. In my position from 1999-2014 I was responsible for delegating implementation via other contractors sub-contracting with US or 9 EYES agencies identifying connectivity, networking and subcontractors that would manage the micro operations.

6. My information is my personal knowledge and ability to detect relationships between the companies and validate that with the cryptographic know-



ledge I know and attest to as well as evidence of these relationships.

7. In addition, I am WELL versed due to my assignments during my time as a private contractor of how elections OCONUS (for countries I have had an assignment at) and CONUS (well versed in HAVA ACT) and more.

8. On or about October 2017 I had reached out to the US Senate Majority Leader with an affidavit claiming that our elections in 2017 may be null and void due to lack of EAC certifications. In fact Sen. Wyden sent a letter to Jack Cobb on 31 OCT 2017 advising discreetly pointing out the importance of being CERTIFIED EAC had issued a certificate to Pro V & V and that expired on Feb 24, 2017. No other certification has been located.