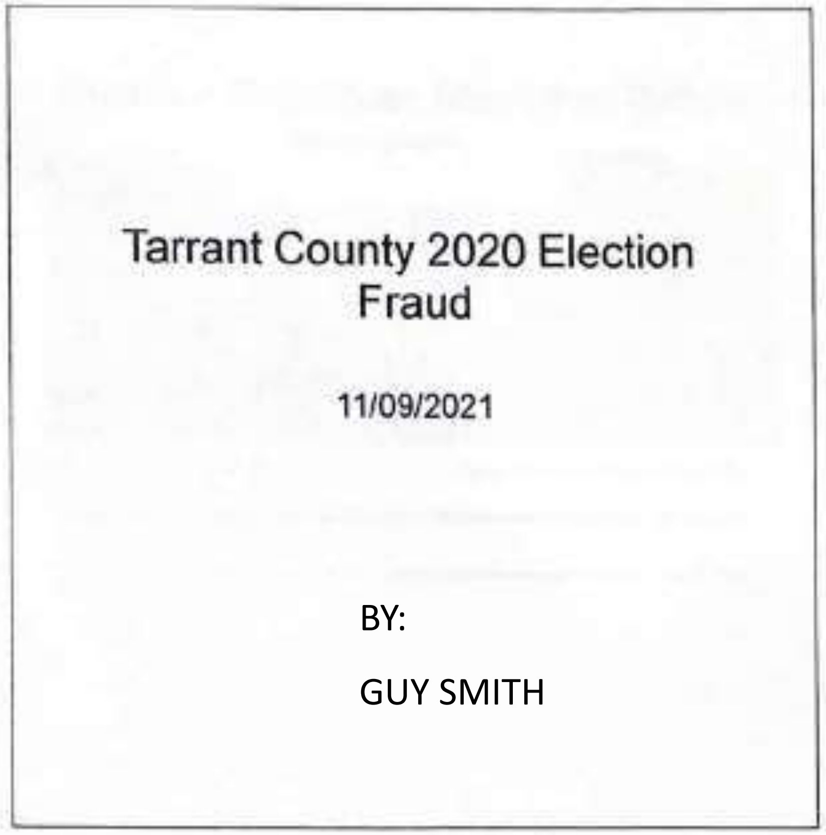
APPENDIX E

STATISTICAL IRREGULARITIES

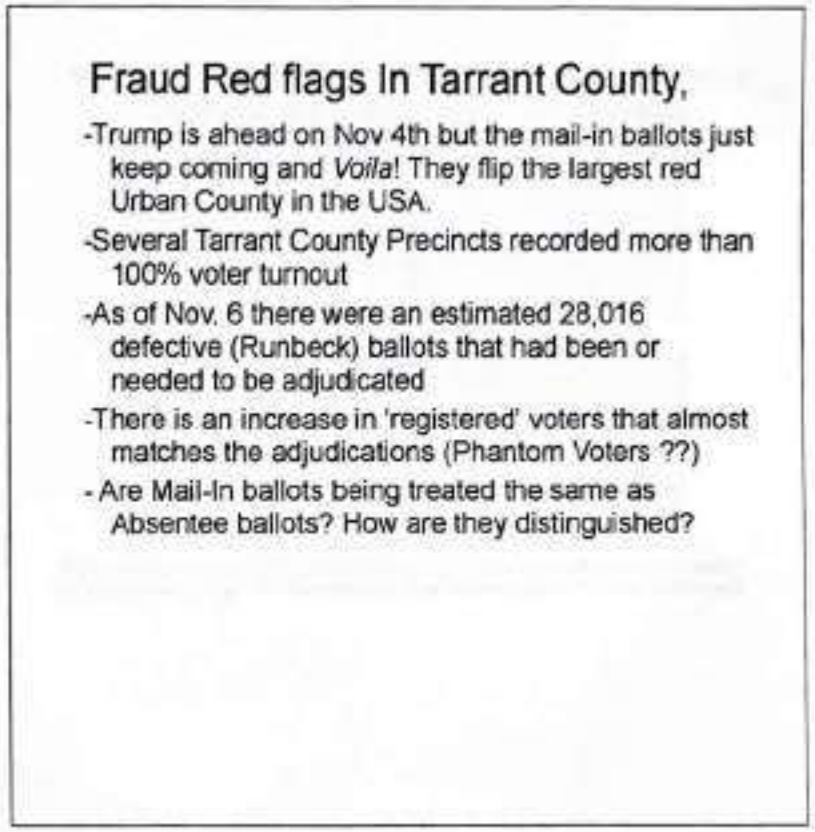


Tarrant County 2020 Election Fraud

11/09/2021

BY:

GUY SMITH



Fraud Red flags In Tarrant County,

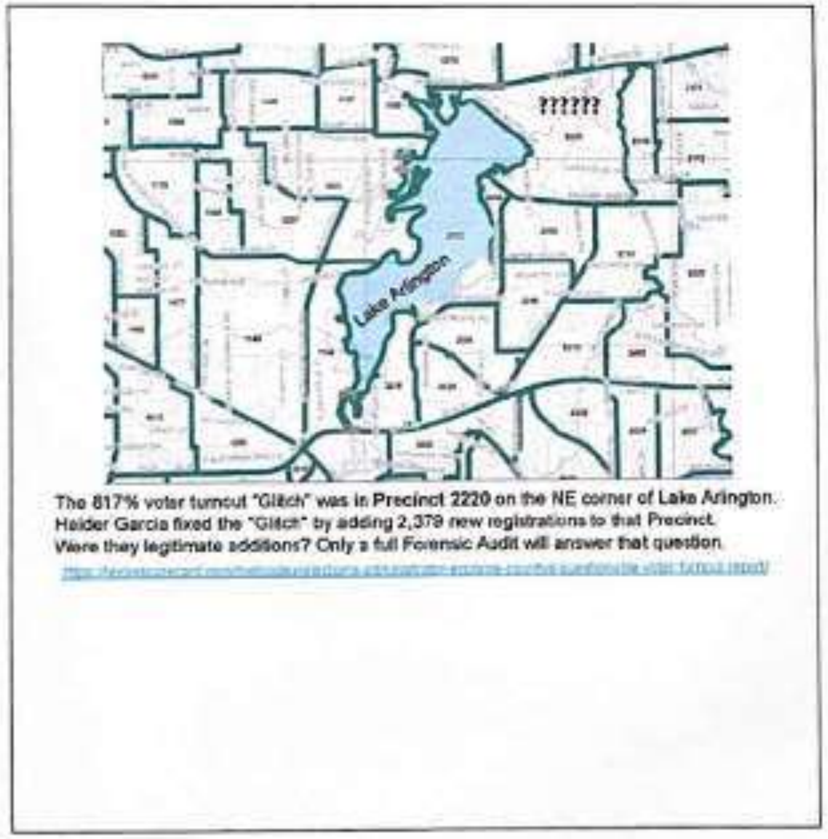
-Trump is ahead on Nov 4th but the mail-in ballots just keep coming and *Voila*! They flip the largest red Urban County in the USA.

-Several Tarrant County Precincts recorded more than 100% voter turnout

-As of Nov. 6 there were an estimated 28,016 defective (Runbeck) ballots that had been or needed to be adjudicated

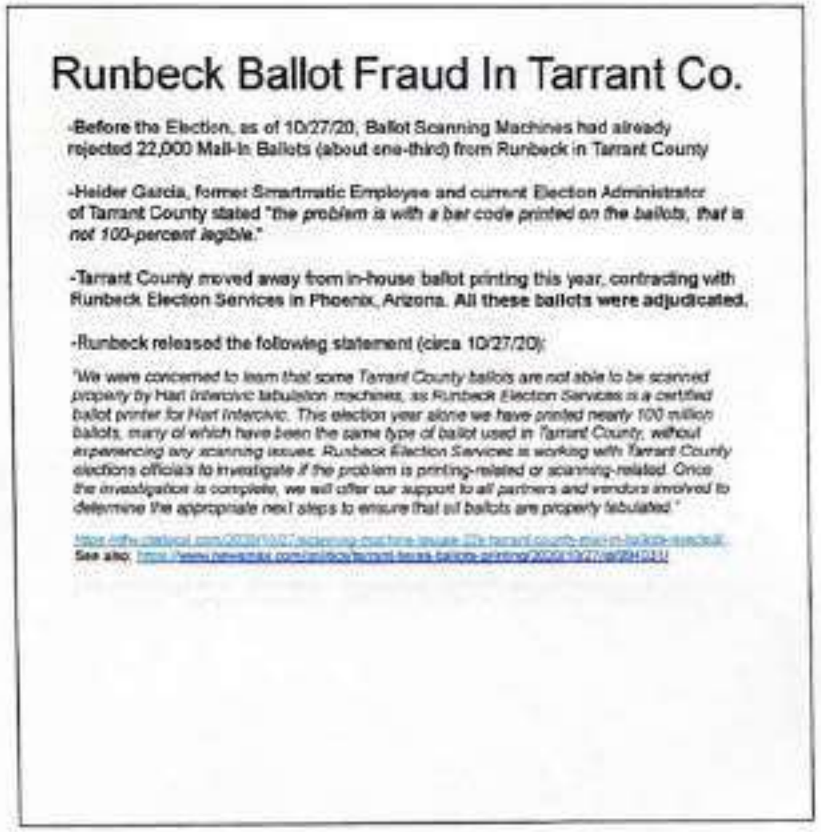
-There is an increase in 'registered' voters that almost matches the adjudications (Phantom Voters ??)

- Are Mail-In ballots being treated the same as Absentee ballots? How are they distinguished?



The 817% voter turnout "Glitch" was in Precinct 2220 on the NE corner of Lake Arlington. Heider Garcia fixed the "Glitch" by adding 2,379 new registrations to that Precinct. Were they legitimate additions? Only a full Forensic Audit will answer that question.

[illegible]



Runbeck Ballot Fraud In Tarrant Co.

-Before the Election, as of 10/27/20, Ballot Scanning Machines had already rejected 22,000 Mail-In Ballots (about one-third) from Runbeck in Tarrant County

-Heider Garcia, former Smartmatic Employee and current Election Administrator of Tarrant County stated "*the problem is with a bar code printed on the ballots, that is not 100-percent legible.*"

-Tarrant County moved away from in-house ballot printing this year, contracting with Runbeck Election Services in Phoenix, Arizona. All these ballots were adjudicated.

-Runbeck released the following statement (circa 10/27/20):

"We were concerned to learn that some Tarrant County ballots are not able to be scanned properly by Hart Intercivic tabulation machines, as Runbeck Election Services is a certified ballot printer for Hart Intercivic. This election year alone we have printed nearly 100 million ballots, many of which have been the same type of ballot used in Tarrant County, without experiencing any scanning issues. Runbeck Election Services is working with Tarrant County elections officials to investigate if the problem is printing-related or scanning-related. Once the investigation is complete, we will offer our support to all partners and vendors involved to determine the appropriate next steps to ensure that all ballots are properly tabulated."

[illegible]

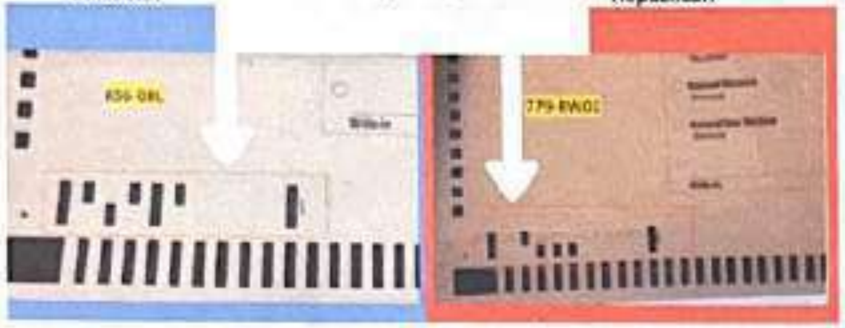
See also: [illegible]

Runbeck Republican Misaligned Ballots

Fulton County Example

Democrat

Republican



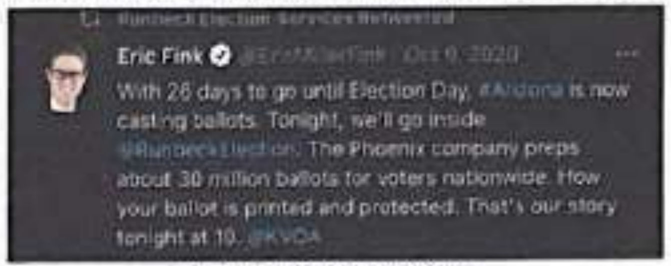
Successfully Scanned

Failed Scanning, Must be Adjudicated

Question: How many of these Runbeck Ballots were Adjudicated for Trump?

[illegible]

RUNBECK Printed 30% of the 2020 Paper Ballots in America

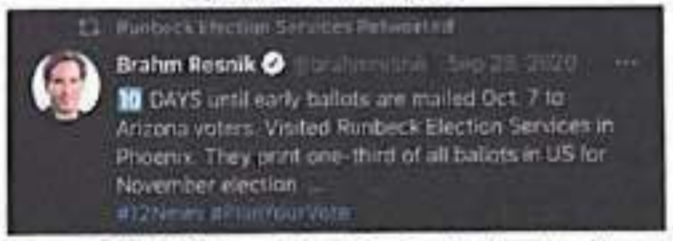


Runbeck Election Services Retweeted

Eric Fink @EricMilesFink · Oct 9, 2020

With 26 days to go until Election Day, #Arizona is now casting ballots. Tonight, we'll go inside @RunbeckElection. The Phoenix company preps about 30 million ballots for voters nationwide. How your ballot is printed and protected. That's our story tonight at 10. @KVOA

https://t.me/CodeMonkeyZ/279

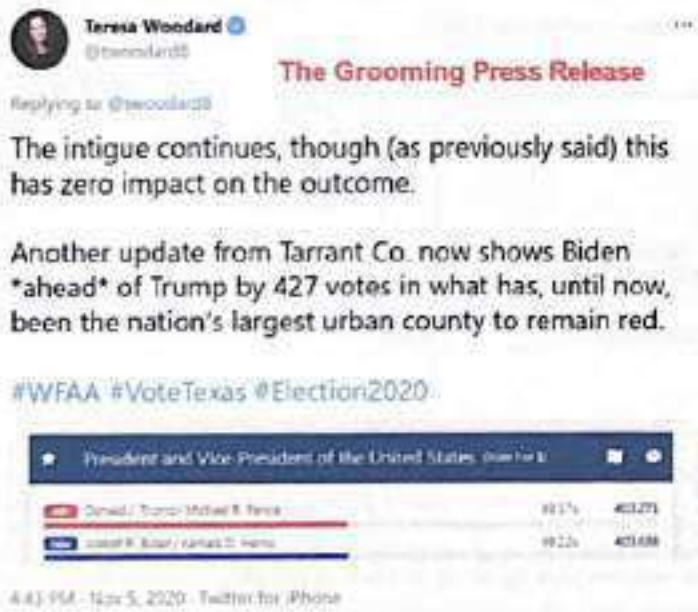


Runbeck Election Services Retweeted

Brahm Resnik @brahmresnik · Sep 28, 2020

10 DAYS until early ballots are mailed Oct. 7 to Arizona voters. Visited Runbeck Election Services in Phoenix. They print one-third of all ballots in US for November election ...
#12News #PlanYourVote

"Did you know that RUNBECK prepped about 30 million ballots nationwide accounting for approximately 30% of all the November paper election ballots?" Ron CodeMonkeyZ



Teresa Woodard @twoodard8

The Grooming Press Release

Replying to @twoodard8

The intigue continues, though (as previously said) this has zero impact on the outcome.

Another update from Tarrant Co. now shows Biden *ahead* of Trump by 427 votes in what has, until now, been the nation's largest urban county to remain red.

#WFAA #VoteTexas #Election2020

President and Vice President of the United States

REP Donald J. Trump / Michael R. Pence	49.17%	403,271
DEM Joseph R. Biden / Kamala D. Harris	49.22%	403,698

4:43 PM · Nov 5, 2020 · Twitter for iPhone

2020 Presidential Results

Tarrant County had a reported **1,185,888** registered voters for the election cycle (Official 2020: 1,216,618*) per the same website,

which meant turnout was 69.51% for this year's presidential election.

As of 6:12 PM CST November 5, 2020

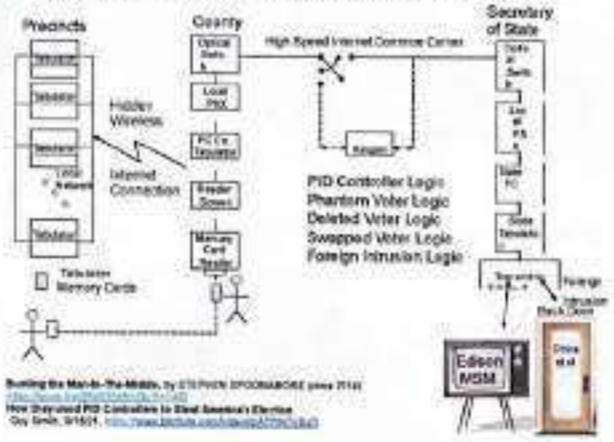
Trump: 403,271 total votes	**Biden: 403,698 total votes**
Absentee: **20,832** votes	Absentee: **34,181** votes
Early In-person: **331,053** votes	Early In-person: **323,384** votes
Election Day In-person: **51,386** votes	Election Day In-person: **46,133** votes

Final 409,741 **votes** (49.09%) The Big Lie Final **411,567** votes (49.31%)
an advantage of 1,826 votes

* **Note there was an increase in registered voters of 30,730 registered voters this year this almost matches the number of adjudicated ballots at 28,016 (Phantom voters??)**

Final **444,286 votes** (53.23%) The Truth Final **377,022** votes (45.17%)
an advantage of 67,264 votes **Trump had an 8.1% margin erased by 1 Intrusion**

Rigged Election Network Architecture



PID Controller Logic
Phantom Voter Logic
Deleted Voter Logic
Swapped Voter Logic
Foreign Intrusion Logic

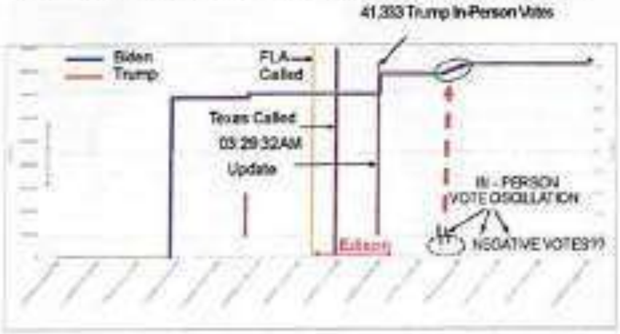
Busting the Man-In-The-Middle, by STEPHEN SPOONAMORE (since 2014)
[illegible]
How they used PID Controllers to Steal America's Election
Guy Smith, 9/1/21, [illegible]

1 Domestic Intruder Swapped Votes in Tarrant County

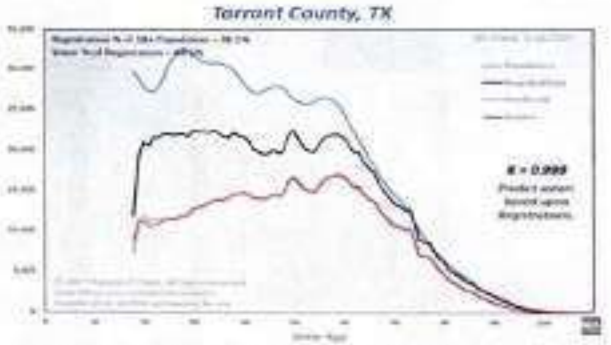
1 Tarrant County Intruder
Lat Long
34.9446 -82.2214 (± 15 feet)
213E Bearden St, Greer, SC, 29651

Date: 11/5/2020 Time: 8:24:38 AM
Swap 34,545 votes from Trump to Biden
Difference ==> 69,090 Lead for Biden
Target: Tarrant County Elections Administrator

Tarrant County Texas Election Fraud 2020

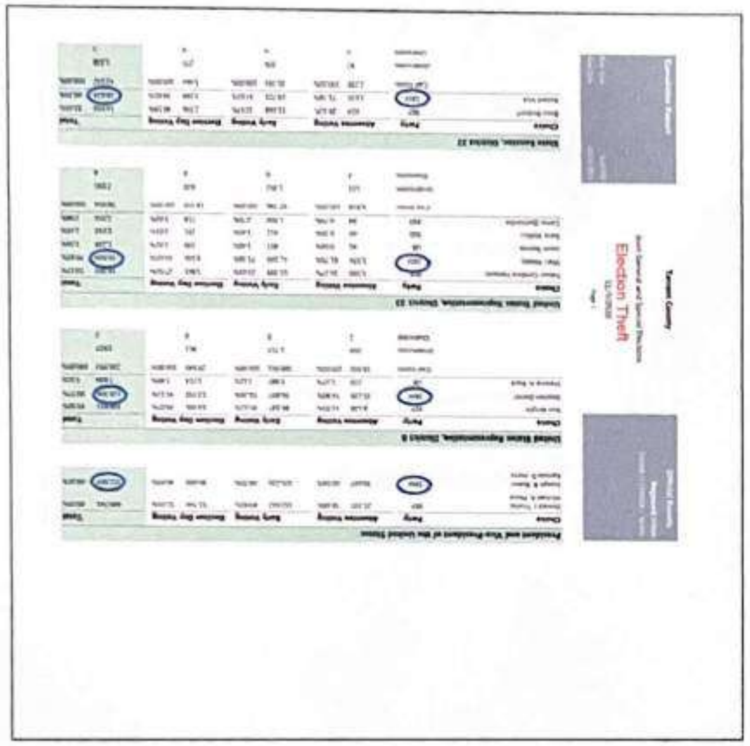


-Immediately after Florida is Called 12:35AM there is a Nationwide shutdown in ENR
-This is called the Edison Zero and it is a rolling 4 hours shutdown
-Texas is then called (1:24 AM) Trump gets 41,333 In-Person votes at 3:29:32 AM
-The Edison Zero in Texas occurs at 5:00:04 AM followed by an alternating sequence of In-Person Votes and Biden pulls slightly ahead for the marginal but definitive 'win'



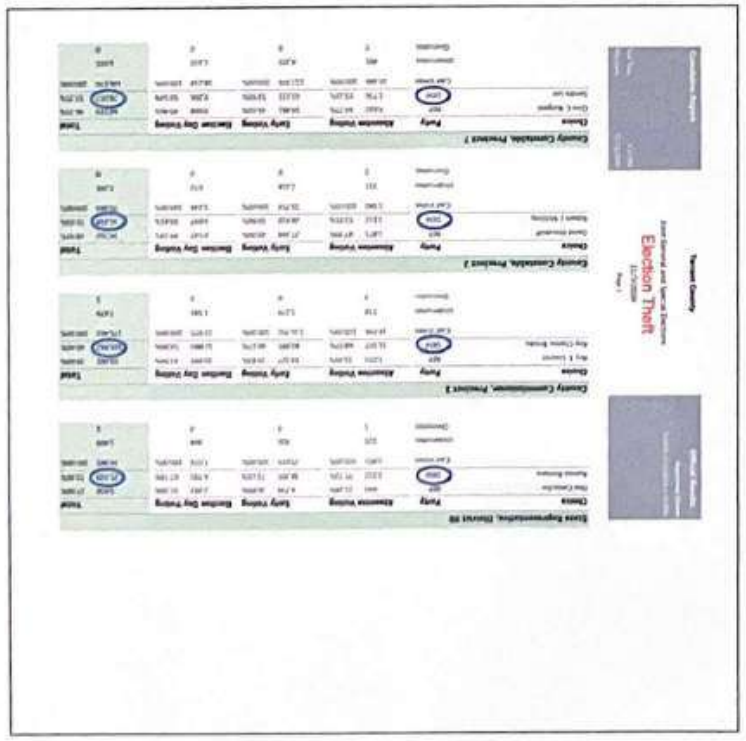
Dr. Frank Predicts 2020 Voter Turnout from Past Voter Registration Data
Collin, Dallas, and Tarrant Counties, 5/18/2021
https://www.youtube.com/watch?v=[illegible] ⟵ Youtube Deleted

No person's vote in Tarrant County was counted. All votes were manipulated by a computer algorithm that produced the result that "Big Brother" wanted



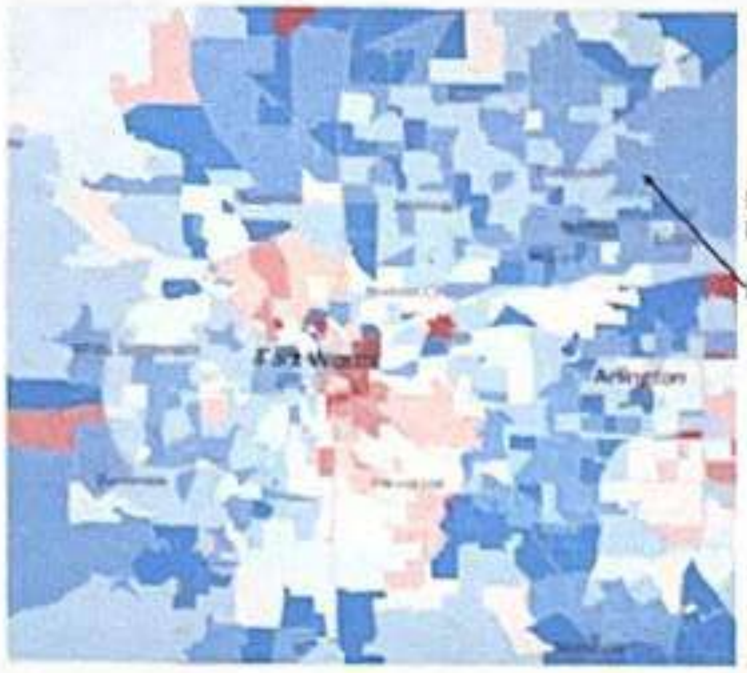
Tarrant County
Joint General and Special Elections
Election Theft
11/3/2020
Page 1

President and Vice President of the United States
[illegible]



Tarrant County
Joint General and Special Elections
Election Theft
Page 1

[illegible]



Likely Phantom Voters In Republican Suburbs

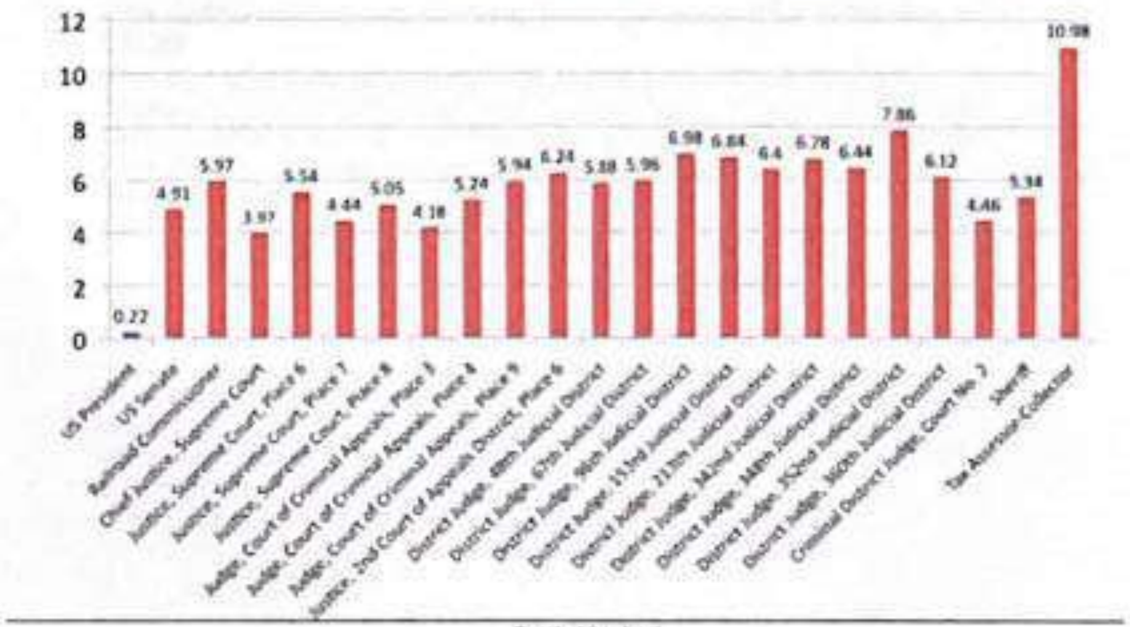
Blue Areas

Many New 2 Party Votes for Biden gained in the suburbs of Fort Worth But Trump still wins those areas
-Seth Keshel
https://cloudgatings.us/videos/seth-keshel-election-fraud-by-the-numbers/

2020
Shift from 2016

November 2020: Tarrant County-Wide Election Results
Displaying Margin of Victory as a %

(Notes: Blue = Democrat won, Red = Republican won
23 races are shown and there are 4 additional Republican judges that ran unopposed for a total of 27 races)



Seth Keshel

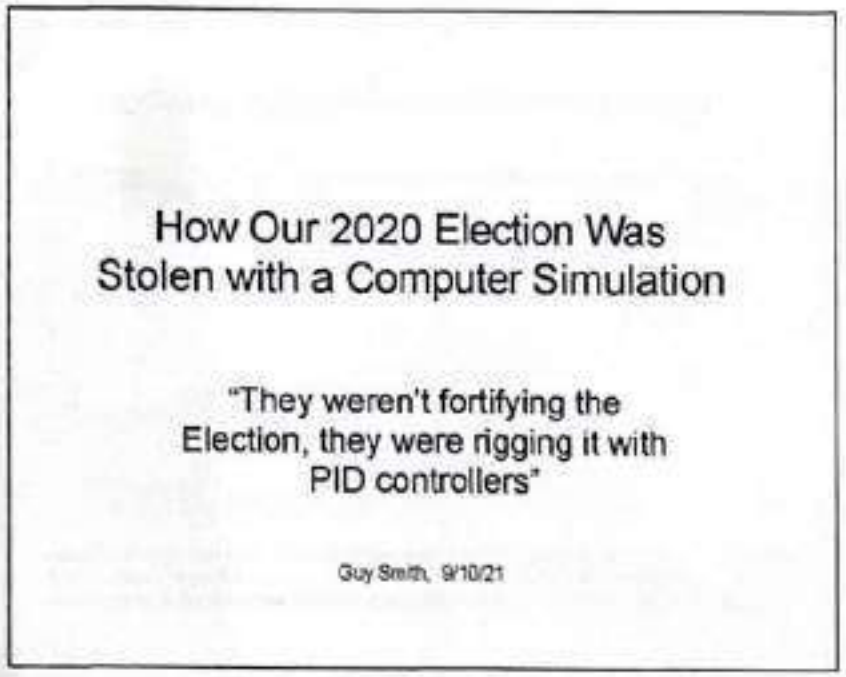
2020 NOVEMBER 3RD GENERAL ELECTION (November)

Why do you think they were updating the TX SOS 2020 Nov 3rd Election Day Voter Turnout Data around the middle of July 2021?

Were they just trying to cover up their crimes?

Conclusion

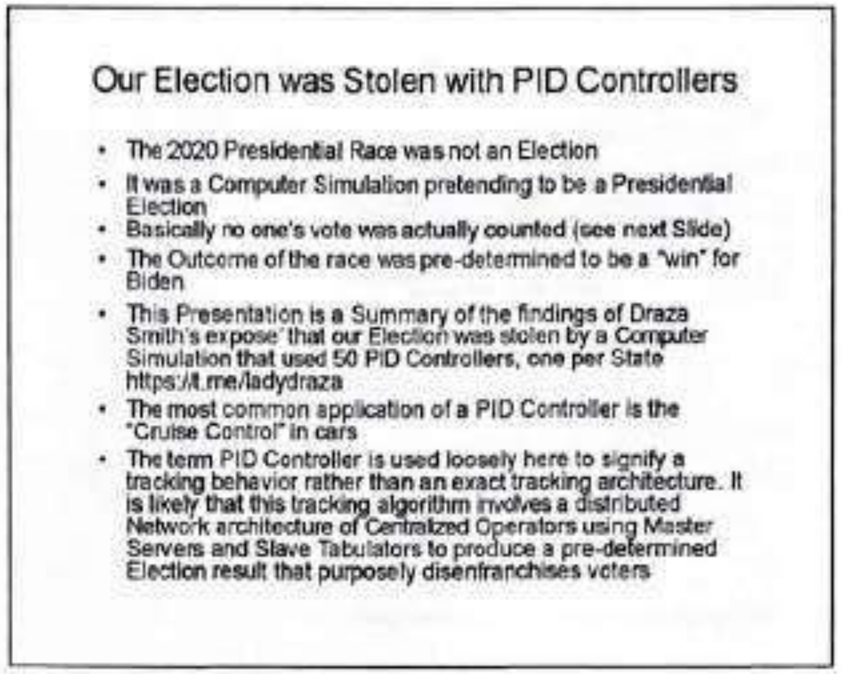
- The dEMS are playing the long game by going after Counties, not States
- The strategy they are using in Williamson & Tarrant is very illuminating as to how they plan to take Texas. They don't flip the County all at once. If you check the down ballots they are mostly Republican with key exceptions. They let most of the Republicans on the ballot win so no one notices what they're doing strategically on the down ballot. Nobody wins a position by accident. It's all carefuly preplanned. The tabulators aren't counting votes, they're simulating them. They go for the Judicial and Law Enforcement positions first. They try to flip Representatives, Judges, Sheriffs, Constables, and Commissioners. Almost exactly what they've done at the Federal Level. They also never miss an opportunity to corrupt Key School Board Positions. After a few cycles Voila the County flips solid Blue. Rinse, Wash, Repeat until you get California. We haven't had a real election in 20 years.
- We need a Full Forensic audit of Tarrant County
- We need a Full Forensic audit of Texas



How Our 2020 Election Was Stolen with a Computer Simulation

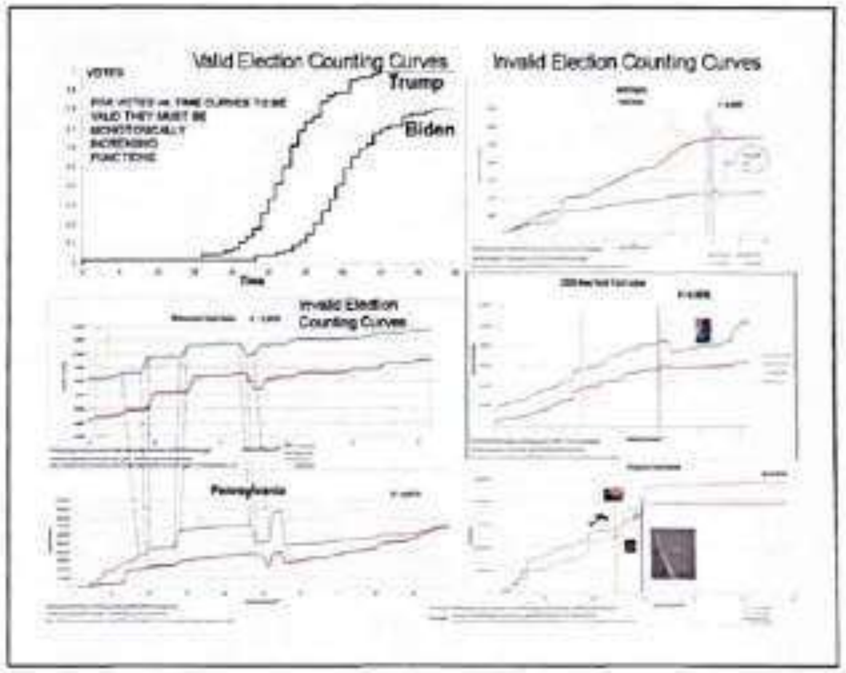
"They weren't fortifying the Election, they were rigging it with PID controllers"

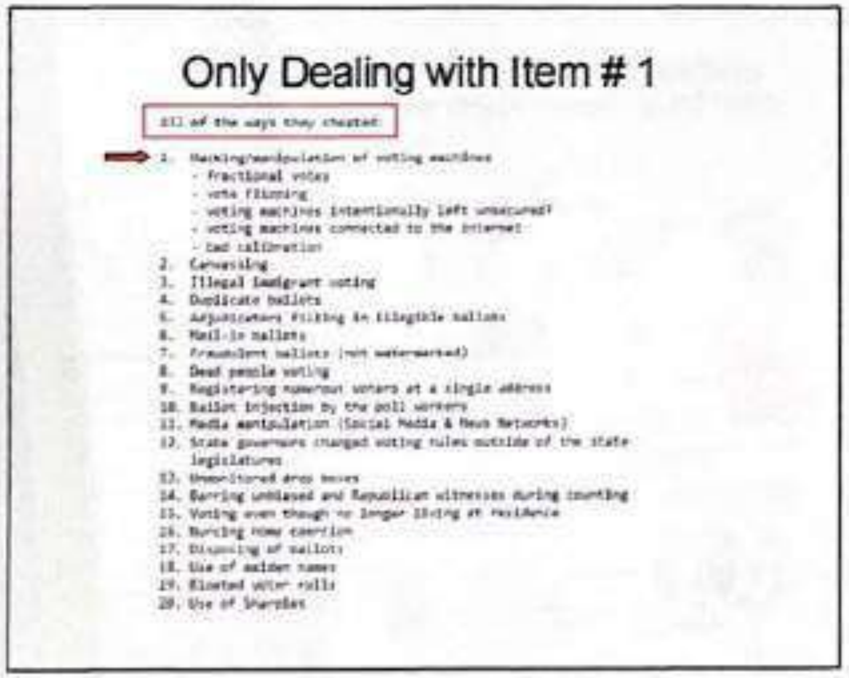
Guy Smith, 9/10/21



Our Election was Stolen with PID Controllers

- The 2020 Presidential Race was not an Election
- It was a Computer Simulation pretending to be a Presidential Election
- Basically no one's vote was actually counted (see next Slide)
- The Outcome of the race was pre-determined to be a "win" for Biden
- This Presentation is a Summary of the findings of Draza Smith's expose' that our Election was stolen by a Computer Simulation that used 50 PID Controllers, one per State https://t.me/ladydraza
- The most common application of a PID Controller is the "Cruise Control" in cars
- The term PID Controller is used loosely here to signify a tracking behavior rather than an exact tracking architecture. It is likely that this tracking algorithm involves a distributed Network architecture of Centralized Operators using Master Servers and Slave Tabulators to produce a pre-determined Election result that purposely disenfranchises voters

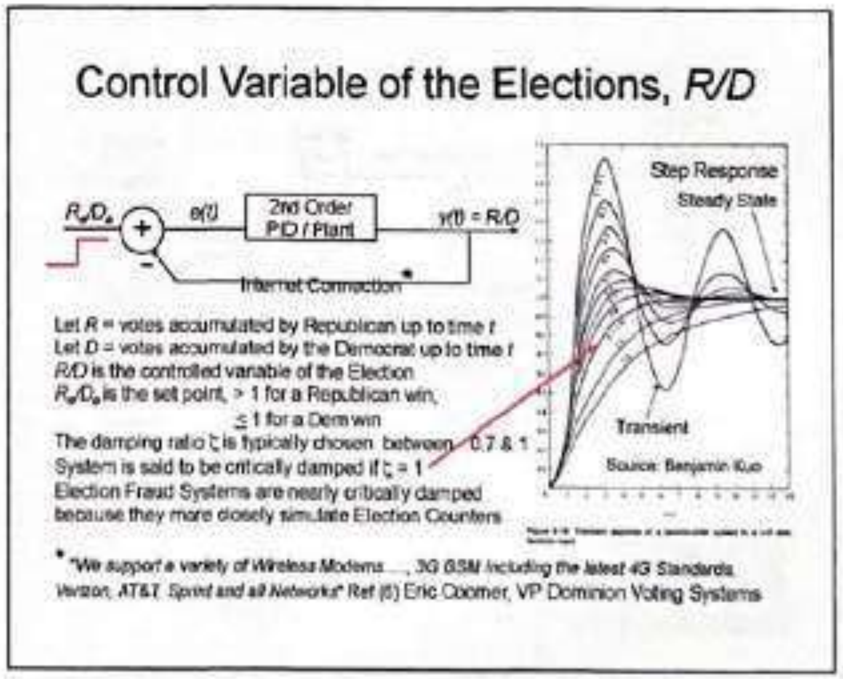




Only Dealing with Item # 1

All of the ways they cheated

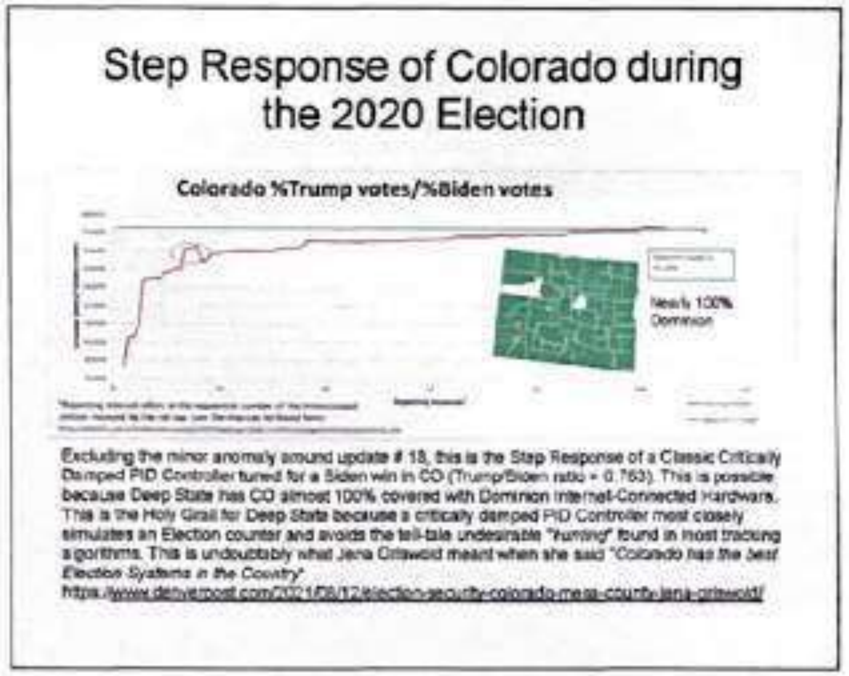
1. Hacking/manipulation of voting machines
   - fractional votes
   - vote flipping
   - voting machines intentionally left unsecured!
   - voting machines connected to the internet
   - bad calibration
2. Canvassing
3. Illegal Immigrant voting
4. Duplicate ballots
5. Adjudicators filling in illegible ballots
6. Mail-in ballots
7. Fraudulent ballots (not watermarked)
8. Dead people voting
9. Registering numerous voters at a single address
10. Ballot injection by the poll workers
11. Media manipulation (Social Media & News Networks)
12. State governors changed voting rules outside of the state legislatures
13. Unmonitored drop boxes
14. Barring unbiased and Republican witnesses during counting
15. Voting even though no longer living at residence
16. Nursing home coercion
17. Disposing of ballots
18. Use of maiden names
19. Bloated voter rolls
20. Use of Sharpies



Control Variable of the Elections, *R/D*

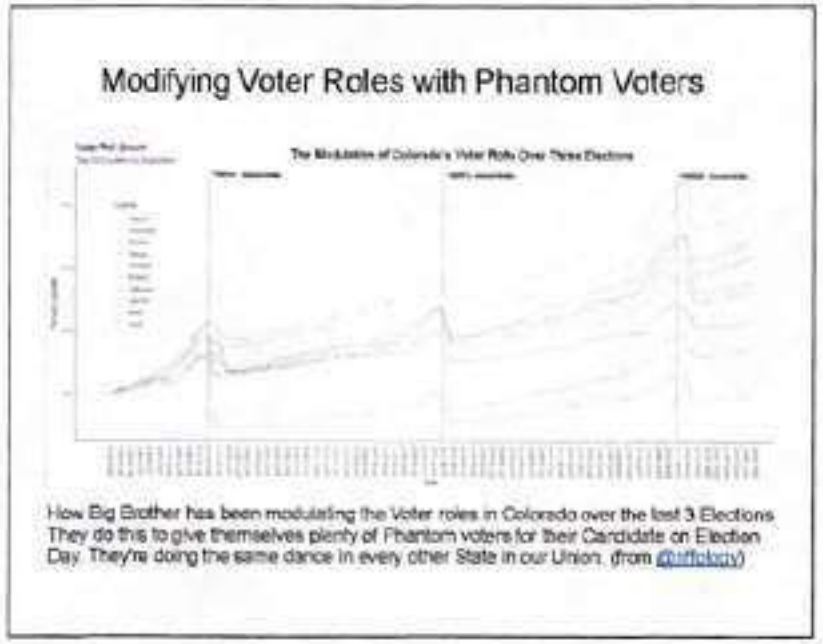
Let R = votes accumulated by Republican up to time t
Let D = votes accumulated by the Democrat up to time t
R/D is the controlled variable of the Election
R_o/D_o is the set point, > 1 for a Republican win,
≤ 1 for a Dem win
The damping ratio ζ is typically chosen between 0.7 & 1
System is said to be critically damped if $\zeta = 1$
Election Fraud Systems are nearly critically damped because they more closely simulate Election Counters

* *"We support a variety of Wireless Modems..., 3G GSM Including the latest 4G Standards Verizon, AT&T, Sprint and all Networks"* Ref (6) Eric Coomer, VP Dominion Voting Systems



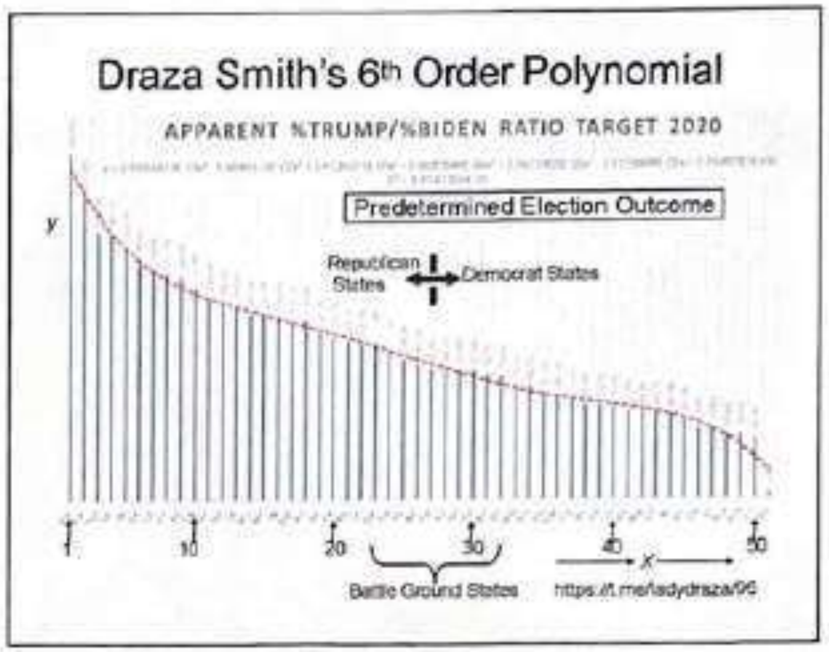
Step Response of Colorado during the 2020 Election

Excluding the minor anomaly around update # 18, this is the Step Response of a Classic Critically Damped PID Controller tuned for a Biden win in CO (Trump/Biden ratio = 0.763). This is possible because Deep State has CO almost 100% covered with Dominion Internet-Connected Hardware. This is the Holy Grail for Deep State because a critically damped PID Controller most closely simulates an Election counter and avoids the tell-tale undesirable *"hunting"* found in most tracking algorithms. This is undoubtably what Jena Griswold meant when she said *"Colorado has the best Election Systems in the Country"*.
https://www.denverpost.com/2021/08/12/election-security-colorado-mesa-county-jena-griswold/



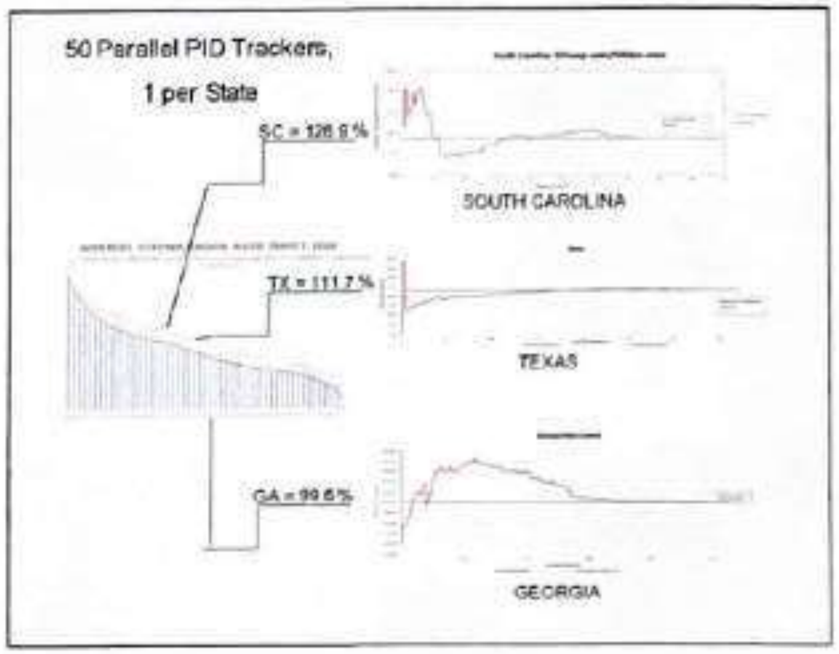
Modifying Voter Roles with Phantom Voters

How Big Brother has been modulating the Voter roles in Colorado over the last 3 Elections They do this to give themselves plenty of Phantom voters for their Candidate on Election Day. They're doing the same dance in every other State in our Union. (from @iffolcry)

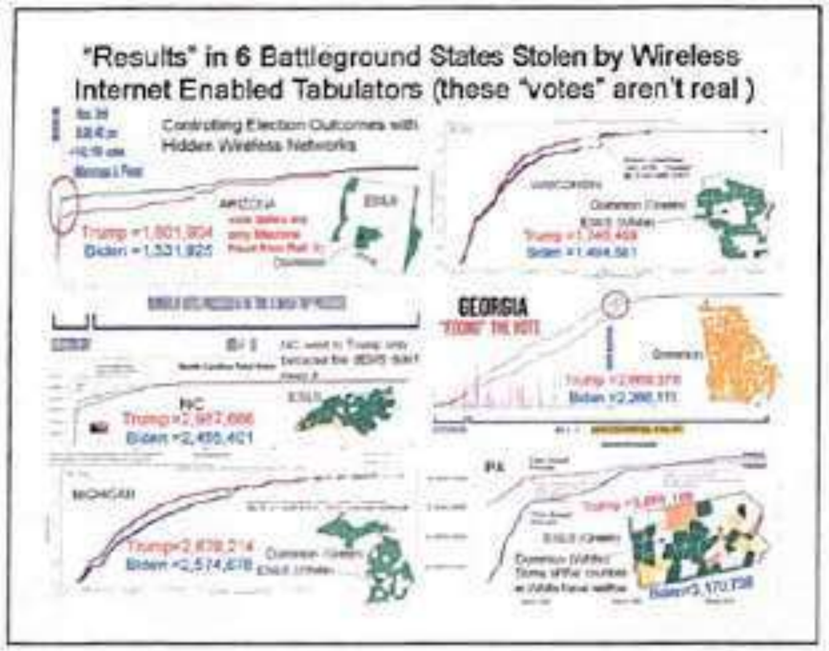


Draza Smith's 6th Order Polynomial

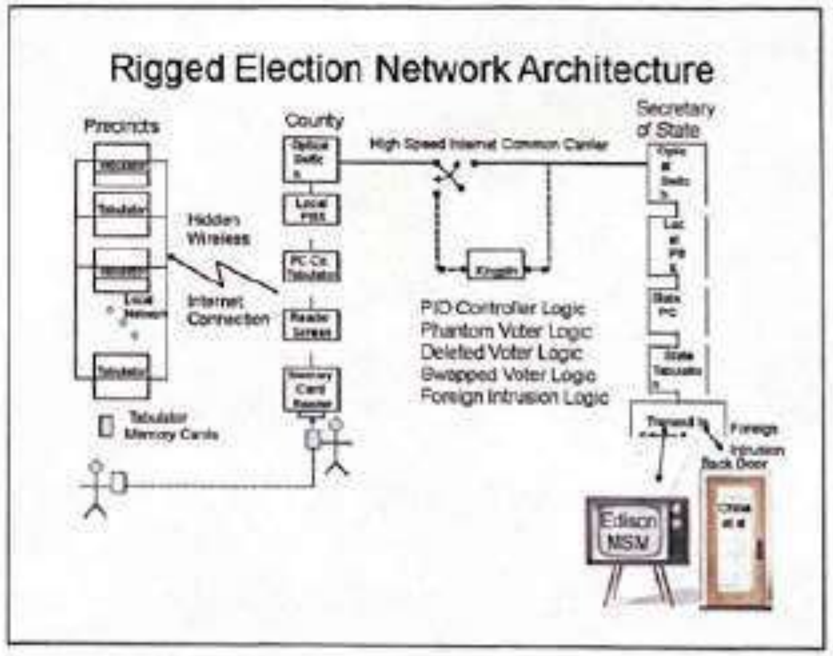
https://t.me/ladydraza/96



50 Parallel PID Trackers, 1 per State

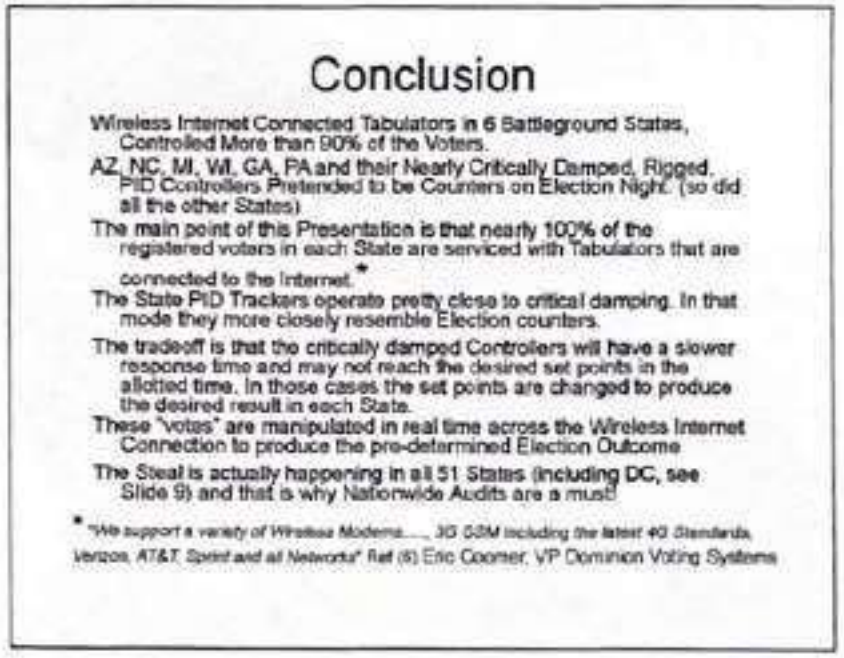


"Results" in 6 Battleground States Stolen by Wireless Internet Enabled Tabulators (these "votes" aren't real)



Rigged Election Network Architecture

PID Controller Logic
Phantom Voter Logic
Deleted Voter Logic
Swapped Voter Logic
Foreign Intrusion Logic



Conclusion

Wireless Internet Connected Tabulators in 6 Battleground States, Controlled More than 90% of the Voters.

AZ, NC, MI, WI, GA, PA and their Nearly Critically Damped, Rigged, PID Controllers Pretended to be Counters on Election Night. (so did all the other States)

The main point of this Presentation is that nearly 100% of the registered voters in each State are serviced with Tabulators that are connected to the Internet.*

The State PID Trackers operate pretty close to critical damping. In that mode they more closely resemble Election counters.

The tradeoff is that the critically damped Controllers will have a slower response time and may not reach the desired set points in the allotted time. In those cases the set points are changed to produce the desired result in each State.

These "votes" are manipulated in real time across the Wireless Internet Connection to produce the pre-determined Election Outcome

The Steal is actually happening in all 51 States (including DC, see Slide 9) and that is why Nationwide Audits are a must!

* *"We support a variety of Wireless Modems...., 3G GSM including the latest 4G Standards, Verizon, AT&T, Sprint and all Networks"* Ref (6) Eric Coomer, VP Dominion Voting Systems

Summary

So This is How They Stole the 2020 Election
They know the outcome before hand. In the Early **Voting**, the Trump votes are likely the first to be discarded. Run the Tracking Simulation (i.e., a *'Cruise Control'* type algorithm) to its predetermined setpoints deleting as many Trump votes as you can in Real-Time while also adding necessary ghost votes for Biden from an almost infinite supply of fake *'registered'* Independents. **After the** Election, assign Phantom names and addresses to the ghost votes. If any of the ghost votes are actually real people they'll never **be contacted** by either Party because they are Independents. Now delete all the unnecessary Phantom voters from the registration roles before any Auditor notices. Then hide all the Phantom voters included in the rigged counts of each State by down-streaming back to the Tabulators **LONG AFTER THE POLLS ARE CLOSED**. Be careful to spread them thinly by selecting their addresses randomly over a thousand Precincts. If anyone notices in a particular Precinct call it a *"Glitch"* or a *"Human error"*. Follow that statement with *"Well it wasn't enough to change the outcome of the Election"*.

References

1) **Draza Smith: Election Fraud on Cruise Control?** [illegible]

2) **Plane to Death 9/4** [illegible]

3) **Mike Lindell's Cyber Symposium 8/10/21** [illegible]

4) **Tuning Optimal PID Controllers for Discrete-time Systems by Election Campaign Optimization Algorithm**, Wang, Li, et al. [illegible] Conference, [illegible]

5) Draza Smith's Telegram Page [illegible]

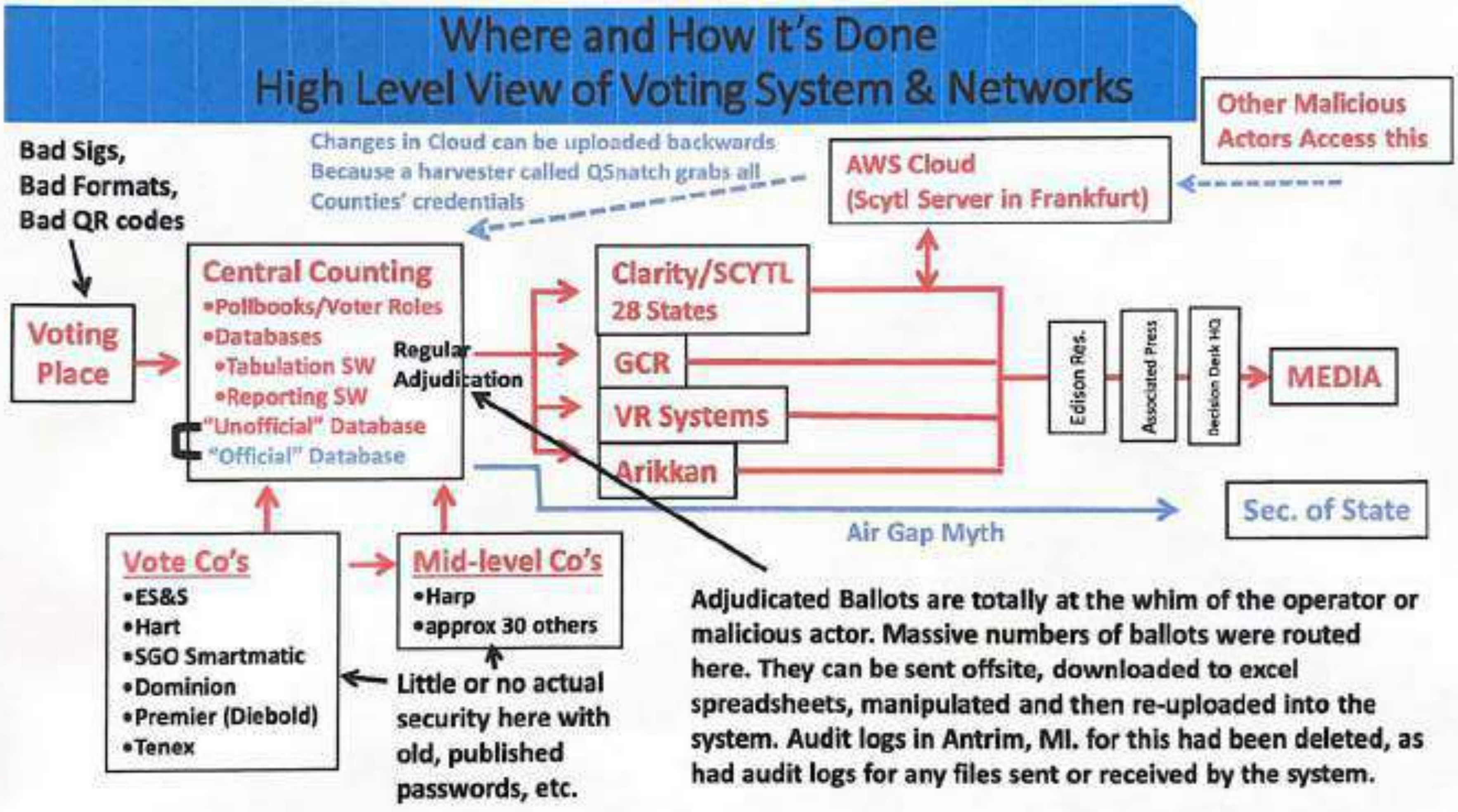
6) The [illegible] "Shifting Paradox", Professor Clements [illegible] https://rumble.com/[illegible]

7) Automatic Control Systems 4th ed., Benjamin C. Kuo, 1982, Prentice Hall pg. 235, ISBN 0-13-[illegible]

8) **MUST SEE: Stunning Video Explaining How, Why And Who Stole Election** [illegible]

9) **Stealing the Election In Plain Sight, by STEPHEN SPOONAMORE** [illegible] [illegible]

COMPONENTS



Where and How It's Done
High Level View of Voting System & Networks

Bad Sigs,
Bad Formats,
Bad QR codes

Voting Place

Central Counting
- Pollbooks/Voter Roles
- Databases
  - Tabulation SW
  - Reporting SW
- "Unofficial" Database
- "Official" Database

Regular
Adjudication

Changes in Cloud can be uploaded backwards
Because a harvester called QSnatch grabs all
Counties' credentials

AWS Cloud
(Scytl Server in Frankfurt)

Other Malicious
Actors Access this

Clarity/SCYTL
28 States

GCR

VR Systems

Arikkan

Edison Res.

Associated Press

Decision Desk HQ

MEDIA

Air Gap Myth

Sec. of State

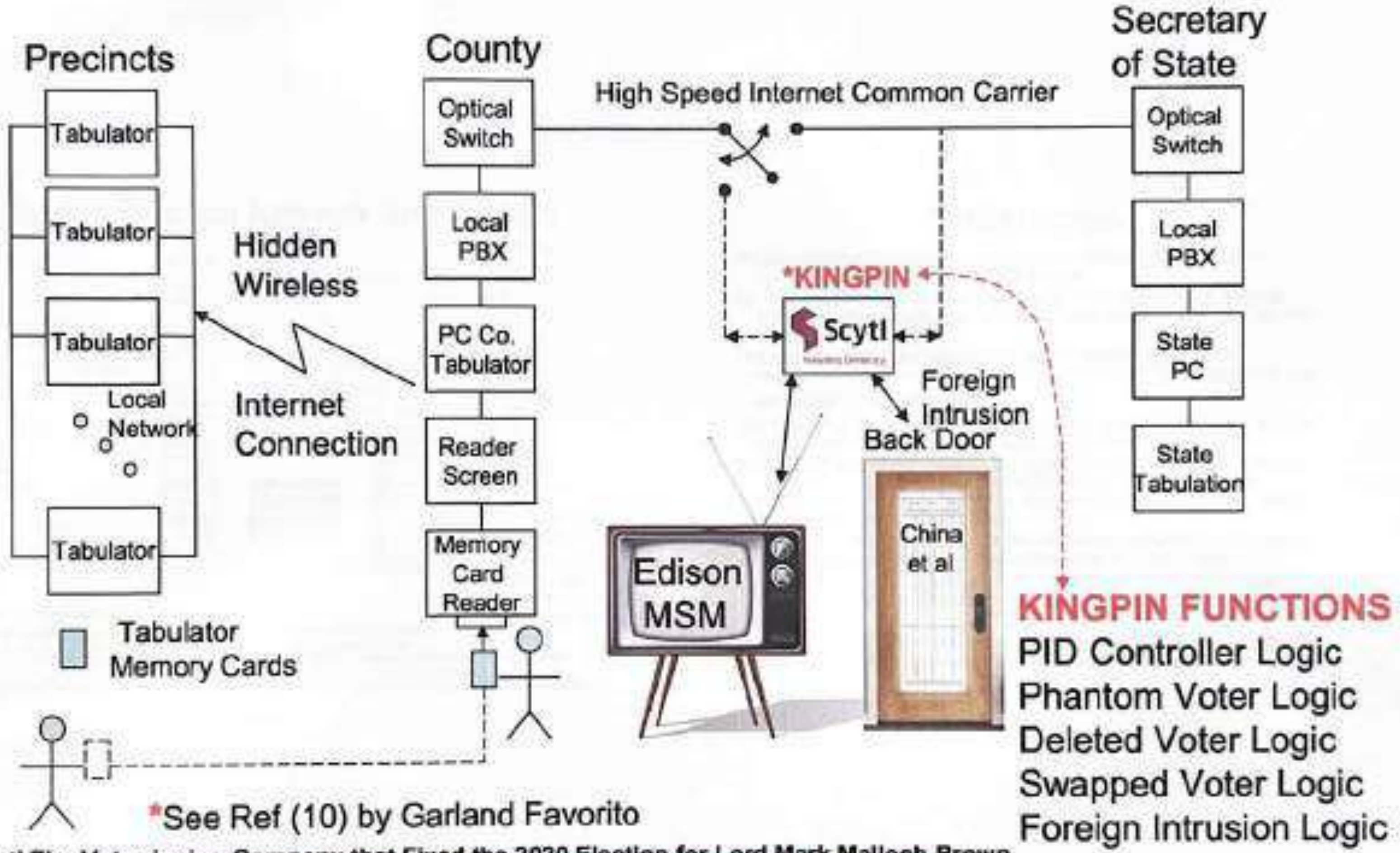
Vote Co's
- ES&S
- Hart
- SGO Smartmatic
- Dominion
- Premier (Diebold)
- Tenex

Mid-level Co's
- Harp
- approx 30 others

Little or no actual security here with old, published passwords, etc.

Adjudicated Ballots are totally at the whim of the operator or malicious actor. Massive numbers of ballots were routed here. They can be sent offsite, downloaded to excel spreadsheets, manipulated and then re-uploaded into the system. Audit logs in Antrim, MI. for this had been deleted, as had audit logs for any files sent or received by the system.

Rigged Election Network Architecture



Precincts

Tabulator
Tabulator
Tabulator
Local Network
Tabulator

Tabulator Memory Cards

Hidden Wireless

Internet Connection

County

Optical Switch
Local PBX
PC Co. Tabulator
Reader Screen
Memory Card Reader

High Speed Internet Common Carrier

*KINGPIN

Scytl

Foreign Intrusion Back Door

Edison MSM

China et al

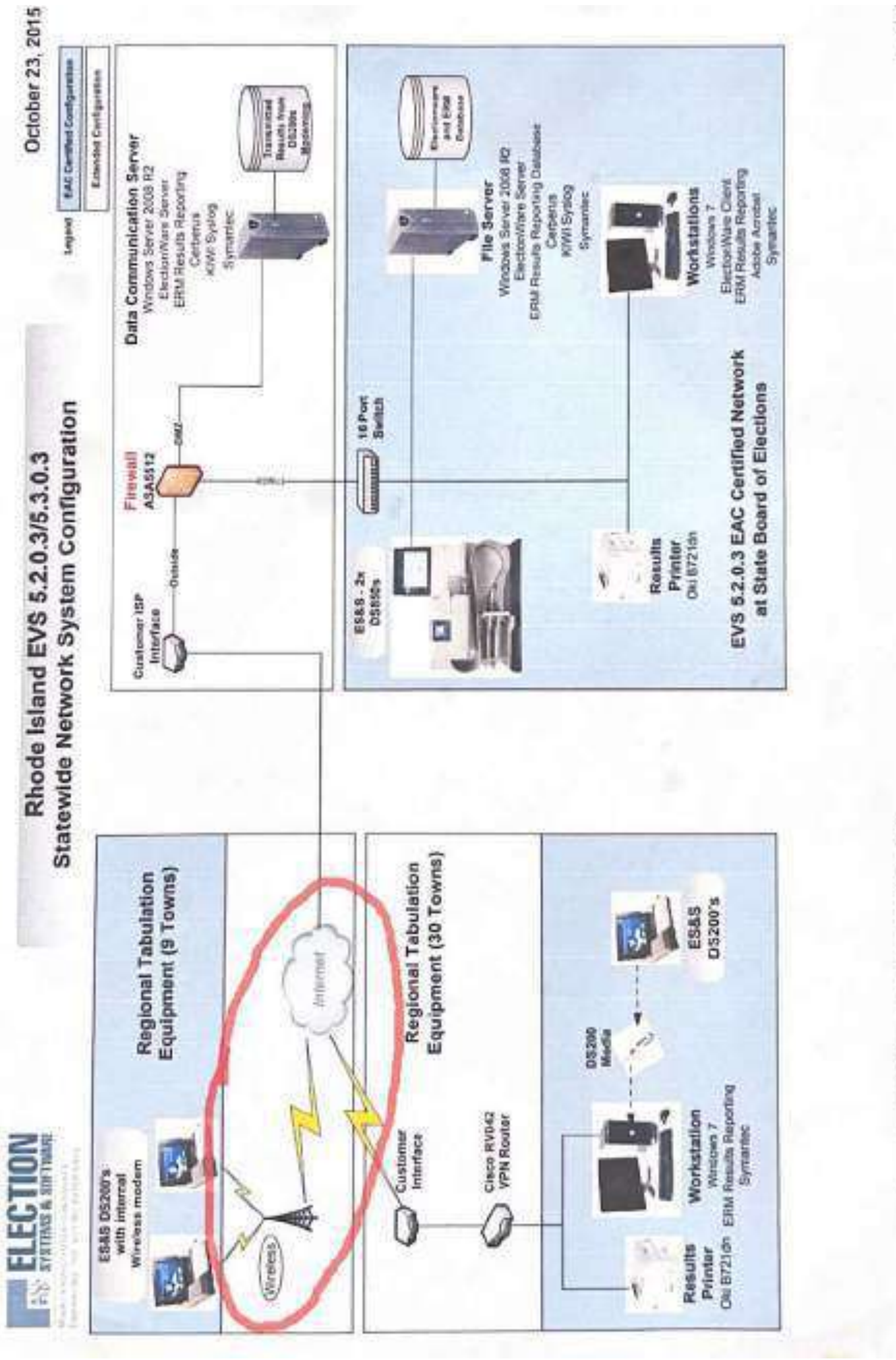
Secretary of State

Optical Switch
Local PBX
State PC
State Tabulation

KINGPIN FUNCTIONS
PID Controller Logic
Phantom Voter Logic
Deleted Voter Logic
Swapped Voter Logic
Foreign Intrusion Logic

*See Ref (10) by Garland Favorito

Scytl The Vote-rigging Company that Fixed the 2020 Election for Lord Mark Malloch-Brown
https://aim4truth.org/2020/11/30/scytl-the-vote-rigging-company-that-fixed-the-2020-election/
7:00 **Georgia - A Close Look at the Data and Events of the General Election - Chapter 1**, "Data Integrity Group" 12/24/20
https://rumble.com/vc5nk7-georgia-a-close-look-at-the-data-and-events-of-the-general-election-chapter.html
Rep. Louie Gohmert on reports of a Scytl server raid in Germany, 11/13/20, https://www.youtube.com/watch?v=LyyQgeRJC58



Rhode Island EVS 5.2.0.3/5.3.0.3 Statewide Network System Configuration

October 23, 2015

https://www.citizen.org/wp-content/uploads/migration/diagram_smooth_circle.jpg

Page 1 of

FROM MICHIGAN CONTRACTS

MICHIGAN VERITY CONFIGURATION

The Contractor's Verity configuration for the State of Michigan supports a seamless workflow and accommodates the varied needs of the State's counties and local jurisdictions.

VERITY VOTING SYSTEM HARDWARE

Precinct Based Scanning Tabulator – Verity Scan

For use at polling places, Verity Scan is a digital scanning solution for paper ballots. After marking a paper ballot, the voter feeds it directly into Verity Scan. Scan uses a touchscreen interface based on EAC/AIGA Design for Democracy styles.

Verity Scan can print ballot count totals or tabulated results in the polling place. The ballot image is stored as a Cast Vote Record (CVR) on a Verity vDrive flash memory device that can be read by the Verity Count tabulation and reporting software. Verity Scan includes a compact and durable integrated storage case for transportation and storage.

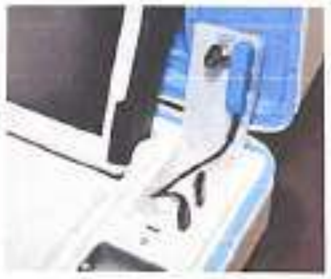
Verity Scan with Relay (Option)

For Michigan, Verity Scan is available with the Relay option, which enables electronic transmission of cast vote records directly from the device to the central election office. Relay automatically starts the data transmission process when polls close and requires no technical engagement by poll workers.

Adaptable: Relay utilizes broadband technology in the form of secure, COTS modems that are compatible with local jurisdictions' preferred telecommunications carrier.

COTS mobile broadband modem with USB connectivity.

Available for both CDMA and GSM carriers.

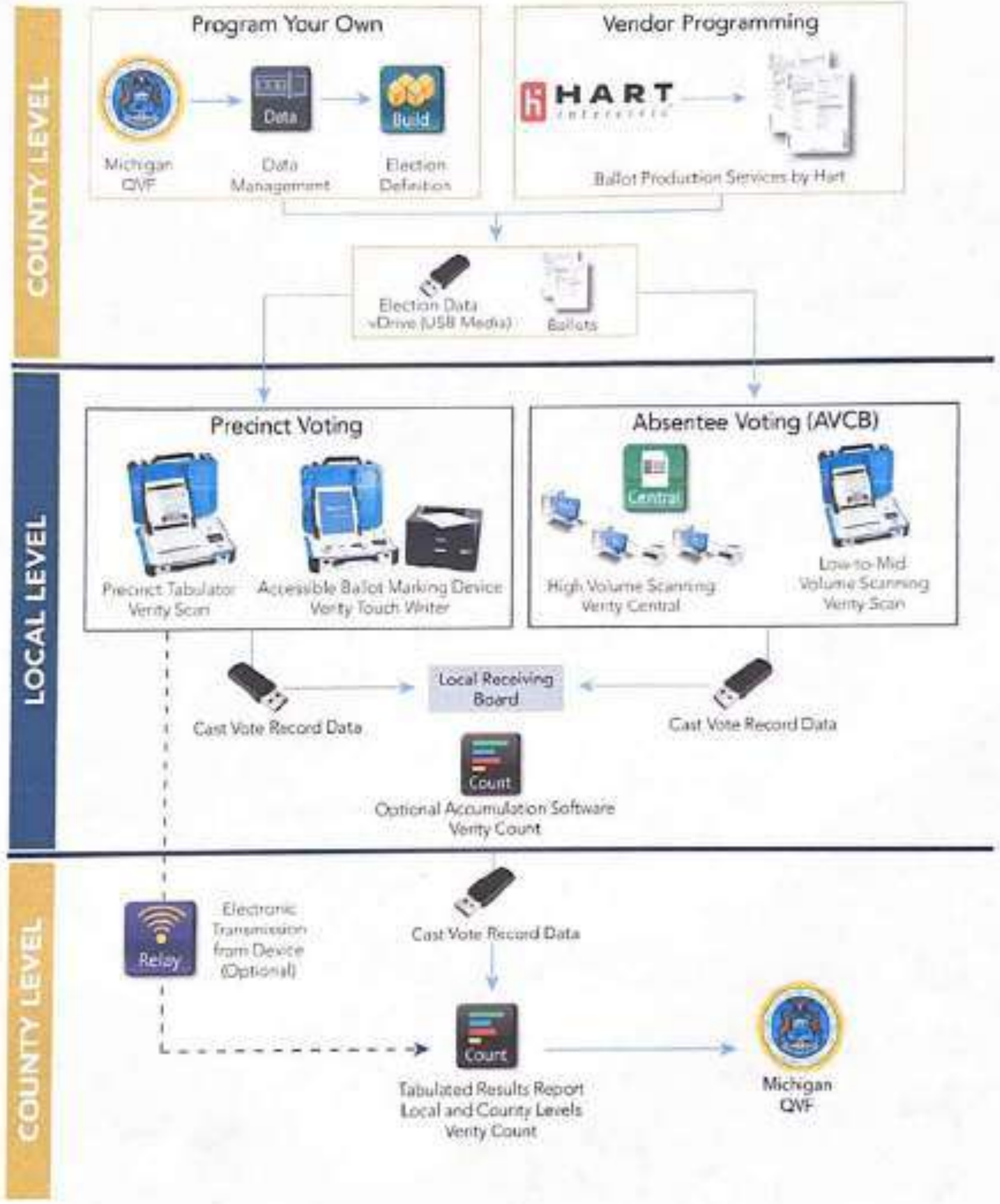


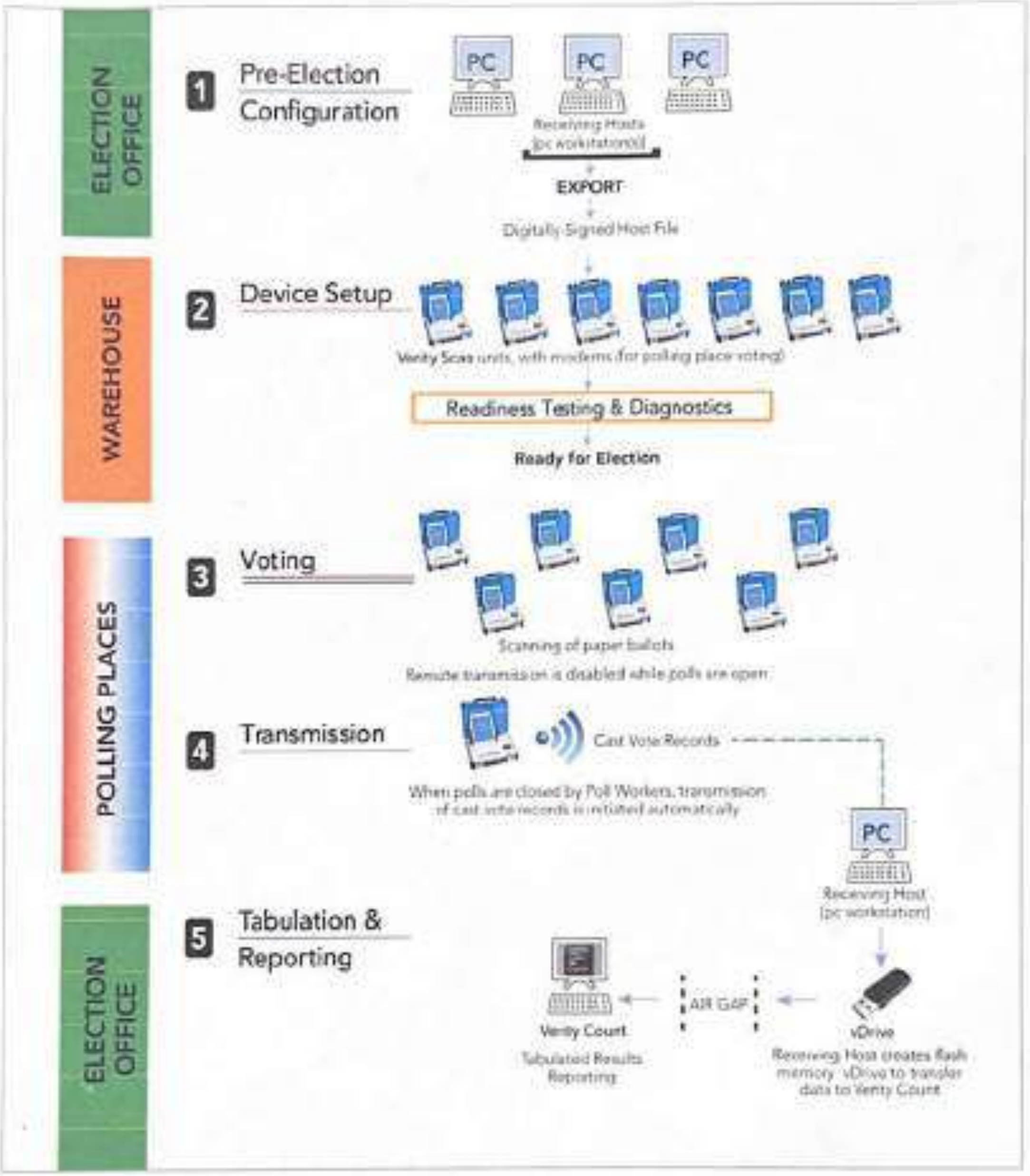
Verity Scan's vDrive/USB/Modem compartment, open, showing modem with USB connection and vDrive.

Verity Scan's vDrive/USB/Modem compartment, closed and locked.

Secure. Like other Verity components, Relay includes Hart and Verity FIPS-compliant encryption and digital signatures for authentication.

Automatic transmission of data. After the poll worker closes the polls and prints a tally, the data transmission process automatically launches.

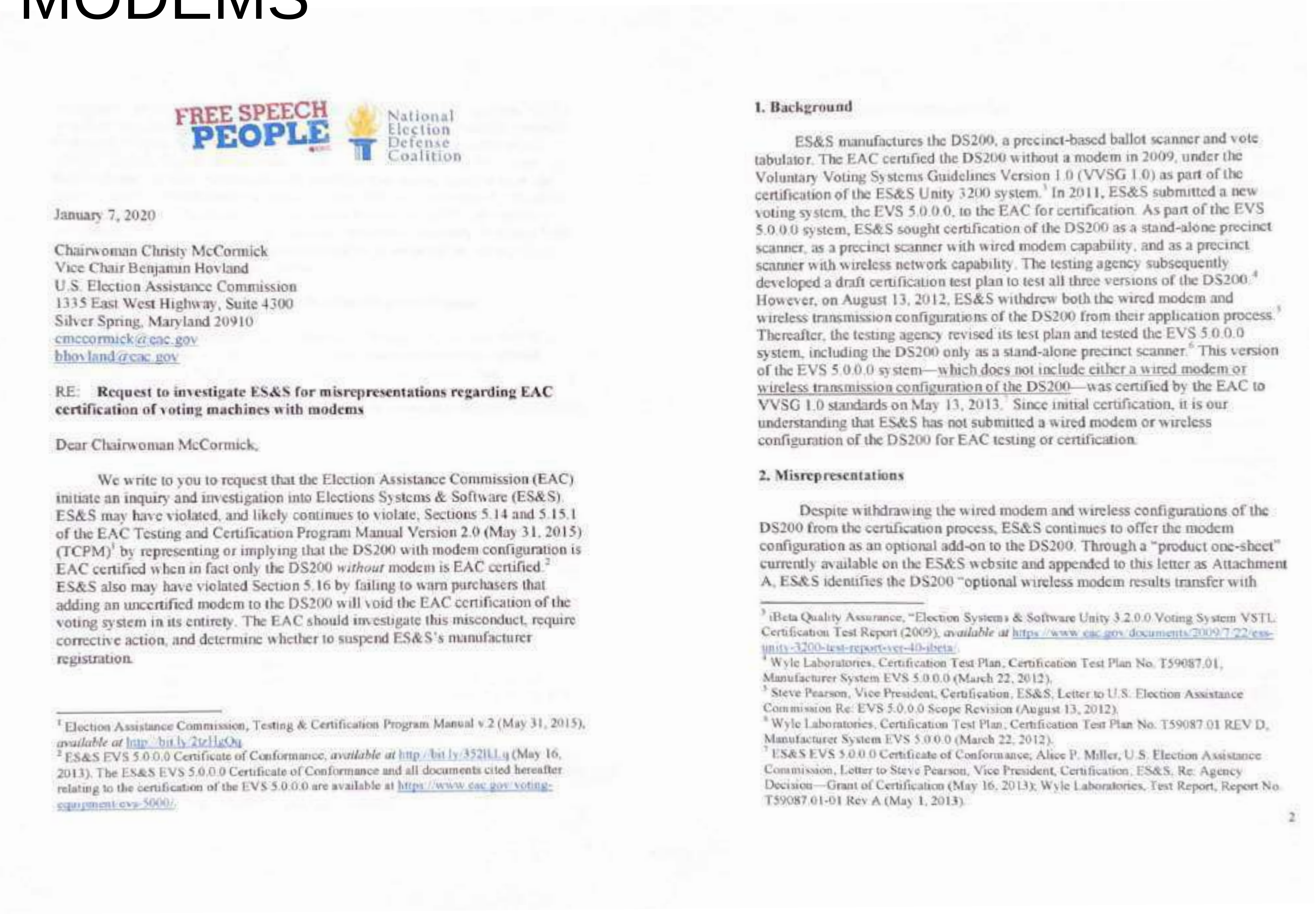

COUNTY LEVEL
Program Your Own
Michigan QVF
Data
Data Management
Build
Election Definition
Vendor Programming
HART intercivic
Ballot Production Services by Hart
Election Data vDrive (USB Media)
Ballots
LOCAL LEVEL
Precinct Voting
Precinct Tabulator Verity Scan
Accessible Ballot Marking Device Verity Touch Writer
Absentee Voting (AVCB)
Central
High Volume Scanning Verity Central
Low-to-Mid Volume Scanning Verity Scan
Cast Vote Record Data
Local Receiving Board
Cast Vote Record Data
Count
Optional Accumulation Software Verity Count
COUNTY LEVEL
Relay
Electronic Transmission from Device (Optional)
Cast Vote Record Data
Count
Tabulated Results Report Local and County Levels Verity Count
Michigan QVF


ELECTION OFFICE
1 Pre-Election Configuration
PC
PC
PC
Receiving Hosts (pc workstation(s))
EXPORT
Digitally Signed Host File
WAREHOUSE
2 Device Setup
Verity Scan units, with modems (for polling place voting)
Readiness Testing & Diagnostics
Ready for Election
POLLING PLACES
3 Voting
Scanning of paper ballots
Remote transmission is disabled while polls are open
4 Transmission
Cast Vote Records
When polls are closed by Poll Workers, transmission of cast vote records is initiated automatically
PC
Receiving Host (pc workstation)
ELECTION OFFICE
5 Tabulation & Reporting
Verity Count
Tabulated Results Reporting
AIR GAP
vDrive
Receiving Host creates flash memory vDrive to transfer data to Verity Count

VERITY REMOTE TRANSMISSION WORKFLOW

Remote transmission functionality is integrated into each step of the election process, from pre-election preparation through Election Day through post-election tabulation and reporting.

MODEMS



FREE SPEECH PEOPLE

National Election Defense Coalition

January 7, 2020

Chairwoman Christy McCormick
Vice Chair Benjamin Hovland
U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, Maryland 20910
cmccormick@eac.gov
bhovland@eac.gov

RE: **Request to investigate ES&S for misrepresentations regarding EAC certification of voting machines with modems**

Dear Chairwoman McCormick,

We write to you to request that the Election Assistance Commission (EAC) initiate an inquiry and investigation into Elections Systems & Software (ES&S). ES&S may have violated, and likely continues to violate, Sections 5.14 and 5.15.1 of the EAC Testing and Certification Program Manual Version 2.0 (May 31, 2015) (TCPM)[1] by representing or implying that the DS200 with modem configuration is EAC certified when in fact only the DS200 *without* modem is EAC certified.[2] ES&S also may have violated Section 5.16 by failing to warn purchasers that adding an uncertified modem to the DS200 will void the EAC certification of the voting system in its entirety. The EAC should investigate this misconduct, require corrective action, and determine whether to suspend ES&S's manufacturer registration.

[1] Election Assistance Commission, Testing & Certification Program Manual v.2 (May 31, 2015), *available at* http://bit.ly/2tzHgOq

[2] ES&S EVS 5.0.0.0 Certificate of Conformance, *available at* http://bit.ly/352lkLq (May 16, 2013). The ES&S EVS 5.0.0.0 Certificate of Conformance and all documents cited hereafter relating to the certification of the EVS 5.0.0.0 are available at https://www.eac.gov/voting-equipment/evs-5000/.

1. Background

ES&S manufactures the DS200, a precinct-based ballot scanner and vote tabulator. The EAC certified the DS200 without a modem in 2009, under the Voluntary Voting Systems Guidelines Version 1.0 (VVSG 1.0) as part of the certification of the ES&S Unity 3200 system.[3] In 2011, ES&S submitted a new voting system, the EVS 5.0.0.0, to the EAC for certification. As part of the EVS 5.0.0.0 system, ES&S sought certification of the DS200 as a stand-alone precinct scanner, as a precinct scanner with wired modem capability, and as a precinct scanner with wireless network capability. The testing agency subsequently developed a draft certification test plan to test all three versions of the DS200.[4] However, on August 13, 2012, ES&S withdrew both the wired modem and wireless transmission configurations of the DS200 from their application process.[5] Thereafter, the testing agency revised its test plan and tested the EVS 5.0.0.0 system, including the DS200 only as a stand-alone precinct scanner.[6] This version of the EVS 5.0.0.0 system—which does not include either a wired modem or wireless transmission configuration of the DS200—was certified by the EAC to VVSG 1.0 standards on May 13, 2013.[7] Since initial certification, it is our understanding that ES&S has not submitted a wired modem or wireless configuration of the DS200 for EAC testing or certification.

2. Misrepresentations

Despite withdrawing the wired modem and wireless configurations of the DS200 from the certification process, ES&S continues to offer the modem configuration as an optional add-on to the DS200. Through a "product one-sheet" currently available on the ES&S website and appended to this letter as Attachment A, ES&S identifies the DS200 "optional wireless modem results transfer with

[3] iBeta Quality Assurance, "Election Systems & Software Unity 3.2.0.0 Voting System VSTL Certification Test Report (2009), *available at* https://www.eac.gov/documents/2009/7/22/ess-unity-3200-test-report-ver-40-ibeta/.

[4] Wyle Laboratories, Certification Test Plan, Certification Test Plan No. T59087.01, Manufacturer System EVS 5.0.0.0 (March 22, 2012).

[5] Steve Pearson, Vice President, Certification, ES&S, Letter to U.S. Election Assistance Commission Re: EVS 5.0.0.0 Scope Revision (August 13, 2012).

[6] Wyle Laboratories, Certification Test Plan, Certification Test Plan No. T59087.01 REV D, Manufacturer System EVS 5.0.0.0 (March 22, 2012).

[7] ES&S EVS 5.0.0.0 Certificate of Conformance; Alice P. Miller, U.S. Election Assistance Commission, Letter to Steve Pearson, Vice President, Certification, ES&S, Re: Agency Decision—Grant of Certification (May 16, 2013); Wyle Laboratories, Test Report, Report No T59087.01-01 Rev A (May 1, 2013).

encryption" as an example of the scanner's "comprehensive" key features.[8] ES&S also distributes the one-sheet, past versions of the one-sheet, and similar materials to potential buyers, including Cuyahoga County, Ohio (2018),[9] South Dakota (2018),[10] Tioga County, Pennsylvania (2019),[11] North Carolina (2019),[12] and Boone County (2019).[13] ES&S also has produced and disseminated at least one other similar DS200 brochure, appended to this letter as Attachment B, including to Grand Traverse, Michigan.[14] It is our understanding that ES&S has produced and distributed these one-sheets and similar promotional materials, featuring both the "EAC certified" logo and the wireless modem as an available option, since approximately 2016, and possibly earlier.

3. Violations of the Testing and Certification Program Manual

ES&S's advertisements violate Sections 5.14 and 5.15.1 of the TCPM by falsely stating or implying that the DS200, when purchased with the optional wireless modem, is certified to EAC standards. The EAC requires that manufacturers accurately display its mark of certification and avoid misleading potential buyers into believing that a system, or any component thereof, is certified when it is not.

[8] *See* ES&S "DS200 Precinct Scanner & Tabulator" (2016), *available at* https://www.essvote.com/wp-content/uploads/2019/07/DS200_One-Sheet.pdf (last visited Dec. 11, 2019). As of December 11, 2019, the document can be found by visiting the DS200 product page on the ES&S website, *available at* https://www.essvote.com/products/ds200/, where ES&S provides the "product one-sheet" as a download.

[9] ES&S, "Cuyahoga County, Ohio Tabulation Equipment Survey" p. 103-04 (Nov. 9, 2018), *available at* http://bit.ly/33Wa6sl

[10] ES&S Information Sheets, DS200 Product One-Sheet at p.3-4, *available at* http://bit.ly/33SeZJ0

[11] ES&S DS200 Product One-Sheet, *available at* http://bit.ly/2BJR4Vo

[12] ES&S DS200 Product One-Sheet, *available at* http://bit.ly/362eJko. The document can be found with other ES&S materials provided to the North Carolina State Board of Elections (NC SBE), which can be found and downloaded through the NC SBE, at https://dl.ncsbe.gov/index.html?prefix=State_Board_Meeting_Docs/2019-07-26/Certification/Voting%20System%20Certification/ES&S/.

[13] ES&S DS200 Product One-Sheet, included in Boone County Commission proceedings at 300-01 (July 16, 2019), *available at* http://bit.ly/34f34Ew. *See id.* at pp. 99-342 (documents related to Boone County purchase of ES&S equipment).

[14] DS200 Product Brochure, *available at* http://bit.ly/36ssZXVJ.

TCPM Section 5.14 provides that:

> Manufacturers may not represent or imply a voting system is EAC certified unless it has received a Certificate of Conformance for the system. Statements regarding EAC certification in brochures, on websites, on displays, and in advertising/sales literature must be made solely in reference to specific systems. Any action by a Manufacturer to suggest EAC endorsement of its product or organization is strictly prohibited and may result in a Manufacturer's suspension or other action pursuant to Federal civil and criminal law. Manufacturers must provide a copy of the Certificate and Scope of Certification document (found at www.eac.gov) to any jurisdiction purchasing an EAC certified system.[15]

Under Section 5.15.1, the TCPM also provides that:

> The Manufacturer may use only the Mark of Certification that accurately reflects the certification held by the voting system as a whole. The certification of individual components or modifications shall not be independently represented by a Mark of Certification. In the event a system has components or modifications tested to various (later) version of the VVSG, the system shall bear only the Mark of Certification of the standard to which the system (as a whole) was tested and certified (i.e. the lesser standard). Ultimately, a voting system shall only display the Mark of Certification of the oldest or least rigorous standard to which any of its components are certified.[16]

Pursuant to Section 5.16, the TCPM also requires that "[t]he user's manual or instruction manual for a certified voting system shall warn purchasers that any changes or modifications to the system not tested and certified by the EAC will void the EAC certification of the voting system."[17]

ES&S has not followed the standards set forth in the TCPM. It displays the mark of certification on its website page for the DS200 and on other advertising materials sent or otherwise made available to election officials. The advertisements clearly indicate to buyers that the DS200—alone or with its optional features, including the modem—is fully certified by the EAC. Election officials easily could be misled into purchasing the DS200 with a wireless modem configuration, not realizing that the modem is uncertified, and that under Section 5.15.1 and Section 5.16, the modem's addition to the DS200 would void its certification and indeed, would void the certification of the entire system.

[15] EAC Testing and Certification Program Manual Version 2.0 § 5.14 (May 31, 2015) (hereinafter "TCPM").

[16] TCPM § 5.15.1 (emphasis added).

[17] TCPM § 5.16 (emphasis added).

ES&S may also be misrepresenting the modem as certified throughout the procurement process, which may qualify as an additional violation of the TCPM. In 2014, for example, in response to the Maryland State Board of Elections Request for Proposal (RFP) for an election system, ES&S submitted a proposal for its EVS 5.2.0.0, which Maryland accepted.[18] It is our understanding that during the procurement process, ES&S proposed the addition of a modem to the DS200 without indicating that its addition would void the system's EAC certification. Ultimately, after providing Maryland with a more expensive version of the EVS that included DS200 with modems, ES&S had to refund $1.2 million to the state of Maryland and remove modems from the already distributed machines.[19] ES&S may well have violated Section 5.16 by failing to warn the Maryland State Board of Elections that installing the modems in the DS200 voided the system's certification.

In Rhode Island, ES&S submitted a proposal in response to the state's RFP for a new voting system.[20] In its proposal, ES&S repeatedly claimed that its voting system, the EVS 5.2.0.3, was EAC certified.[21] Although it acknowledged that modem transmissions were not part of the EAC certification process, ES&S did not disclose that use of non-certified components will void the entire system's EAC certification.[22] ES&S also submitted a diagram that coded the DS200 with internal wireless modem as being part of the "EAC Certified Configuration."[23] Furthermore, though the diagram showed a system that integrated EAC-certified and non-certified components, ES&S did not clarify that under EAC guidelines, inclusion of any non-certified component in a voting system would void the entire system's certification. ES&S may well have violated Section 5.15.1, as well as 5.16 by failing to disclose to the Rhode Island Board of Elections that the EVS 5.2.0.3 may no longer be EAC certified if used with the DS200 with internal modems.

[18] Maryland State Board of Elections Request for Proposals, No. D38B4400019 (July 22, 2014); State of Maryland State Board of Elections, Meeting Minutes—October 30, 2014, at p. 9, *available at* http://bit.ly/2PAtaW5.

[19] State of Maryland State Board of Elections, Meeting Minutes—July 17, 2015, at p. 5-6, *available at* http://bit.ly/36rGmUo; State of Maryland State Board of Elections, Meeting Minutes—August 27, 2015, at p. 4, *available at* http://bit.ly/38DLkPM.

[20] ES&S, "Enhancing the Election Process for the State of Rhode Island: Request for Proposal RFP #7549934 Voting Equipment System (Oct. 30, 2015) (hereinafter ES&S Rhode Island Proposal). Relevant excerpts are appended to this letter as Attachment C, and we have made the entire document available on the Free Speech For People website, at http://bit.ly/2LIMFLh.

[21] *Id.* at 9 ("Certified Proven Products—ES&S is bidding the proven DS200 precinct based scanner"); *id.* at 55 ("Designed and federally certified to meet the rigorous security standards of the 2005 Voluntary Voting Systems Guidelines, the operating system controls, limits, and detects unauthorized access to all critical system components"); *id.* at 117 ("The proposed version of the DS200 is the latest version of the DS200 which is certified to the U.S. EAC VVSG 2005 standard . . . .").

The TCPM correctly recognizes that an election technology manufacturer cannot be allowed to falsely claim certification that its systems have not earned. And ES&S's omissions in its advertisements and procurement-related communications do precisely this. Though the EVS 5.0.0.0 and its subsequent versions are certified, inclusion of the uncertified modem voids the entire system's certification. ES&S clearly violates the TCPM by omitting this information from its advertisements and its procurement communications.

Courts throughout the country have long recognized that omission of material facts may void contracts and give rise to cognizable claims for damages against the omitting party. As the Supreme Court recently confirmed "[b]ecause common-law fraud has long encompassed certain misrepresentations by omission, 'false or fraudulent claims' include more than just claims containing express falsehoods . . . misrepresentations by omission can give rise to liability."[24] Omission of critical information about "statutory, regulatory, or contractual requirements" may well result in "misleading half-truths" that give rise to cognizable claims of fraudulent misrepresentation.[25]

But counties and states should not have to resort to contract disputes with election vendors. They must be able to trust the accuracy of vendor assurances about EAC certification.

[22] *See id.* at 49 (noting that modem transmissions were not part of the EAC certification process).

[23] *Id.* at 166-67.

[24] *Universal Health Servs., Inc. v. United States*, 136 S. Ct. 1989, 1999 (2016).

[25] *Id.* at 2001. Though federal contract law does not govern ES&S's fraudulent misrepresentations, omission of material fact is recognized as a form of fraud in states throughout the country, including those in which ES&S has contracted.

4. Requested action

The EAC should rigorously apply its standards and protections, and take swift response where vendors make false and misleading claims. Section 5.15.4 of the Testing and Certification Program Manual provides a broad range of remedies for vendor misrepresentation of certification status, including requiring corrective action, decertification, and manufacturer suspension.[26]

> If the EAC determines a voting system is not in compliance with the VVSG, and the system has already been sold or otherwise distributed bearing the Mark of Certification, the EAC shall provide written notice to the Manufacturer. If the Manufacturer fails to take corrective action within 15 days of receipt of such notice, the EAC shall have the right to announce publicly that the voting system may no longer comply with its original certification, and may choose to initiate decertification actions as outlined in Chapter 7 of the *Manual*, and/or suspension of Manufacturer Registration as outlined in Section 2.6 of the *Manual*. Corrective action may include modification of the voting system to bring it into compliance with the VVSG, or removal of the Mark of Certification from the product.

(Section 5.15.4)

For this reason, we strongly urge the EAC to investigate ES&S's alleged violations of Sections 5.14, 5.15.1, and 5.16. And if ES&S requests an opportunity to cure its violations, the EAC should require substantive action on the vendor's part. Simply removing the advertisements or adding curative language is necessary, but not sufficient. ES&S must take proactive steps to correct its error, including but not limited to negotiating with parties that have purchased the equipment to reach an appropriate settlement of damages; running public advertisements in all states that have, or are considering the purchase of the DS200, to acknowledge and correct the omissions; and conducting public forums for voters who have had to, or may have to, vote on modem-equipped DS200 machines. Furthermore, the EAC should subject ES&S to rigorous overview of its advertisements for such period of time as necessary to reassure voters throughout the country that ES&S has learned to accurately advertise its certifications. Finally, the EAC should reserve the right, based on information derived from its investigation or if ES&S is any way uncooperative, to suspend the company's registration indefinitely.

States and counties across the country rely upon the EAC certification process to guide their choice in voting systems and vendors. And the EAC correctly requires vendors to advertise certification only when *all* components of the advertised system has been thoroughly tested and certified by the EAC. Rules 5.14, 5.15.1, and 5.16 are important rules that protect purchasing states and counties, and through them, the voters, from having to cast votes on systems that have not been properly vetted by the EAC. ES&S has repeatedly advertised its DS200 with internal modem—a critical component to ES&S's voting systems—as being EAC certified when, in fact, it is not. We therefore again respectfully request that EAC investigate and take action to correct this serious issue.

Sincerely,

Courtney Hostetler, Counsel
Ronald A. Fein, Legal Director
John C. Bonifaz, President
Ben T. Clements, Chair of the Board
Free Speech For People
1320 Centre St. #405
Newton, MA 02459
(617) 249-3015
chostetler@freespeechforpeople.org

Susan Greenhalgh
Vice President of Policy and Program
National Election Defense Coalition

[26] Section 2.6 provides that "[w]hen Manufacturers violate the certification program's requirements by engaging in management activities inconsistent with this Manual or failing to cooperate with the EAC, their registration may be suspended until such time as the issue is remedied." Under Section 2.6.2, suspension of registration means that "[a] suspended Manufacturer may not submit a voting system for certification."

September 15, 2020

The Honorable Laurel Lee
Election Director Maria Matthews
Division of Elections
Florida Department of State
R.A. Gray Building
500 South Bronough Street
Tallahasse, Florida

Dear Secretary Lee and Director Matthews,

We, as members of the computer science, cybersecurity, and election integrity communities, are writing to urge you to act now to protect election systems and minimize attack vectors by eliminating the use of wireless modems and public telecommunication infrastructure, including the Internet, in election systems.

As we rapidly approach the 2020 general elections, election administrators face unprecedented challenges conducting elections. The COVID-19 pandemic continues to disrupt ordinary operations and requires new procedures and protocols. As officials grapple with these extraordinary events, we must not lose sight of the fact that our elections remain under attack by the opponents of a free and fair democracy, who wish to compromise our election infrastructure to sow chaos, distrust, or even manipulate the election outcome.

During the 2016 election cycle, Russian intelligence agents gained and maintained access to State and County board election networks.[1] These efforts have not abated; intelligence officials maintain that foreign agents continue to try to hack into U.S. election systems.[2] We must assume that all election systems are under attack by hostile agents seeking to corrupt, manipulate or disrupt our election systems.

Wireless modems connect voting systems to the Internet

It has been asserted that voting machines are not vulnerable to remote hacking because they are never connected to the Internet, but both the premise and the conclusion are false. Election systems can be directly or indirectly exposed to internet-based attacks. Moreover, many voting machines currently in use around the country use embedded or integrated wireless cellular

[1] "Assessing Russian Activities and Intentions in Recent US Elections," Office of the Director of National Intelligence, January 6, 2017. *Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf*

[2] William Evanina, the election security czar for the White House, recently issued a statement warning that foreign agents "seek to compromise our election infrastructure … we continue to monitor malicious cyber actors trying to gain access to U.S. state and federal networks, including those responsible for managing elections." "Statement by NCSC Director William Evanina: 100 Days Until Election 2020," Office of the Director of National Intelligence, July 24, 2020. *Available at: https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020*

modems to transmit unofficial vote totals to county election management systems. These vote totals are typically received at the County on standard PCs that are regularly used to program voting machines and aggregate vote totals. Though these systems should never be directly or indirectly connected or exposed to the Internet, the use of wireless modems directly connects those devices to the Internet and exposes them to Internet-based attacks.

Voting system vendors may have asserted that cellular modems utilize a different network, but today's cellular modems are part of the Internet, making the systems vulnerable to common Internet-based attacks. This fact has been explicitly and unequivocally affirmed by the National Institute of Standards and Technology (NIST).[3] In fact, computer security researchers have demonstrated that these systems are visible on the Internet to potential attackers.[4] Furthermore, wireless modems introduce their own inherent weaknesses that can be exploited to compromise an election system.[5] In addition, a cellular device can be tricked into connecting to false mobile cell towers (such as Stingray surveillance devices[6]) enabling significant disruption, and if there is improper authentication of a connection, there could be false reports from devices impersonating precinct voting machines.

Connecting to the Internet, even briefly during machine maintenance, programming, pre-election testing, poll worker training, or on Election Day, makes the system vulnerable to attacks that could impact current or future election results. When contemplating the use of wireless modems and connectivity to public networks in the next generation of the federal voluntary voting system guidelines, NIST wrote:

> *"There are significant security concerns introduced when networked devices are then connected to the voting system. This connectivity provides an access path to the voting system through the Internet and thus an attack can be orchestrated from anywhere in the world (e.g., Nation State Attacks). The external network connection leaves the voting system vulnerable to attacks, regardless of whether the connection is only for a limited period or if it is continuously connected."*[7]

[3] At a December 18th 2019 presentation to the EAC's Technical Guidelines Development Committee, a NIST official stated that use of wireless modems: "*...make the voting system a node on the internet... [and] also could potentially provide an entryway for remote attackers, but not just close-range remote attackers, once you're on the internet now even further nation-state attackers may have access to you. What's the impact of that? It could be a loss of confidentiality and integrity of that voting system and that information that's on the voting system...If you're able to inject malware into the voting system, now you can change the data, now you can change the information that's within the voting system, or change the behavior of the voting system itself...*" *Available at:* https://www.eac.gov/events/2019/12/18/eac-technical-guidelines-development-committee-conference-call-meeting-121819 29:30

[4] Kim Zetter, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," *Vice*, August 8, 2019. *Available at: https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials*

[5] Modems are known to have been compromised by foreign agents by exploiting known weaknesses in a commonly used Border Gateway Protocol (BGP) to re-route traffic at the direction of the attacker. This weakness has been termed the "notorious BGP" and is reckoned to be the "internet's biggest security hole. *See:* Kim Zetter. "Revealed: The Internet's Biggest Security Hole," *Wired*, Aug. 26, 2008. *Available at: https://www.wired.com/2008/08/revealed-the-in/*

[6] For an introductory overview of these devices, see generally, MSI-catcher, https://en.wikipedia.org/w/index.php?title=IMSI-catcher&oldid=856220555 (last visited Oct. 2, 2018).

[7] "Draft Recommendations for Requirements for the Voluntary Voting System Guidelines VVSG 2.0," National Institute of Standards and Technology, January 31, 2020. *Available at:* https://collaborate.nist.gov/voting/pub/Voting/VVSG20DraftRequirements/vvsg-2.0-2020-01-31-DRAFT-requirements.pdf

NIST extended its warning to caution that wireless modems expose voting systems to ransomware attacks, a dangerous threat that has crippled municipalities.[8]

Recognizing that election administrators will need other options for transferring election results efficiently, NIST outlined several alternative ways to transfer election results which protect the integrity of the voting by ensuring a robust airgap at the voting machines and the election management system. This is most easily accomplished by transferring the results (by appropriate means) to a separate device which is on the Internet, transmitting the results to another device at the county headquarters which is also on the Internet, then transferring the data from that device to the election management system manually or by barcode, while maintaining a secure "air-gap" for the election system itself. We urge you to review their document[9] which provides alternative transmission methods.

Therefore, we strongly urge election administrators to cease all use of wireless modems and provide these recommendations:

1. Voting system components—from vote capture and tabulation machines to election management systems—should not be connected to the internet, cellular network, or other public telecommunications infrastructure at any time, even temporarily, from the time of manufacture until end of life through wireless modems or other means.
2. Election administrators should not transmit election results from vote tabulation devices over any network, including cellular networks, "dial-up" connections, and the Internet. Instead, they should adopt procedures to transfer election results on digital media such as memory cards, thumb drives, or paper to election management systems. Removable media should not be re-used: only brand-new storage devices from a trustworthy source. No device that is ever connected to a voting machine, tabulator, or election management system should ever be connected to the Internet or any other network, including cellular networks.
3. Cellular modems within voting systems should be *physically removed*, not simply disabled in software.

These recommendations do not imply that posting unofficial election results on properly configured and protected public accessible government web sites should be stopped.

Discontinuing the use of wireless modems in voting systems will not make voting systems impenetrable. Many other attack vectors still exist. The only way to ensure resilience in voting systems is by requiring voter-verified paper ballots, verifiably secure chain of custody of the ballots, and robust, manual post-election audits of the results against the paper ballots.

[8] "Baltimore government held hostage by hackers' ransomware," *BBC News*, May 23, 2019. *Available at: https://www.bbc.com/news/world-us-canada-48371476*

[9] Alternative methods of election results transmissions are outlined in this document "Wireless Use Case Analysis," from the National Institute of Standards and Technology Cyber Security Working Group. *Available at: https://collaborate.nist.gov/voting/pub/Voting/CyberSecurity/WirelessUseCaseAnalysis-OpenArea-Sept16-2019.pdf*

The undersigned thank you for your service and your immediate attention to this critical national security issue. We stand ready to work with you to protect our nation's election infrastructure from all threats, foreign and domestic.

Sincerely,

Free Speech For People

Electronic Frontier Foundation

Dr. Andrew W. Appel*
Professor of Computer Science, Princeton University

Cindy Cohn
President
Electronic Frontier Foundation

Aleksander Essex, Ph.D, P.Eng*
Associate Professor
Associate Chair, Graduate
Department of Electrical and
Computer Engineering
Western University
London, ON, Canada

Lowell Finley*
former Deputy Secretary of State
California

Susan Greenhalgh
Senior Advisor on Election Security
Free Speech For People

Center for Scientific Evidence in Public Issues (EPI Center)
American Association for the Advancement of Science

OSET Institute Inc.

Dr. Duncan Buell NCR*
Professor in Computer Science and
Engineering Dept of Computer Science and
Engineering University of South Carolina

Dr. Richard A. DeMillo*
Charlotte B. and Roger C. Warren Professor
of Computer Science
College of Computing
Georgia Institute of Technology

Dr. Michael D. Fernandez
Founding Director
Center for Scientific Evidence in Public
Issues (EPI Center)
American Association for the Advancement
of Science

Dr. Juan E. Gilbert*
Andrew Banks Family Preeminence Endowed
Professor & Chair
Computer & Information Science &
Engineering Department
University of Florida

Dr. J. Alex Halderman*
Professor, Computer Science and Engineering
Director Center for Computer Security and
Society
University of Michigan

Harri Hursti*
Founding Partner
Nordic Innovation Labs.

Dr. David Jefferson*
Lawrence Livermore Laboratories
(Retired)

Dr. Peter G. Neumann*
Chief Scientist,
SRI International Computer Science Lab

Dr. Avi Rubin*
Professor, Computer Science
Johns Hopkins University

E. John Sebes
Chief Technology Officer
OSET Institute, Inc.

Professor Eugene H. Spafford*
Executive Director Emeritus, CERIAS
Purdue University

Dr. Dan S. Wallach*
Professor, Department of Computer Science
Rice Scholar, Baker Institute for Public
Policy
Rice University

Dr. Douglas W. Jones*
Associate Professor
Department of Computer Science
University of Iowa

Gregory A. Miller
Chief Operating Officer
OSET Institute, Inc

Mark Ritchie*
Former MN Secretary of State
Member of the EAC Board of Advisors
Former president of the National Associa
of Secretaries of State

Bruce Schneier*
Fellow and Lecturer
Harvard Kennedy School

Kevin Skoglund*
Chief Technologist
Citizens for Better Elections

Dr. Philip B. Stark*
Professor, Associate Dean of Mathemati
and Physical Sciences
Department of Statistics
University of California at Berkeley

Dr. Poorvi L. Vora*
Professor of Computer Science
The George Washington University

*Affiliations listed are for identification purposes only and do not imply institutional endorsement.

Are voting-machine modems truly divorced from the Internet?

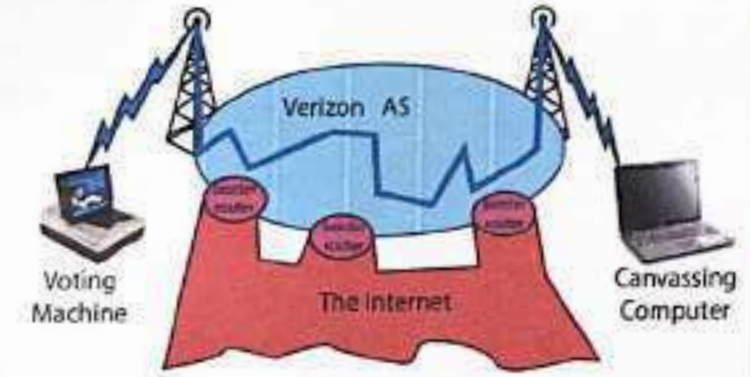
FEBRUARY 22, 2018 BY ANDREW APPEL

(This article is written jointly with my colleague Kyle Jamieson, who specializes in wireless networks.)

[See also: The myth of the hacker-proof voting machine]

The ES&S model DS200 optical-scan voting machine has a cell-phone modem that it uses to upload election-night results from the voting machine to the "county central" canvassing computer. We know it's a bad idea to connect voting machines (and canvassing computers) to the Internet, because this allows their vulnerabilities to be exploited by hackers anywhere in the world. (In fact, a judge in New Jersey ruled in 2009 that the state must not connect its voting machines and canvassing computers to the internet, for that very reason.) So the question is, does DS200's cell-phone modem, in effect, connect the voting machine to the Internet?

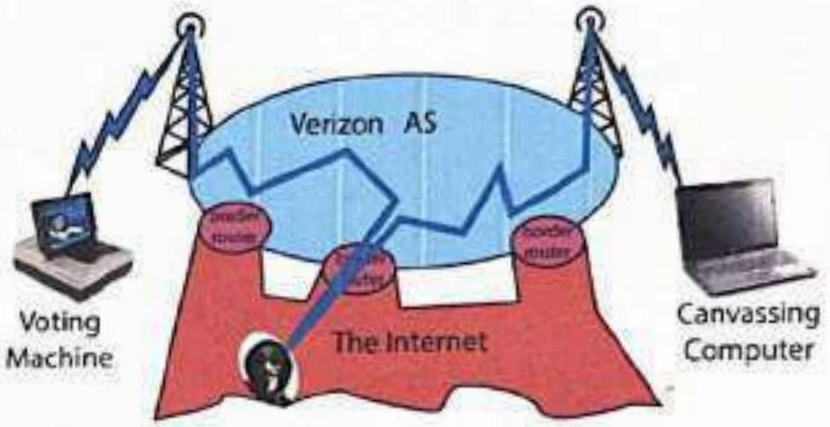
The vendor (ES&S) and the counties that bought the machine say, "no, it's an analog modem." That's not true; it appears to be a Multitech MTSMC-C2-N3-R.1 (Verizon C2 series modem), a fairly complex digital device. But maybe what they mean is "it's just a phone call, not really the Internet." So let's review how phone calls work:



The voting machine calls the county-central computer using its cell-phone modem to the nearest tower; this connects through Verizon's "Autonomous System" (AS), part of the

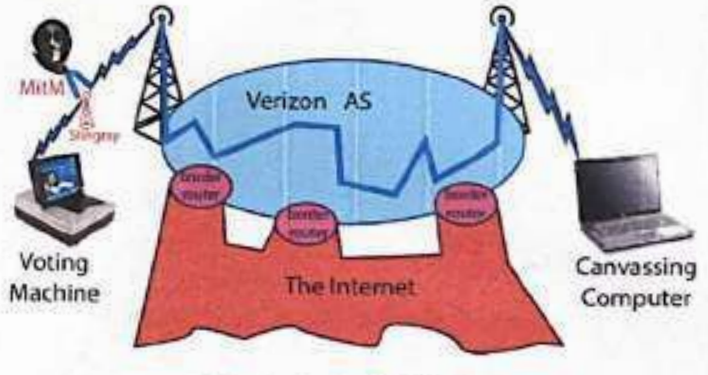
packet-switched Internet, to a cell tower (or land-line station) near the canvassing computer.

Verizon attempts to control access to the routers internal to its own AS, using firewall rules on the border routers. Each border router runs (probably) millions of lines of software; as such it is subject to bugs and vulnerabilities. If a hacker finds one of these vulnerabilities, he can modify messages as they transit the AS network:



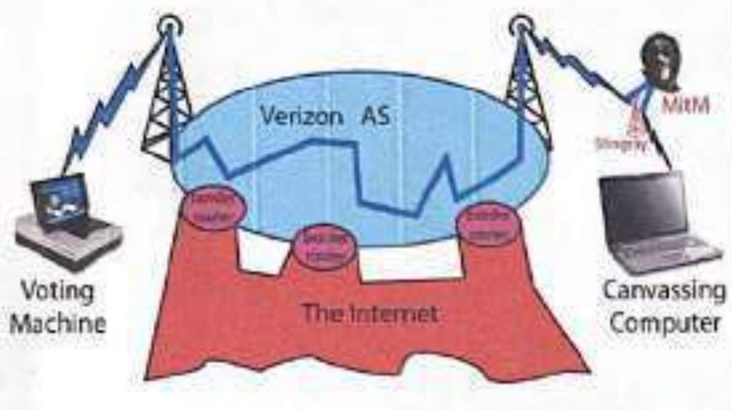
Do border routers actually have vulnerabilities in practice? Of course they do! US-CERT has highlighted this as an issue of importance. It would surprising if the Russian mafia or the FBI were not equipped to exploit such vulnerabilities.

Even easier than hacking through router bugs is just setting up an imposter cell-phone "tower" near the voting machine; one commonly used brand of these, used by many police departments, is called "Stingray."



I've labelled the hacker as "MitM" for "man-in-the-middle." He is well positioned to alter vote

totals as they are uploaded. Of course, he will do better to put his Stingray near the county-central canvassing computer, so he can hack all the voting machines in the county, not just one near his Stingray:



So, in summary: phone calls are *not* unconnected to the Internet; the hacking of phone calls is easy (police departments with Stingray devices do it all the time); and even between the cell-towers (or land-line stations), your calls go over parts of the Internet. If your state laws, or a court with jurisdiction, say not to connect your voting machines to the Internet, then you probably shouldn't use telephone modems either.

FILED UNDER: OTHER TOPICS   TAGGED WITH: VOTING MACHINES, VOTING SECURITY

Attorney General Dana Nessel
G. Mennen Williams Building, 7th Floor
525 W. Ottawa St.
P.O. Box 30212
Lansing, MI 48909

October 5, 2020

Dear Attorney General Nessel,

We write to you to request your office initiate an inquiry and investigation into Election Systems & Software (ES&S), regarding misrepresentations in its voting system contract with the state of Michigan relevant to the use of the DS200 ballot tabulator with wireless modem.[1]

ES&S sold a version of its system to several Michigan localities that is expressly designed to transmit election results from the DS200 ballot tabulator to the election management system via wireless modems. In its contract with Michigan, ES&S characterized this as a connection to "cellular networks," while simultaneously and repeatedly insisting to both government officials and the public that none of its voting systems *ever* connect to the internet. This false and misleading distinction between "cellular networks" and the internet has been conclusively refuted—ES&S's systems with modems *are* exposed to the internet.

ES&S should be compelled to remove the wireless modems from its systems at no cost to taxpayers, as required by the contract. If ES&S refuses, your office should consider legal action against ES&S for breach of contract, breach of warranty, and/or fraudulent or reckless misrepresentation. By selling an internet-connected voting system, ES&S has not only misled the voters and local election officials, but also endangered the security of Michigan's elections.

[1] Free Speech For People is a non-profit, non-partisan public interest legal organization that works to renew our democracy and our United States Constitution for the people. As part of our mission, we are committed to promoting, through legal actions, secure, transparent, trustworthy and accessible voting systems for all voters.

I. Background

a. DS200s with modems are not federally certified

ES&S manufactures the DS200, a precinct-based ballot scanner and vote tabulator. In 2011, ES&S submitted a new voting system, the EVS 5.0.0.0, to the U.S. Election Assistance Commission (EAC) for federal certification. As part of the EVS 5.0.0.0 system, ES&S sought certification of the DS200 in three versions: (1) as a stand-alone precinct scanner, (2) as a precinct scanner with wired modem capability, and (3) as a precinct scanner with wireless network capability. In the third configuration, a wireless modem is present in the polling place tabulation system and used to transmit unofficial election results to the jurisdiction's election management systems. This means both the ballot tabulating machine and the election management system (EMS), a critical component that programs the voting system and aggregates vote totals, connect to the internet.

Unable to meet federal requirements for modems, ES&S withdrew both the wired modem and wireless transmission configurations of the DS200 from their application process in August of 2012.[2] This version of the EVS 5.0.0.0 system—which does not include either a wired modem or wireless transmission configuration of the DS200—was certified by the EAC to VVSG 1.0 standards on May 13, 2013.[3] Several subsequent versions have also been certified, all without modems.

There is widespread consensus among election cybersecurity experts that voting systems with the capability to connect to the internet, through wireless modems or other means, are highly insecure.[4] In contemplating the security concerns specific to the use of wireless modems in voting systems, the National Institute of Standards and Technology (NIST) wrote:

[2] Steve Pearson, Vice President, Certification, ES&S, Letter to U.S. Election Assistance Commission Re: EVS 5.0.0.0 Scope Revision (August 13, 2012).
[3] ES&S EVS 5.0.0.0 Certificate of Conformance; Alice P. Miller, U.S. Election Assistance Commission, Letter to Steve Pearson, Vice President, Certification, ES&S, Re: Agency Decision—Grant of Certification (May 16, 2013); Wyle Laboratories, Test Report, Report No. T59087.01-01, Rev A (May 1, 2013).
[4] National Academies of Sciences, Engineering, and Medicine, "Securing the Vote," 2018. *Available at* https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

> *"If an attacker gains access to the voting system through wireless technology, they may be able to remotely inject malware or modify files within the voting system. This impacts the integrity of the information on the voting system if the malware is able to modify files such as, maliciously tampering with tabulation results or deleting ballot records. The confidentiality of the information on the voting system is impacted if the malware is used to reconfigure the wireless technology to send data to an unauthorized receiver…*
> *Exposure to the internet may also enable nation-state attackers to remotely inject malware that maliciously modifies or deletes files within the voting system."*[5]

According to NIST any device that has this capability can be hacked remotely, including by nation-state actors.[6]

Since initial certification, it is our understanding that ES&S has not submitted a wired modem or wireless configuration of the DS200 for EAC testing or certification. Instead, ES&S offers the DS200 with wireless modem configuration to customers under its never EAC-certified system EVS 5.3.2.0 and other versions.[7] Though not federally certified, ES&S repeatedly falsely claimed to its customers, in marketing materials and publicly available information, that the DS200 systems with modems were federally certified.[8]

ES&S sold DS200 scanners in seven Michigan counties: Bay County, Emmet County, Grand Traverse County, Kalamazoo County, Macomb County, Mason County, and Roscommon County.[9] Researchers have found ES&S election management systems for at least four Michigan localities visible on the internet, indicating that ES&S delivered this configuration to, at least, these four jurisdictions.[10]

b. Contract

In 2017, the Michigan Secretary of State approved three vendor statewide contract proposals, allowing localities to purchase systems under any of the approved contracts.[11]

The ES&S contract offers a base system and then identifies a proposed modification to the proposed base Michigan voting system, to include the wireless modems. In the contract, ES&S acknowledges that the modification is not EAC certified:

> *"EVS 5.3.2.0 is a modification of the EVS 5.2.2.0 that allows for the transmission of unofficial election results on election night via landline or wireless modeming from a precinct based DS200 and/or from regional collection sites to election central via the AT&T, Sprint, or Verizon network."*[12]

However, the contract goes on to misstate the difference and omit the fact that the modem modification will make the system internet-connected.

> ***"ES&S Footnote:*** *ES&S confirms that the* ***only functional difference*** *between the Base System (EVS 5.2.2.0.) and the Modified System (EVS 5.3.2.0.) is the addition of modem functionality to allow for electronic transmission of unofficial results."*[13] (Emphasis added.)

It is important to understand that in this configuration the connection and exposure to the internet is not limited to the tabulator with the wireless modem. In order to receive the transmitted unofficial results, the election management system (a

[5] "Draft Recommendations for Requirements for the Voluntary Voting System Guidelines VVSG 2.0," National Institute of Standards and Technology, January 31, 2020. *Available at:* https://collaborate.nist.gov/voting/pub/Voting/VVSG20DraftRequirements/vvsg-2.0-2020-01-31-DRAFT-requirements.pdf

[6] *Ibid.*

[7] Elections Systems Software, LLC, Exhibit 2, Attachment 1.1 Voting System Hardware, Contract No. 071B7700120 (Mar. 1, 2017), [illegible] at 1-1-A.17

[8] Kim Zetter, "Election commission orders top voting machine vendor to correct misleading claims," *Politico*, August 13, 2020. *Available at: https://www.politico.com/news/2020/08/13/election-voting-machine-misleading-claims-394891*

[9] *See:* https://verifiedvoting.org/verifier/#mode/search/year/2020/state/26/make/Election%20Systems%20&%20Software/model/DS200

[10] Kim Zetter, "Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials," *Vice*, (Aug. 8, 2019). *Available at:* [illegible]

[11] *See* "Voting System Purchase Resources and Instructions for Michigan Election Officials." *Available at:* https://www.michigan.gov/sos/0,4670,7-127-1633_11976_78905---,00.html

[12] State of Michigan Enterprise Procurement, Contract No. 071B7700120, Department of Technology, Management, and Budget (Mar. 1, 2017) Exhibit 1 to Schedule A. (page 47). Available at: https://www.michigan.gov/documents/sos/071B7700120_ESS_Contract_555359_7.pdf

[13] *Ibid.*

critical component of the election system which not only aggregates vote totals but also programs voting machines) must be connected and exposed to the internet for a sustained period of time. This constitutes an additional significant functional difference in that the election management system must be enabled for internet connectivity, have access to the internet, and be actively connected to the internet for sustained periods of time in order to receive the electronic transmission of unofficial results from the modems.

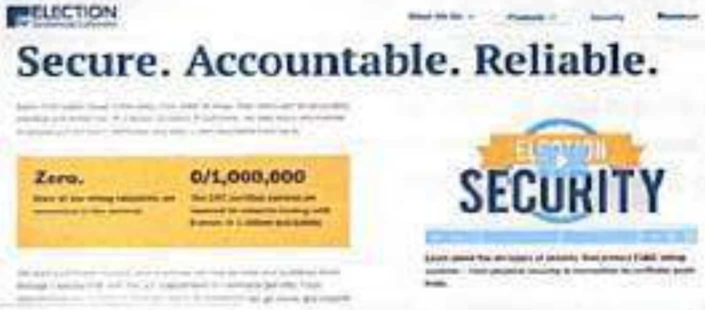
c. <u>ES&S False Claims</u>

Internet connectivity

If Michigan officials did not understand that use of wireless modems directly connect and expose a system to the internet, this can be directly attributed, not just to ES&S's conspicuous omission of this fact, but to potential false claims and misrepresentations made by ES&S in other materials.

Through the contract and in public statements, ES&S represents the wireless modems only as using "cellular networks." (By contrast, when discussing the transmission and posting of election night reporting systems - which are expected to be transmitted and posted on the public internet - ES&S explicitly acknowledges the transmission will be conducted via the internet.) But much more importantly, ES&S has repeatedly represented to its customers that *none* of its voting systems *ever* connect to the internet. As recently as January 2020, the ES&S website stated:

"Zero. None of our voting tabulators are connected to the Internet."[14]



Secure. Accountable. Reliable.

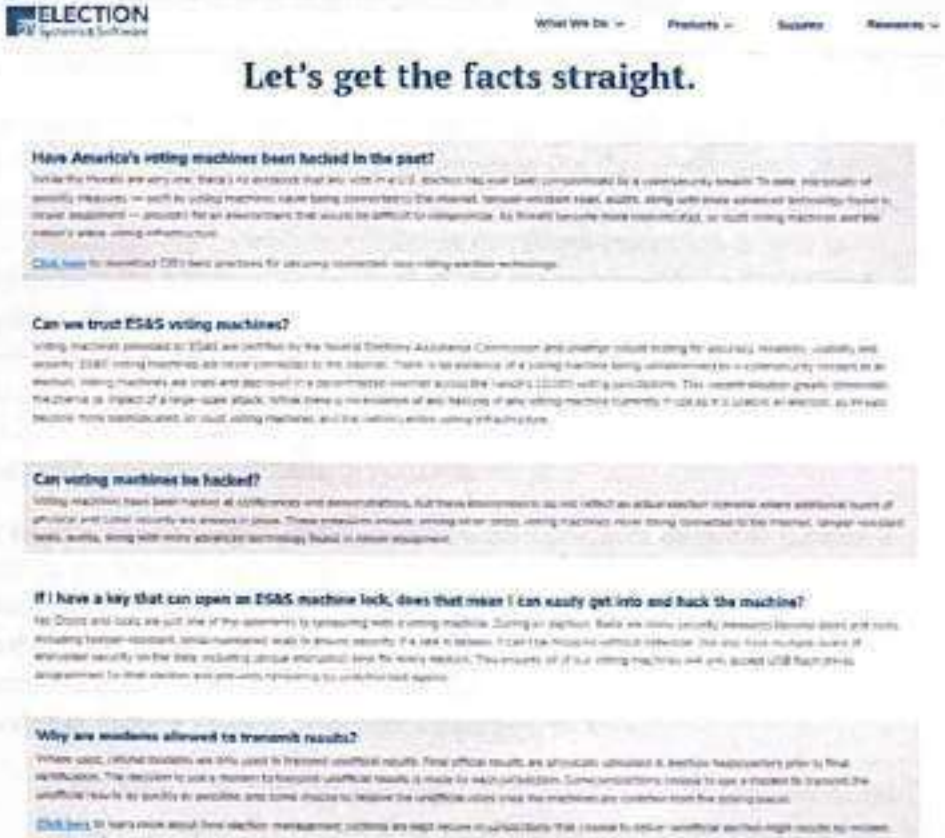
Zero.

0/1,000,000

[14] Internet Archive capture on Jan 10, 2020:
https://web.archive.org/web/20200110012456/https://www.essvote.com/featurelsecurity/

Another ES&S webpage titled "**Let's get the facts straight** –" stated:

"ES&S voting machines are never connected to the Internet."[15]



Let's get the facts straight.

Have America's voting machines been hacked in the past?

Can we trust ES&S voting machines?

Can voting machines be hacked?

If I have a key that can open an ES&S machine lock, does that mean I can easily get into and hack the machine?

Why are modems allowed to transmit results?

ES&S has also repeated this misinformation in direct emails to its customers. In an email sent to ES&S customers on the eve of the 2017 DEF CON hackers conference ES&S sent an email to its customers that stated:

[15] Internet Archive capture on Oct. 29, 2019:
https://web.archive.org/web/20191029124002/https://www.essvote.com/faqs/

> **"Can you perform a cyber-attack on something that is not connected to the internet?**
>
> The units that tabulate votes and the computers that contain the software to program those units are NEVER connected to the internet."[16]

ES&S made these claims while selling devices configured specifically to connect to and receive unofficial results over the internet.

Federal Certification

As noted, ES&S's misstatements regarding its systems with wireless modems extend to misrepresentations regarding federal certification. In January of 2020, Free Speech For People sent a letter to the EAC detailing evidence of false claims and deceptive marketing practices by ES&S designed to misrepresent its voting systems with wireless modems as federally certified. The EAC conducted an investigation and concluded that ES&S misrepresented its systems with modems as federally certified when they were not. The EAC also directed ES&S to contact all its customers that had bought systems with wireless modems and acknowledge that it had falsely claimed its modemed systems had been certified.[17]

Though Michigan law does not require EAC certification, the State clearly values it. The Michigan contract explicitly stated:

> *"A. Federal Testing and Certification Requirements*
>
> *Contractor's system shall have been tested and successfully completed all certification steps required by the U.S. Election Assistance Commission (EAC) before the system will be approved for implementation in Michigan."*[18]

In short, ES&S appears to have misled Michigan officials to believe that its modemed systems use "cellular networks," not the internet, because ES&S voting systems "never" connect to the internet. ES&S also advertised its systems with

[16] See attachment A.
[17] *See:* Zetter, note 8.
[18] State of Michigan Enterprise Procurement, Contract No. 071B7700120, Department of Technology, Management, and Budget (Mar. 1, 2017) page 24.
https://www.michigan.gov/documents/sos/071B7700120_ESS_Contract_555359_7.pdf
At 1.5.A

modems as federally certified when they are not, and ES&S claimed that the only functional difference from its federally certified system is the transmission of election results, without acknowledging that both the voting tabulator and critical election management system must be connected to the internet.

2. Grounds to compel removal of modems

In August of 2019, a news report disclosed that researchers had identified ES&S EMSs on the internet in Michigan, meaning that they could clearly identify the IP addresses of ES&S EMSs on the internet in the state. This means the EMSs were connected to the internet and visible to the ethical researchers as well as malicious actors. The researchers reported that even after notifying the national Elections Infrastructure and Information Sharing and Analysis Center (EI-ISAC)—a 24-hour watch center funded by the Department of Homeland Security—of their discovery, systems in Kalamazoo and Roscommon remained online. Another Michigan system was also online, but researchers were unable to pinpoint the jurisdiction in which the IP address is located.[19]

The state should compel ES&S to remove the modems at no cost to the state or localities. Michigan Secretary of State Jocelyn Benson later commented that if her cybersecurity election committee recommends the modems be taken out, "we'll take them out."[20] Removing these modems may prove costly. However, the contract obligates ES&S to cure any "defects or malfunctions" in the system, as provided in Section 1.6 of the Contract's statement of work:

> *"Contractor shall promptly notify the State and any Authorized User of any defects or malfunctions in the Deliverable, associated System Software or Documentation of which it learns from any source, correct any such defects or malfunctions or provide a workaround until corrected within five (5) Business Days of knowledge of such defect or malfunction and provide the*

[19] *See:* Zetter, note 10.
[20] Kartikay Mehrotra, "America Won't Give Up Its Hackable Wireless Voting Machines (1)," Bloomberg Law, (Jan. 3, 2020), https://news.bloomberglaw.com/privacy-and-data-security/america-wont-give-up-its-hackable-wireless-voting-machines.

> *State or Authorized User with corrections of same, at no additional cost to the State or Authorized User."*[21]

The systems with internet connectivity should constitute a "defect," as they do not conform to the contract's terms. Consequently, upon demand, ES&S must, within five business days, correct this defect "at no additional cost" to the state or localities.

If ES&S does not agree to correct this defect within five business days after your demand, your office should consider judicial action. If it turns out that, by including internet connectivity in its modems, ES&S either breached an express warranty, engaged in misrepresentation, or else breached the contract, the state may be able to compel ES&S to remove the modems at no cost.

By including the EVS 5.3.2.0 in its product options for Michigan counties, ES&S may have breached an express warranty. Specifically, by warranting that its voting system conforms to the specifications set forth in the contract, ES&S may have also warranted that its voting systems do *not* connect to the internet.[22] Specifically, as noted above, in the contract ES&S "confirm[ed] that the only functional difference between the Base System (EVS 5.2.2.0.) and the Modified System (EVS 5.3.2.0.) is the addition of modem functionality to allow for electronic transmission of unofficial results."[23] And while today's cellular modems do connect to the internet, the fact that ES&S expressly warranted that the "only" functional difference was connecting to cellular data networks means that their connection to the internet is contrary to this warranty. Further, ES&S neatly omits the fact that the EMS must be enabled for internet connectivity, requires access to an internet connection and must have a live internet connection to receive the transmission.

[21] State of Michigan Enterprise Procurement, Contract No. 071B7700120, Department of Technology, Management, and Budget (Mar. 1, 2017) at 1.6.A.2 (p. 26) https://www.michigan.gov/documents/dtmb/071B7700120_ESS_Contract_555350_7.pdf

[22] Elections System Software, LLC, Exhibit 2, Attachment 1.1 Voting System Hardware, Contract No. 071B7700120 (Mar. 1, 2017). https://www.michigan.gov/documents/dtmb/071B7700120_ESS_Exh_2_to_Sch_A_Tec_Req_555360_7.pdf at 1.2.A.3

[23] See note 18 at Exhibit 1 to Schedule A (C)

Consequently, EVS 5.3.2.0 has an important functional difference (internet connectivity) with EVS 5.2.2.0 that was not disclosed—a violation of ES&S's express representation that "the only functional difference" was functionality enabling connection via landline or specified cellular data networks. Moreover, this lack of conformity may also represent a general breach of contract. If so, the state must give the vendor at least 30 days to cure such a breach or else the State may terminate the contract for cause, in whole or in part.[24]

3. Conclusion

As the country approaches to the 2020 election—the first presidential election since 2016 when Russian hackers attempted to infiltrate numerous voting systems across the United States—it is critical, now more than ever, that states across the nation secure the safety of our elections. This includes ensuring that voting systems cannot be hacked remotely by sophisticated hackers because those systems connect to the internet. The Michigan Attorney General should act now to investigate Michigan's contract with ES&S in order to compel the removal of wireless, internet-connecting modems in DS200s across the state.

Please do not hesitate to reach out to us if you have any questions or if we can be of any assistance. We stand ready to assist you and your colleagues in any way we can.

Sincerely,

Susan Greenhalgh
Senior Advisor on Election Security
susan@freespeechforpeople.org

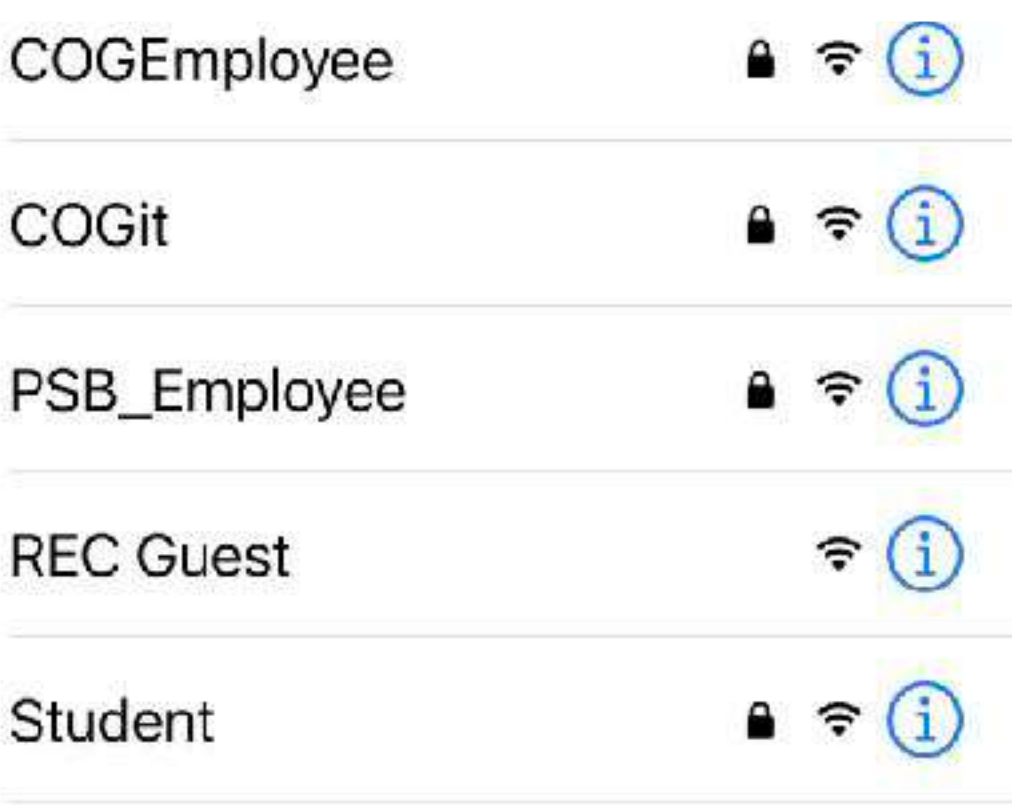
Ron Fein
Legal Director
RFein@freespeechforpeople.org

cc. The Honorable Jocelyn Benson
Michigan Department of State
Bureau of Elections
PO Box 20126
Lansing, MI 48901-0726

[24] State of Michigan Enterprise Procurement, Contract No. 071B7700120, Department of Technology, Management, and Budget (Mar. 1, 2017) at pg 14.
https://www.michigan.gov/documents/dtmb/071B7700120_ESS_Contract_555350_7.pdf

Network Availability Across Precincts

Grapevine, 3/1/22



COGEmployee 🔒

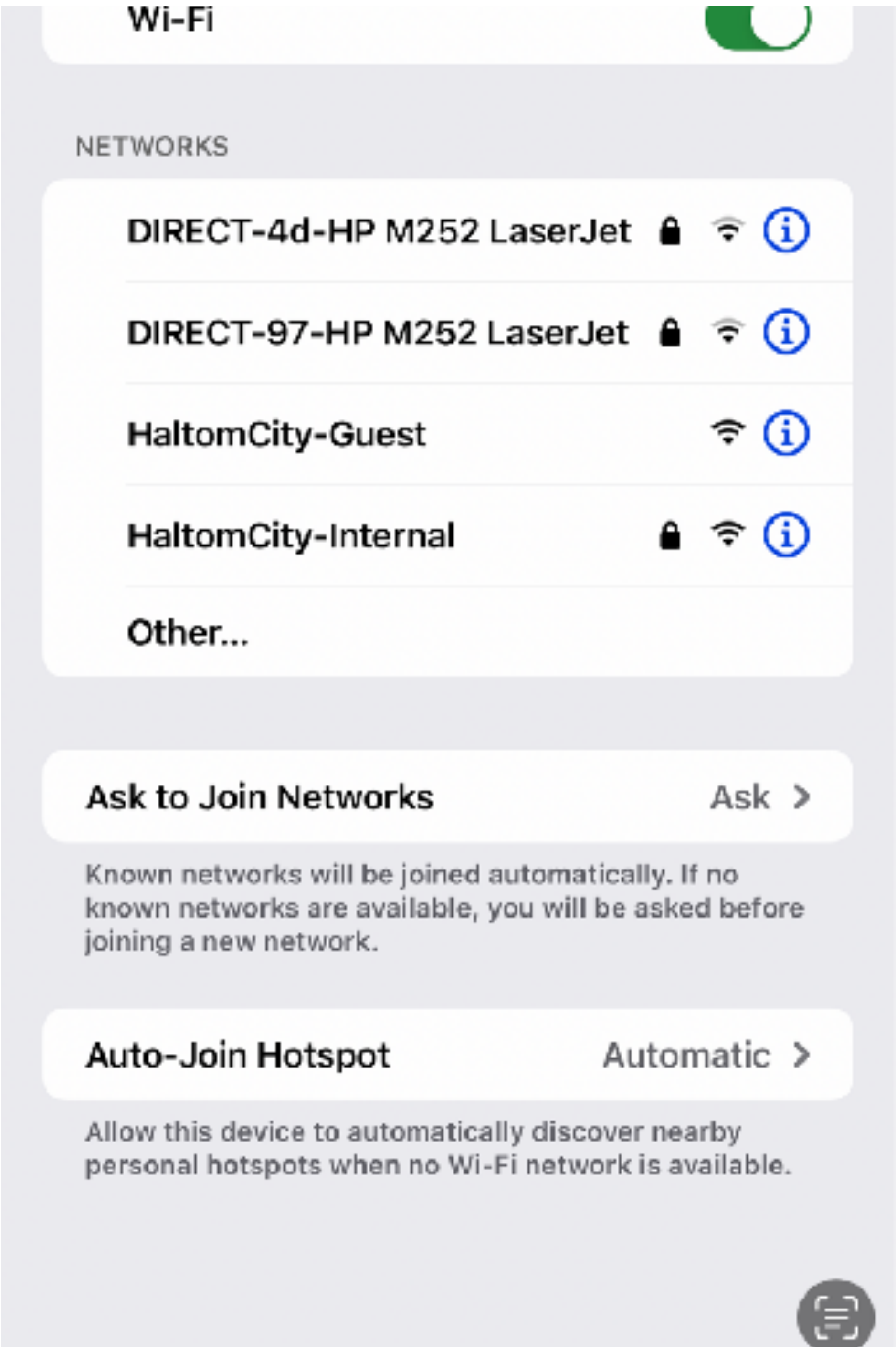
COGit 🔒

PSB_Employee 🔒

REC Guest

Student 🔒

Haltom City, 3/1/22



Wi-Fi

NETWORKS

DIRECT-4d-HP M252 LaserJet 🔒

DIRECT-97-HP M252 LaserJet 🔒

HaltomCity-Guest

HaltomCity-Internal 🔒

Other...

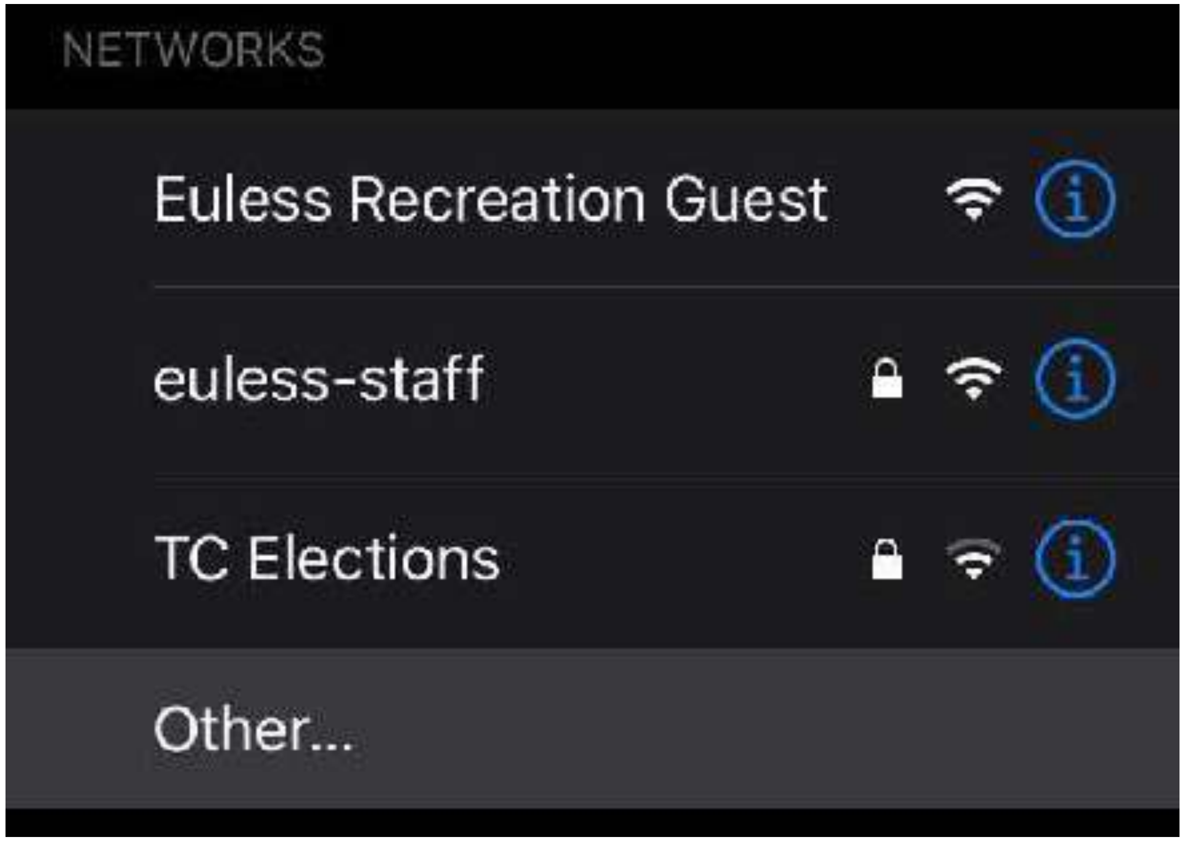
Ask to Join Networks — Ask >

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

Auto-Join Hotspot — Automatic >

Allow this device to automatically discover nearby personal hotspots when no Wi-Fi network is available.

Euless, 11/2/2021



NETWORKS

Euless Recreation Guest

euless-staff 🔒

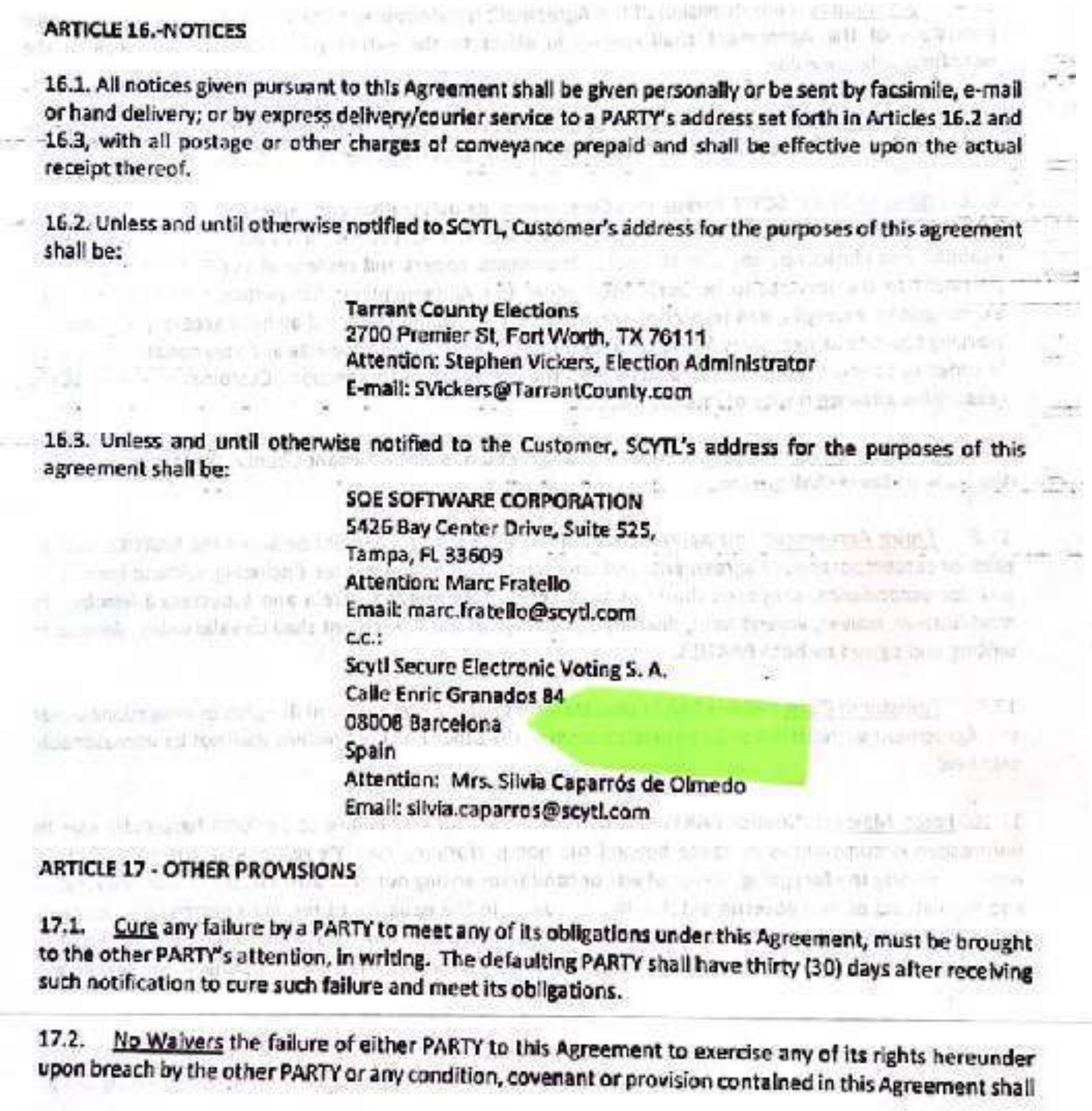
TC Elections 🔒

Other...

TARRANT COUNTY, TEXAS

Election Results 2020
Are our Votes Safe from Foreign Interference?

From Master Agreement Between Tarrant County and Scytl 2017



ARTICLE 16.-NOTICES

16.1. All notices given pursuant to this Agreement shall be given personally or be sent by facsimile, e-mail or hand delivery; or by express delivery/courier service to a PARTY's address set forth in Articles 16.2 and 16.3, with all postage or other charges of conveyance prepaid and shall be effective upon the actual receipt thereof.

16.2. Unless and until otherwise notified to SCYTL, Customer's address for the purposes of this agreement shall be:

Tarrant County Elections
2700 Premier St, Fort Worth, TX 76111
Attention: Stephen Vickers, Election Administrator
E-mail: SVickers@TarrantCounty.com

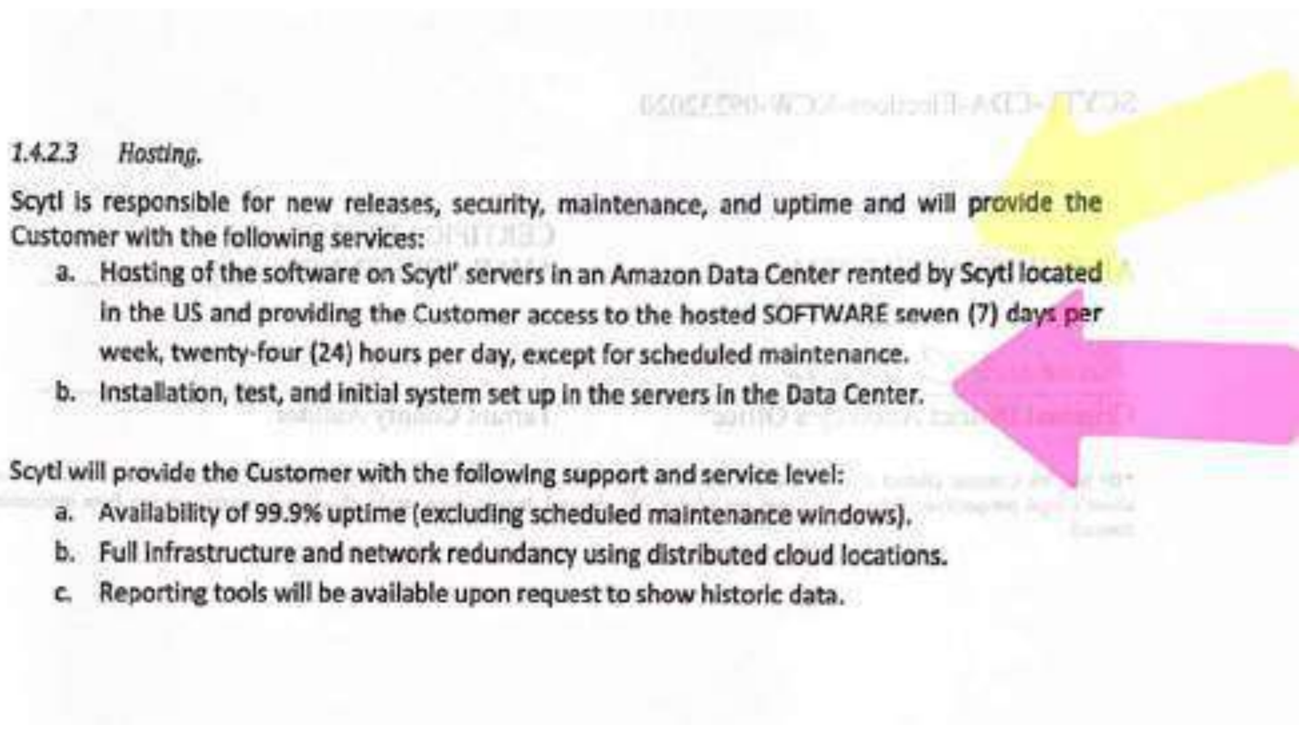
16.3. Unless and until otherwise notified to the Customer, SCYTL's address for the purposes of this agreement shall be:

SOE SOFTWARE CORPORATION
5426 Bay Center Drive, Suite 525,
Tampa, FL 33609
Attention: Marc Fratello
Email: marc.fratello@scytl.com
C.C.:
Scytl Secure Electronic Voting S. A.
Calle Enric Granados 84
08008 Barcelona
Spain
Attention: Mrs. Silvia Caparrós de Olmedo
Email: silvia.caparros@scytl.com

ARTICLE 17 - OTHER PROVISIONS

17.1. <u>Cure</u> any failure by a PARTY to meet any of its obligations under this Agreement, must be brought to the other PARTY's attention, in writing. The defaulting PARTY shall have thirty (30) days after receiving such notification to cure such failure and meet its obligations.

17.2. <u>No Waivers</u> the failure of either PARTY to this Agreement to exercise any of its rights hereunder upon breach by the other PARTY or any condition, covenant or provision contained in this Agreement shall



1.4.2.3 Hosting.

Scytl is responsible for new releases, security, maintenance, and uptime and will provide the Customer with the following services:

a. Hosting of the software on Scytl' servers in an Amazon Data Center rented by Scytl located in the US and providing the Customer access to the hosted SOFTWARE seven (7) days per week, twenty-four (24) hours per day, except for scheduled maintenance.

b. Installation, test, and initial system set up in the servers in the Data Center.

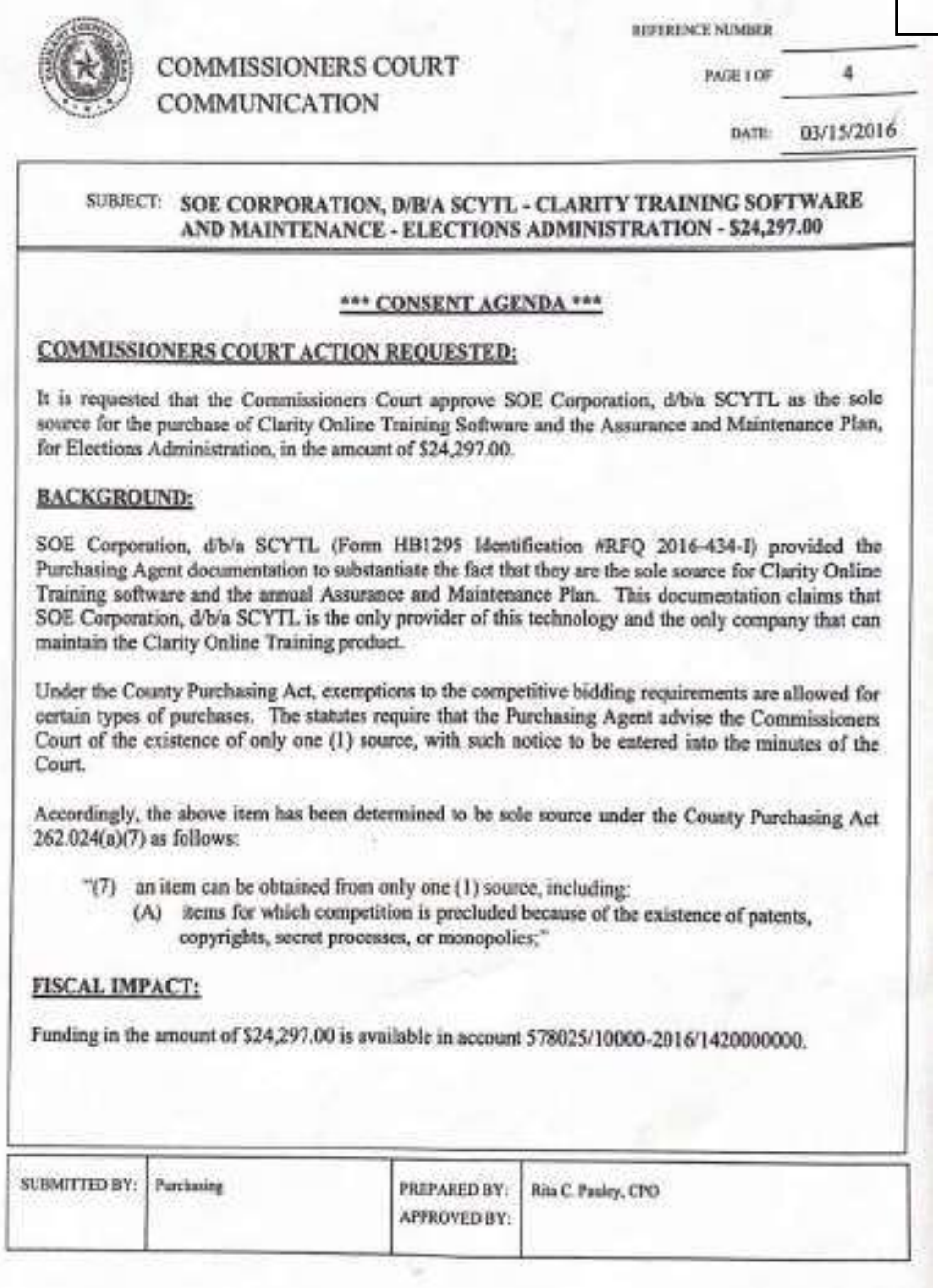
Scytl will provide the Customer with the following support and service level:

a. Availability of 99.9% uptime (excluding scheduled maintenance windows).

b. Full infrastructure and network redundancy using distributed cloud locations.

c. Reporting tools will be available upon request to show historic data.

2016-2017



COMMISSIONERS COURT COMMUNICATION

REFERENCE NUMBER

PAGE 1 OF 4

DATE: 03/15/2016

SUBJECT: SOE CORPORATION, D/B/A SCYTL - CLARITY TRAINING SOFTWARE AND MAINTENANCE - ELECTIONS ADMINISTRATION - $24,297.00

*** CONSENT AGENDA ***

COMMISSIONERS COURT ACTION REQUESTED:

It is requested that the Commissioners Court approve SOE Corporation, d/b/a SCYTL as the sole source for the purchase of Clarity Online Training Software and the Assurance and Maintenance Plan, for Elections Administration, in the amount of $24,297.00.

BACKGROUND:

SOE Corporation, d/b/a SCYTL (Form HB1295 Identification #RFQ 2016-434-I) provided the Purchasing Agent documentation to substantiate the fact that they are the sole source for Clarity Online Training software and the annual Assurance and Maintenance Plan. This documentation claims that SOE Corporation, d/b/a SCYTL is the only provider of this technology and the only company that can maintain the Clarity Online Training product.

Under the County Purchasing Act, exemptions to the competitive bidding requirements are allowed for certain types of purchases. The statutes require that the Purchasing Agent advise the Commissioners Court of the existence of only one (1) source, with such notice to be entered into the minutes of the Court.

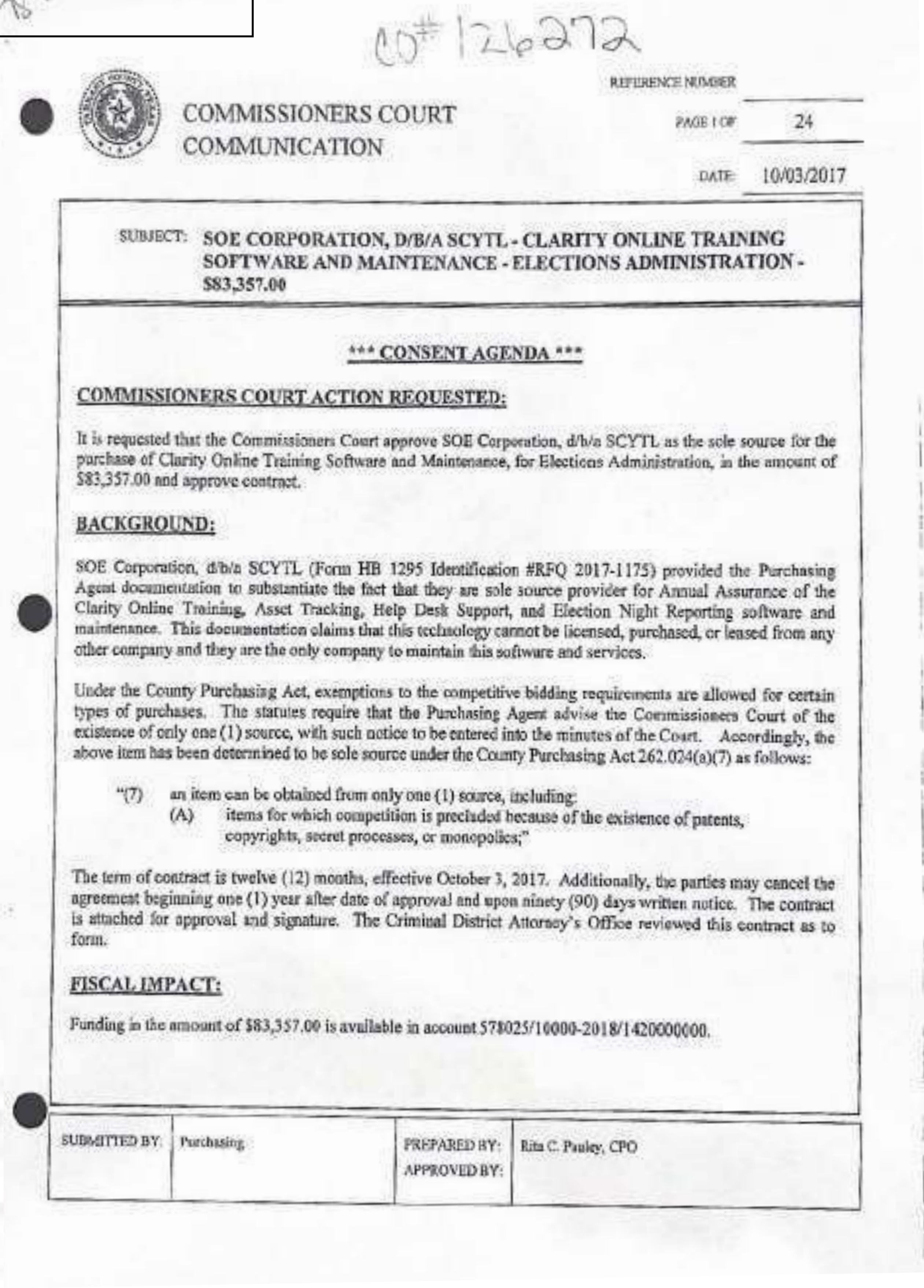
Accordingly, the above item has been determined to be sole source under the County Purchasing Act 262.024(a)(7) as follows:

"(7) an item can be obtained from only one (1) source, including:
(A) items for which competition is precluded because of the existence of patents, copyrights, secret processes, or monopolies;"

FISCAL IMPACT:

Funding in the amount of $24,297.00 is available in account 578025/10000-2016/1420000000.

SUBMITTED BY:	Purchasing	PREPARED BY: APPROVED BY:	Rita C. Pauley, CPO



CO# 126272

COMMISSIONERS COURT COMMUNICATION

REFERENCE NUMBER

PAGE 1 OF 24

DATE: 10/03/2017

SUBJECT: SOE CORPORATION, D/B/A SCYTL - CLARITY ONLINE TRAINING SOFTWARE AND MAINTENANCE - ELECTIONS ADMINISTRATION - $83,357.00

*** CONSENT AGENDA ***

COMMISSIONERS COURT ACTION REQUESTED:

It is requested that the Commissioners Court approve SOE Corporation, d/b/a SCYTL as the sole source for the purchase of Clarity Online Training Software and Maintenance, for Elections Administration, in the amount of $83,357.00 and approve contract.

BACKGROUND:

SOE Corporation, d/b/a SCYTL (Form HB 1295 Identification #RFQ 2017-1175) provided the Purchasing Agent documentation to substantiate the fact that they are sole source provider for Annual Assurance of the Clarity Online Training, Asset Tracking, Help Desk Support, and Election Night Reporting software and maintenance. This documentation claims that this technology cannot be licensed, purchased, or leased from any other company and they are the only company to maintain this software and services.

Under the County Purchasing Act, exemptions to the competitive bidding requirements are allowed for certain types of purchases. The statutes require that the Purchasing Agent advise the Commissioners Court of the existence of only one (1) source, with such notice to be entered into the minutes of the Court. Accordingly, the above item has been determined to be sole source under the County Purchasing Act 262.024(a)(7) as follows:

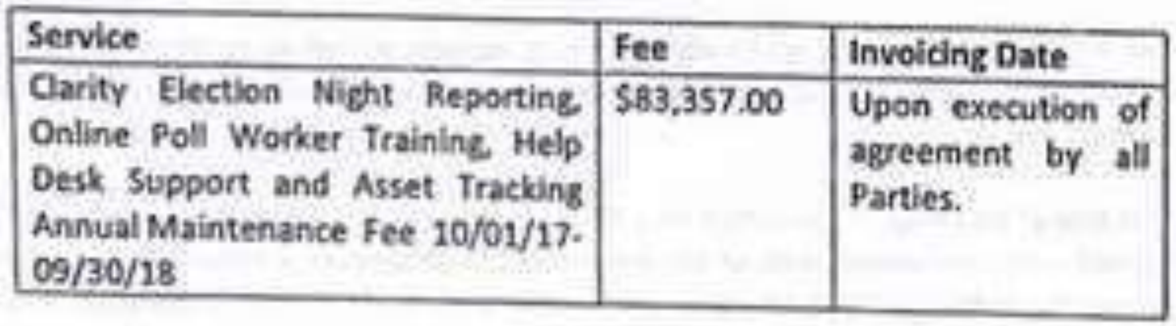
"(7) an item can be obtained from only one (1) source, including:
(A) items for which competition is precluded because of the existence of patents, copyrights, secret processes, or monopolies;"

The term of contract is twelve (12) months, effective October 3, 2017. Additionally, the parties may cancel the agreement beginning one (1) year after date of approval and upon ninety (90) days written notice. The contract is attached for approval and signature. The Criminal District Attorney's Office reviewed this contract as to form.

FISCAL IMPACT:

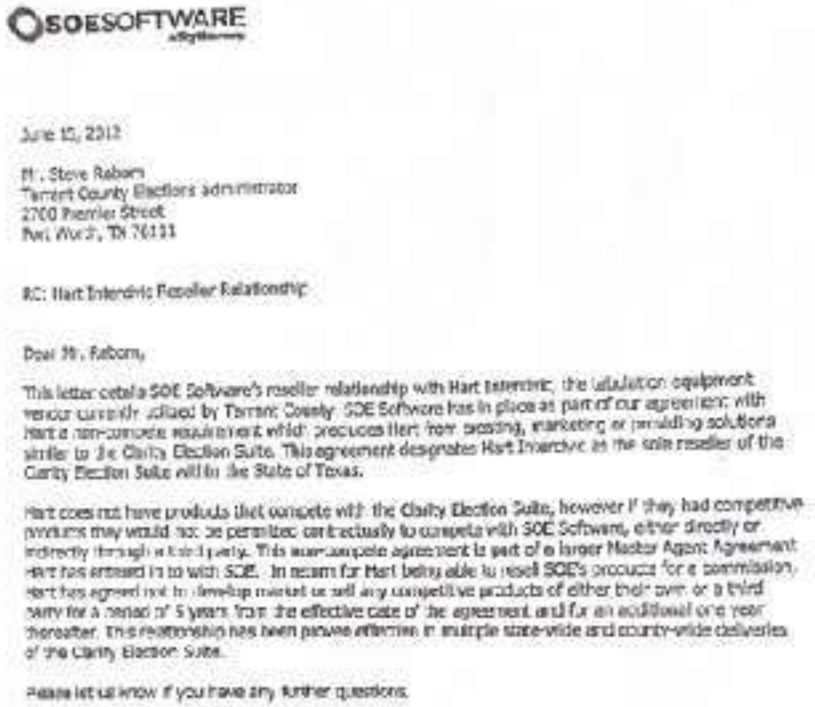
Funding in the amount of $83,357.00 is available in account 578025/10000-2018/1420000000.

SUBMITTED BY:	Purchasing	PREPARED BY: APPROVED BY:	Rita C. Pauley, CPO



Service	Fee	Invoicing Date
Clarity Election Night Reporting, Online Poll Worker Training, Help Desk Support and Asset Tracking Annual Maintenance Fee 10/01/17-09/30/18	$83,357.00	Upon execution of agreement by all Parties.

Portions of Old SOE D/B/A Scytl Contracts



SOESOFTWARE
a Scytl company

June 15, 2012

Mr. Steve Raborn
Tarrant County Elections administrator
2700 Premier Street
Fort Worth, TX 76111

RE: Hart Intercivic Reseller Relationship

Dear Mr. Raborn,

This letter details SOE Software's reseller relationship with Hart Intercivic, the tabulation equipment vendor currently utilized by Tarrant County. SOE Software has in place as part of our agreement with Hart a non-compete requirement which precludes Hart from creating, marketing or providing solutions similar to the Clarity Election Suite. This agreement designates Hart Intercivic as the sole reseller of the Clarity Election Suite within the State of Texas.

Hart does not have products that compete with the Clarity Election Suite, however if they had competitive products they would not be permitted contractually to compete with SOE Software, either directly or indirectly through a third party. This non-compete agreement is part of a larger Master Agent Agreement Hart has entered in to with SOE. In return for Hart being able to resell SOE's products for a commission, Hart has agreed not to develop market or sell any competitive products of either their own or a third party for a period of 5 years from the effective date of the agreement and for an additional one year thereafter. This relationship has been proven effective in multiple state-wide and county-wide deliveries of the Clarity Election Suite.

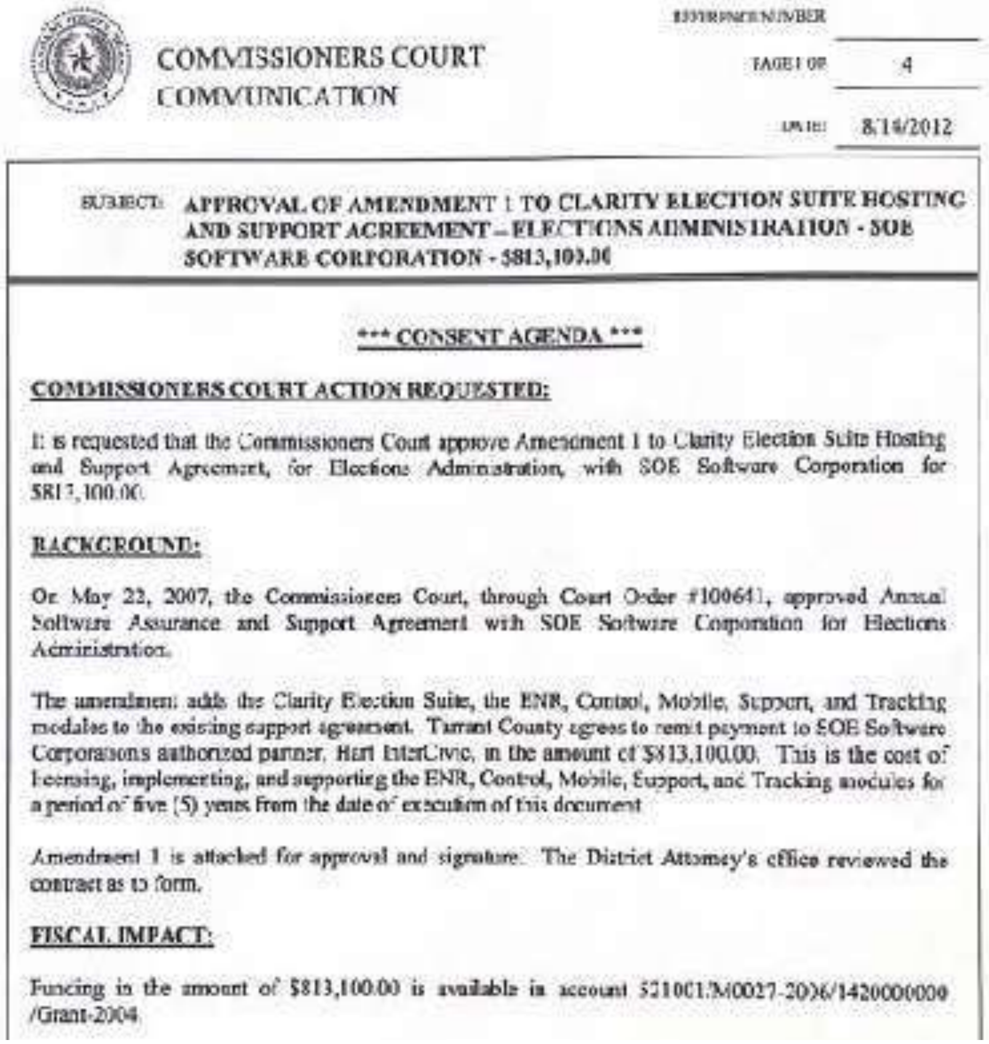
Please let us know if you have any further questions.

Best Regards,

Marc J. Fratello

Marc J. Fratello, CEO
SOE Software
3426 Bay Center Drive, Suite 500
Tampa, FL 33609
(813) 490-7140

2012



COMMISSIONERS COURT
COMMUNICATION

REFERENCE NUMBER	
PAGE 1 OF	4
DATE:	8/14/2012

SUBJECT: **APPROVAL OF AMENDMENT 1 TO CLARITY ELECTION SUITE HOSTING AND SUPPORT AGREEMENT – ELECTIONS ADMINISTRATION - SOE SOFTWARE CORPORATION - $813,100.00**

***** CONSENT AGENDA *****

COMMISSIONERS COURT ACTION REQUESTED:

It is requested that the Commissioners Court approve Amendment 1 to Clarity Election Suite Hosting and Support Agreement, for Elections Administration, with SOE Software Corporation for $813,100.00.

BACKGROUND:

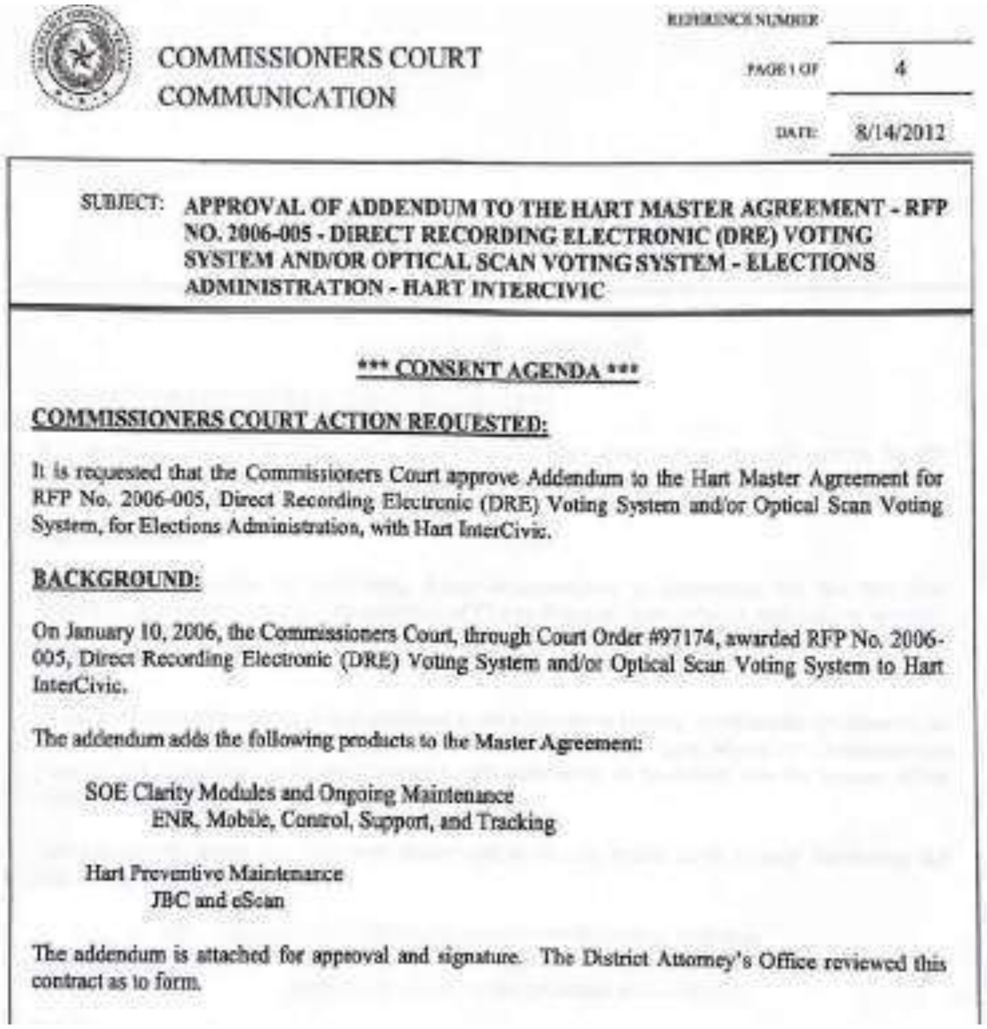
On May 22, 2007, the Commissioners Court, through Court Order #100641, approved Annual Software Assurance and Support Agreement with SOE Software Corporation for Elections Administration.

The amendment adds the Clarity Election Suite, the ENR, Control, Mobile, Support, and Tracking modules to the existing support agreement. Tarrant County agrees to remit payment to SOE Software Corporations authorized partner, Hart InterCivic, in the amount of $813,100.00. This is the cost of licensing, implementing, and supporting the ENR, Control, Mobile, Support, and Tracking modules for a period of five (5) years from the date of execution of this document.

Amendment 1 is attached for approval and signature. The District Attorney's office reviewed the contract as to form.

FISCAL IMPACT:

Funding in the amount of $813,100.00 is available in account 521001/M0027-2006/1420000000 /Grant-2004.



COMMISSIONERS COURT
COMMUNICATION

REFERENCE NUMBER	
PAGE 1 OF	4
DATE:	8/14/2012

SUBJECT: **APPROVAL OF ADDENDUM TO THE HART MASTER AGREEMENT - RFP NO. 2006-005 - DIRECT RECORDING ELECTRONIC (DRE) VOTING SYSTEM AND/OR OPTICAL SCAN VOTING SYSTEM - ELECTIONS ADMINISTRATION - HART INTERCIVIC**

***** CONSENT AGENDA *****

COMMISSIONERS COURT ACTION REQUESTED:

It is requested that the Commissioners Court approve Addendum to the Hart Master Agreement for RFP No. 2006-005, Direct Recording Electronic (DRE) Voting System and/or Optical Scan Voting System, for Elections Administration, with Hart InterCivic.

BACKGROUND:

On January 10, 2006, the Commissioners Court, through Court Order #97174, awarded RFP No. 2006-005, Direct Recording Electronic (DRE) Voting System and/or Optical Scan Voting System to Hart InterCivic.

The addendum adds the following products to the Master Agreement:

SOE Clarity Modules and Ongoing Maintenance
ENR, Mobile, Control, Support, and Tracking

Hart Preventive Maintenance
JBC and eScan

The addendum is attached for approval and signature. The District Attorney's Office reviewed this contract as to form.

ARTICLE 2. - SOFTWARE SUBSCRIPTION

2.1. Provision of the SOFTWARE. Under the terms and conditions hereunder agreed SCYTL provides the Customer with (i) the SOFTWARE as SaaS; (ii) Maintenance and support services as defined in Article 4; and (iii) hosting for the SOFTWARE (all of them referred hereinafter as the Subscription).

2.2. Grant of License. Subject to the terms and conditions of this Agreement and payment of the Subscription fees, Scytl hereby grants the Customer a non-exclusive, non-perpetual, non-transferable license to use the SOFTWARE and the Documentation for internal purposes.

2.3. Reservation of Rights. The SOFTWARE and Documentation are licensed, not sold. SCYTL and affiliates own and shall retain all right, title and interest (including without limitation all patent rights, copyrights, trademark rights, trade secret rights and all other intellectual property rights), in and to the SOFTWARE and Documentation and any copies, corrections, bug fixes, enhancements, modifications, Updates, Upgrades, or new versions thereof, all of which shall be deemed part of the SOFTWARE, as the case may be, and subject to all of the provisions of this Agreement. The Customer shall keep the SOFTWARE and Documentation free and clear of all liens, encumbrances and/or security interests. No rights are granted to the Customer pursuant to this Agreement other than as expressly set forth in this Agreement.

2.4. Restrictions. The Customer shall not (and shall not allow its customers or any third party) to: (a) modify, translate, reverse engineer, decompile, disassemble, or create derivative works based on the SOFTWARE and/or Documentation, except to the extent that such restriction is permitted by applicable law; (b) circumvent any user limits or other license timing or use restrictions that are built into the SOFTWARE; (c) sell, resell, rent, lend, transfer, distribute, license, sublicense or grant any rights in the SOFTWARE and/or Documentation in any form to any person without the written consent of Scytl except for the right to authorize the use of the SOFTWARE by its customers under the terms and conditions hereunder agreed; (d) remove any proprietary notices, labels, or marks from the SOFTWARE and/or Documentation except those trademarks which are configurable; (e) unbundle any component of the SOFTWARE and/or Documentation; (f) build a product or service that is competitive with the SOFTWARE; (g) copy any ideas, features, functions or graphics of the SOFTWARE and/or Documentation; (h) copy, frame or mirror any part of the SOFTWARE; (i) permit any third party to access the administrative portion of the SOFTWARE or (ii) use the SOFTWARE and/or the Documentation in violation of applicable laws.

ARTICLE 3. - HOSTING AND INSTALLATION

3.1. SCYTL shall provide the Customer with the following services included in the Subscription Fee as defined in Article 2.

a. Hosting of the SOFTWARE in SCYTL's servers in a Cloud Hosted Data Center rented by SCYTL located in the US and providing the Customer access to the hosted SOFTWARE seven (7) days per week, twenty four (24) hours per day except for scheduled maintenance, which must be previously agreed to by both PARTIES.
b. Installation, test and initial system set up in the servers in the Data Center.
c. Standard documentation including setup and back-office user guides in English.

3.2. SCYTL shall provide the Customer with the following hosting support and service level:

a. Availability of 99.9% uptime (excluding scheduled maintenance windows).
b. Reporting tools will be available upon request to show historic data.
c. Full infrastructure and network redundancy using distributed cloud locations.

ARTICLE 4. - MAINTENANCE AND SUPPORT

4.1. During the Term of this Agreement SCYTL shall provide the Customer with maintenance services and third level support in accordance with the Service Level Agreement attached hereto as an Appendix 1, being integral part of this Agreement, which shall consist of (i) the updating and upgrading of the SOFTWARE and (ii) the modification and/or adaptation of the SOFTWARE in order to correct and solve any defects, errors or malfunctions in the SOFTWARE;

4.2 The PARTIES have appointed the following persons as their respective Single Point of Contact (SPOC)

CUSTOMER: Stephen Vickers
Email: svickers@Tarrantcounty.com

SCYTL: Wendy Williams
Email: Wendy.Williams@Scytl.com

ARTICLE 5. - CUSTOMER AND CUSTOMER DATA

5.1. As between SCYTL and the Customer, Customer exclusively owns all rights, title and interest in and to all its Data. Upon termination of the contract, SCYTL will assist the Customer with the transfer of Customer files, election data, documentation, and other materials (at no additional cost), with the understanding that the ENR, Support, Training, and Asset Tracking software themselves are pre-existing solutions and remain the sole intellectual property of SCYTL. Both PARTIES will determine an agreed upon timeframe for the return of the data.

5.2. SCYTL shall not access Customer's Data, except to prevent or respond to service or technical problems or otherwise at Customer request. SCYTL shall not disclose any Customer Data except as compelled by law or as expressly permitted in writing by Customer.

ARTICLE 6. - DATA PROTECTION

6.1. In order to provide Maintenance and Support Services, under this Agreement SCYTL may need to have access or process personal data under the control of the Customer. In that case, SCTYL, as data processor, undertakes to comply with the requirements set forth in the applicable data protection laws and regulations and, in particular:

a. To process the personal data only in accordance with the instructions provided by the Customer as data controller;
b. To not apply or use the personal data for a purpose other than set out in this Agreement, and
c. To not communicate the personal data to other persons even for their preservation.

1 Software Maintenance and Support – Technical Service description

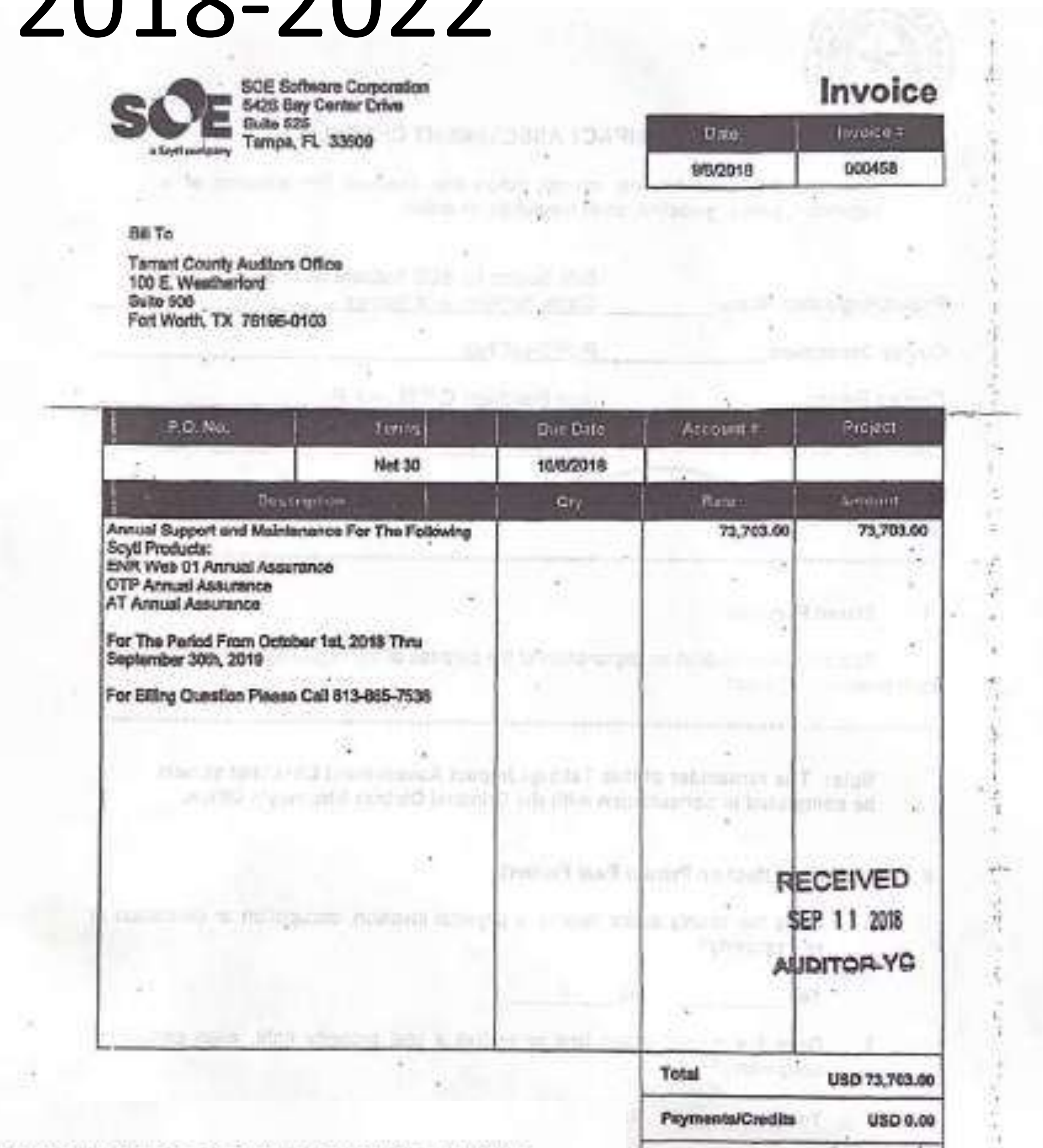
1.1 Definitions

The definitions used in the Agreement are incorporated herein by reference. In addition, the following terms shall have the following meaning:

- **"Software maintenance"** is defined as the process of modifying a software system or component after delivery to correct faults, errors and bugs, to improve performance or other attributes, or adapt to a changed environment.
- **"Perfective maintenance"** includes modifications and upgrades done in order to keep the software usable over a long period of time. It includes new features and new user requirements for refining the software and improving its reliability and performance.
- **"Adaptive maintenance"** includes modifications and upgrades applied to keep the software product up-to date and tuned to the changing environment.
- **"Preventive maintenance"** includes modifications and upgrades to prevent future issues of the software. It aims to attend problems, which are not significant at this moment but may cause serious issues in future.
- **"Corrective maintenance"** includes modifications and upgrades done in order to correct or fix faults, errors and bugs, which are either discovered by the Customer or concluded by user error reports.
- **Response time** means the time elapsing between the reporting of an Issue by a Customer and the response from a Scytl's Technical Support Services engineer acknowledging receipt of the reported Issue.
- **Diagnosis time** means the time elapsing between the Response time and the diagnosis of the Issue made by Scytl's Technical Support Services.
- **"Issue"** means either
  a) A failure of the Software to conform to the specifications set out in the documentation relating to that version of the Software, resulting in the inability to use, or restriction in the use of the Software, or
  b) A problem in current features requiring new procedures, clarifications, additional information and/or requests for product enhancements.
- **"Resolution or patch or Bug Fix"** means either a software modification or addition that, when made or added to the Software, corrects an Issue, or a procedure or routine that, when observed in the regular installation or operation of the Software, eliminates the practical adverse effect of the issue on you.

- **"Upgrade"** means a revision or change of version of the Software released by Scytl to its end user customers generally, during the Support Services Term, to add new and different functions or to increase the capacity of the Software.
- **"Maintenance Release"** is a release of or for the Software that includes the most recent Patches and Upgrades.
- **"Current Software Version"** means the most recently released commercially available version of the Software at the time a Customer Support Contact relates a particular support incident to Scytl hereunder.
- **"Supported Versions"**. SCYTL' obligations with respect to the Maintenance Services shall apply only to those versions of the Software that are within one (1) year time frame of Current Software Version.
- **"Hosted System"** means Software hosted by Scytl externally in its data center to which the Customer may access it over the internet from anywhere at any time.

2018-2022



SOE Software Corporation
5426 Bay Center Drive
Suite 525
Tampa, FL 33609

a Scytl company

Invoice

Date	Invoice #
9/6/2018	000458

Bill To

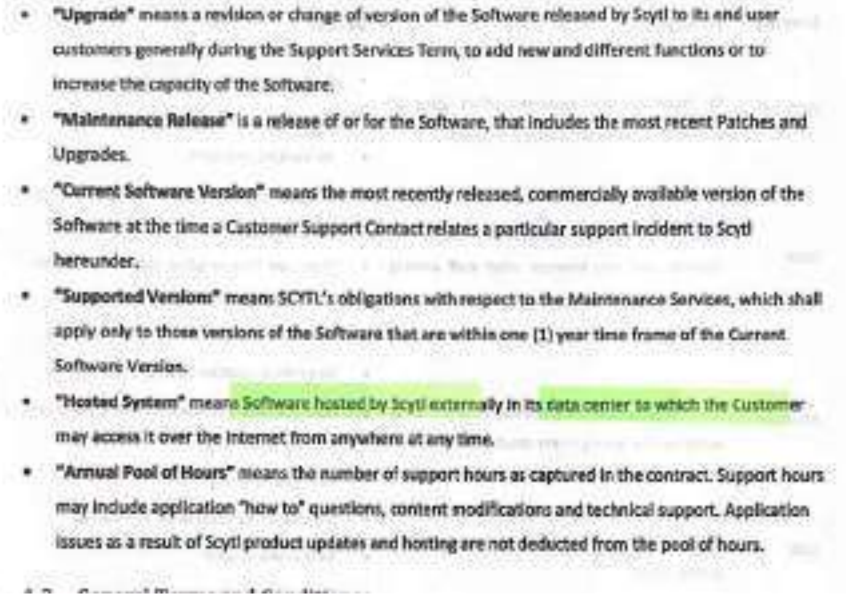
Tarrant County Auditors Office
100 E. Weatherford
Suite 506
Fort Worth, TX 76196-0103

P.O. No.	Terms	Due Date	Account #	Project
	Net 30	10/6/2018		

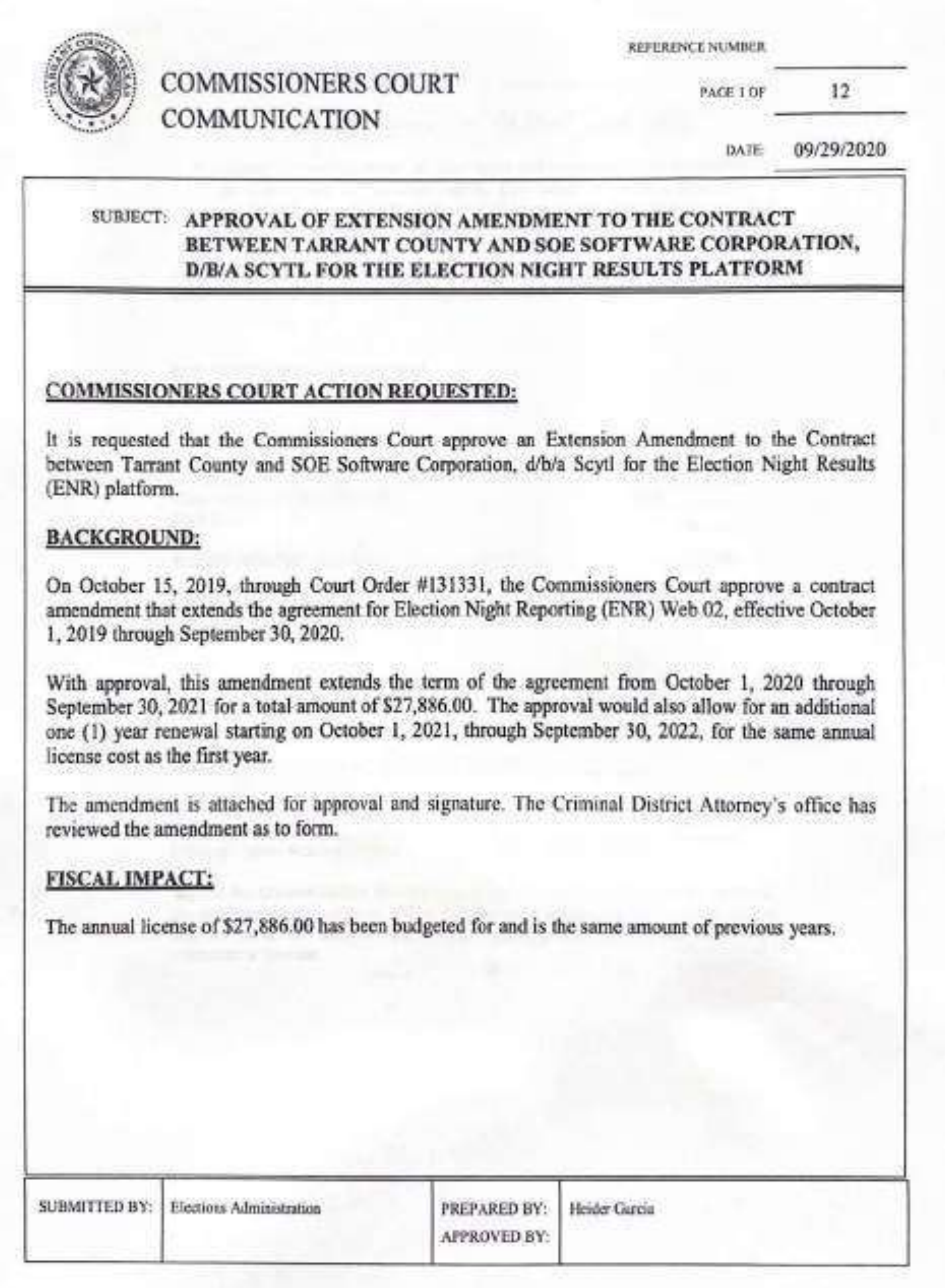
Description	Qty	Rate	Amount
Annual Support and Maintenance For The Following Scytl Products: ENR Web 01 Annual Assurance OTP Annual Assurance AT Annual Assurance For The Period From October 1st, 2018 Thru September 30th, 2019 For Billing Question Please Call 813-865-7536		73,703.00	73,703.00

RECEIVED
SEP 11 2018
AUDITOR-YC

Total	USD 73,703.00
Payments/Credits	USD 0.00
Balance Due	USD 73,703.00



- **"Upgrade"** means a revision or change of version of the Software released by Scytl to its end user customers generally during the Support Services Term, to add new and different functions or to increase the capacity of the Software.
- **"Maintenance Release"** is a release of or for the Software, that includes the most recent Patches and Upgrades.
- **"Current Software Version"** means the most recently released, commercially available version of the Software at the time a Customer Support Contact relates a particular support incident to Scytl hereunder.
- **"Supported Versions"** means SCYTL's obligations with respect to the Maintenance Services, which shall apply only to those versions of the Software that are within one (1) year time frame of the Current Software Version.
- **"Hosted System"** means Software hosted by Scytl externally in its data center to which the Customer may access it over the Internet from anywhere at any time.
- **"Annual Pool of Hours"** means the number of support hours as captured in the contract. Support hours may include application "how to" questions, content modifications and technical support. Application issues as a result of Scytl product updates and hosting are not deducted from the pool of hours.



COMMISSIONERS COURT
COMMUNICATION

REFERENCE NUMBER

PAGE 1 OF 12

DATE: 09/29/2020

SUBJECT: **APPROVAL OF EXTENSION AMENDMENT TO THE CONTRACT BETWEEN TARRANT COUNTY AND SOE SOFTWARE CORPORATION, D/B/A SCYTL FOR THE ELECTION NIGHT RESULTS PLATFORM**

COMMISSIONERS COURT ACTION REQUESTED:

It is requested that the Commissioners Court approve an Extension Amendment to the Contract between Tarrant County and SOE Software Corporation, d/b/a Scytl for the Election Night Results (ENR) platform.

BACKGROUND:

On October 15, 2019, through Court Order #131331, the Commissioners Court approve a contract amendment that extends the agreement for Election Night Reporting (ENR) Web 02, effective October 1, 2019 through September 30, 2020.

With approval, this amendment extends the term of the agreement from October 1, 2020 through September 30, 2021 for a total amount of $27,886.00. The approval would also allow for an additional one (1) year renewal starting on October 1, 2021, through September 30, 2022, for the same annual license cost as the first year.

The amendment is attached for approval and signature. The Criminal District Attorney's office has reviewed the amendment as to form.

FISCAL IMPACT:

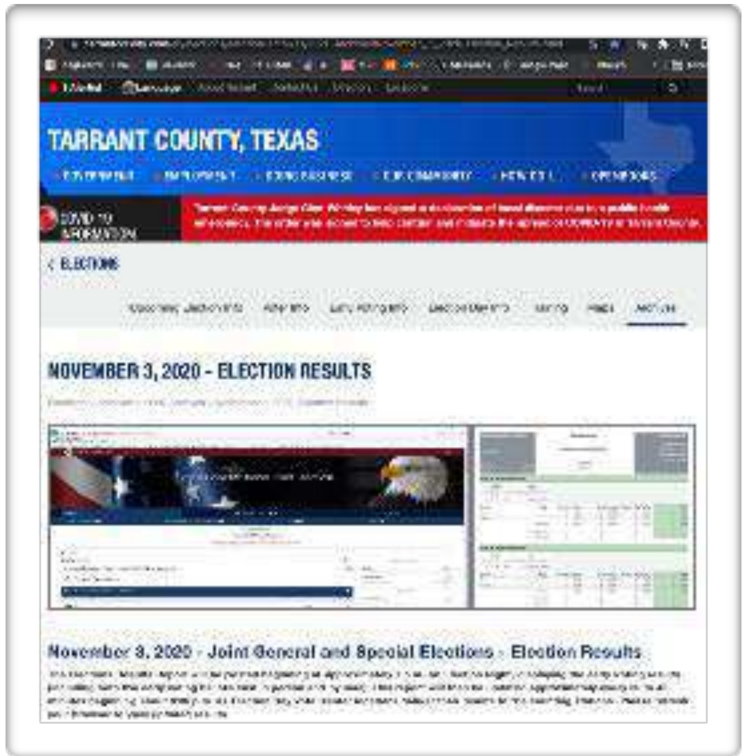
The annual license of $27,886.00 has been budgeted for and is the same amount of previous years.

SUBMITTED BY:	Elections Administration	PREPARED BY: APPROVED BY:	Heider Garcia

November 3, 2020
Election Results

- Tarrant County archives
- TarrantCounty.com URL
- URL property of Tarrant County

→



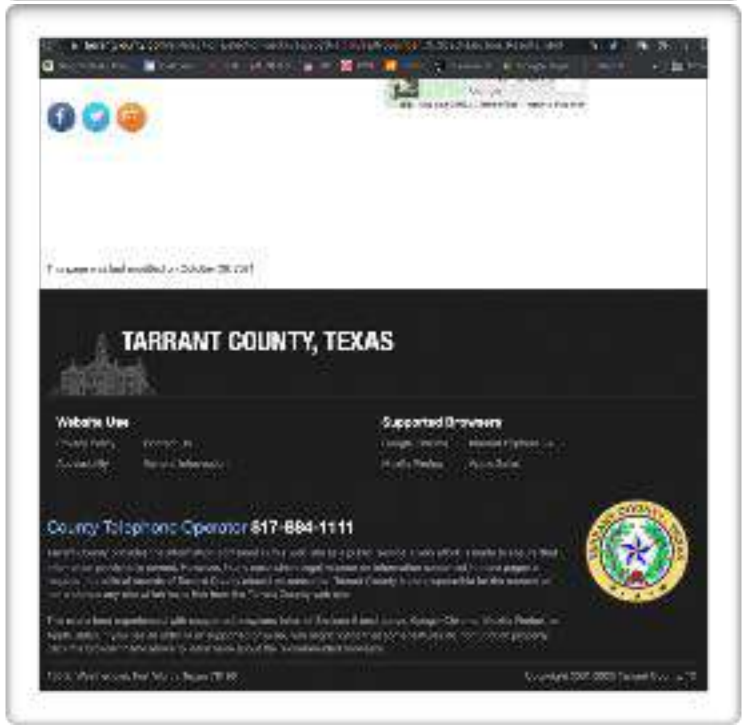
TARRANT COUNTY, TEXAS

COVID-19 INFORMATION

‹ ELECTIONS

NOVEMBER 3, 2020 - ELECTION RESULTS

November 3, 2020 - Joint General and Special Elections - Election Results



TARRANT COUNTY, TEXAS

Website Use

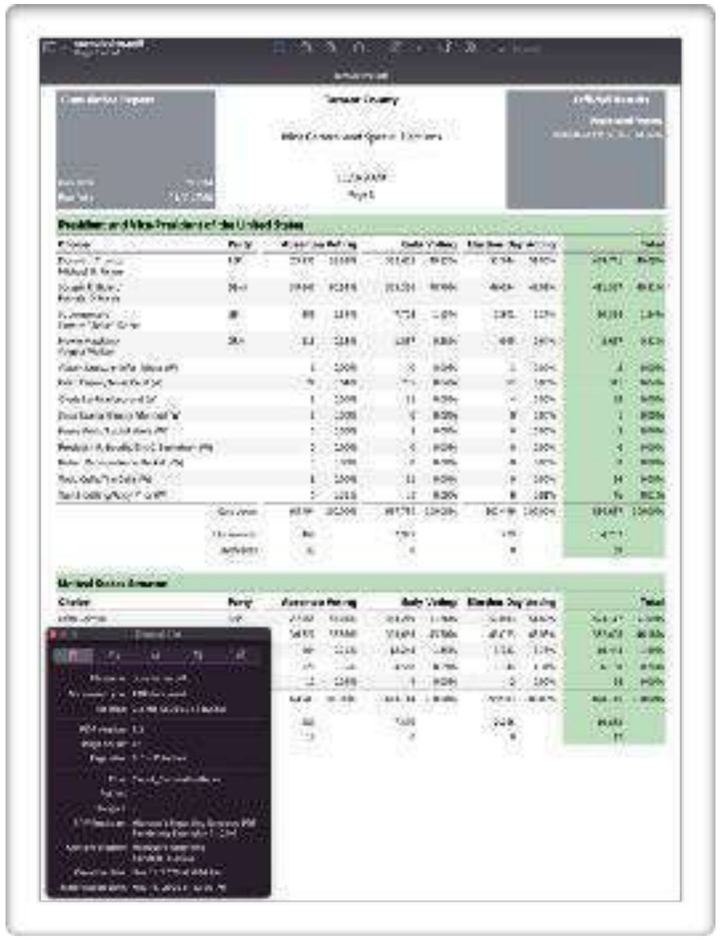
Supported Browsers

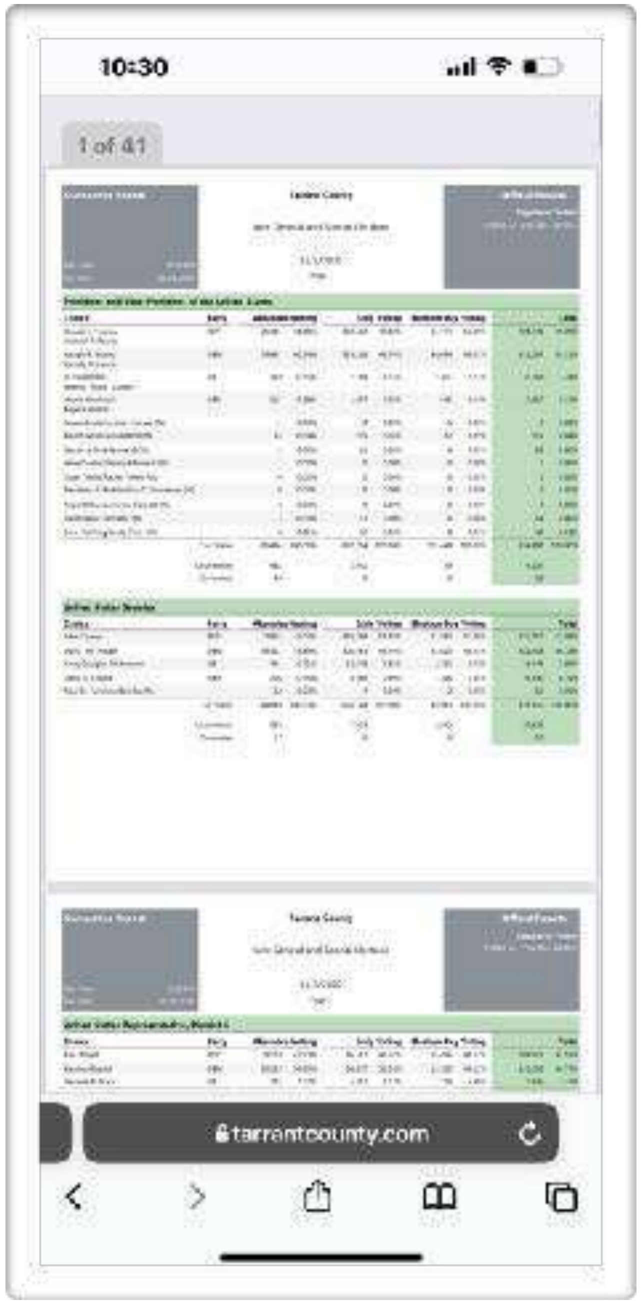
County Telephone Operator 817-884-1111

→

View a Cumulative Report

- Cumulative Reports listed on Tarrant's web page
- Click on View a Cumulate Report on Tarrant's web page
- Cumulative PDF created by Microsoft Reporting Services 11.0.0.0 from web page
- While doing a search on cell phone cumulative report shows to be on <u>TarrantCounty.com</u>





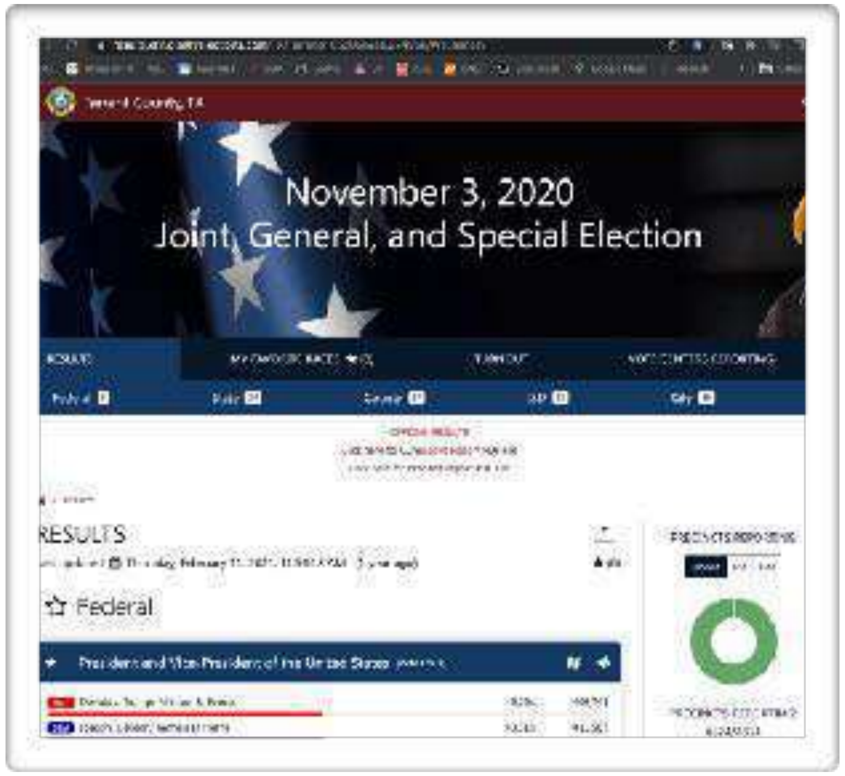
View the graphical Election Night Reporting Tool (ENR)

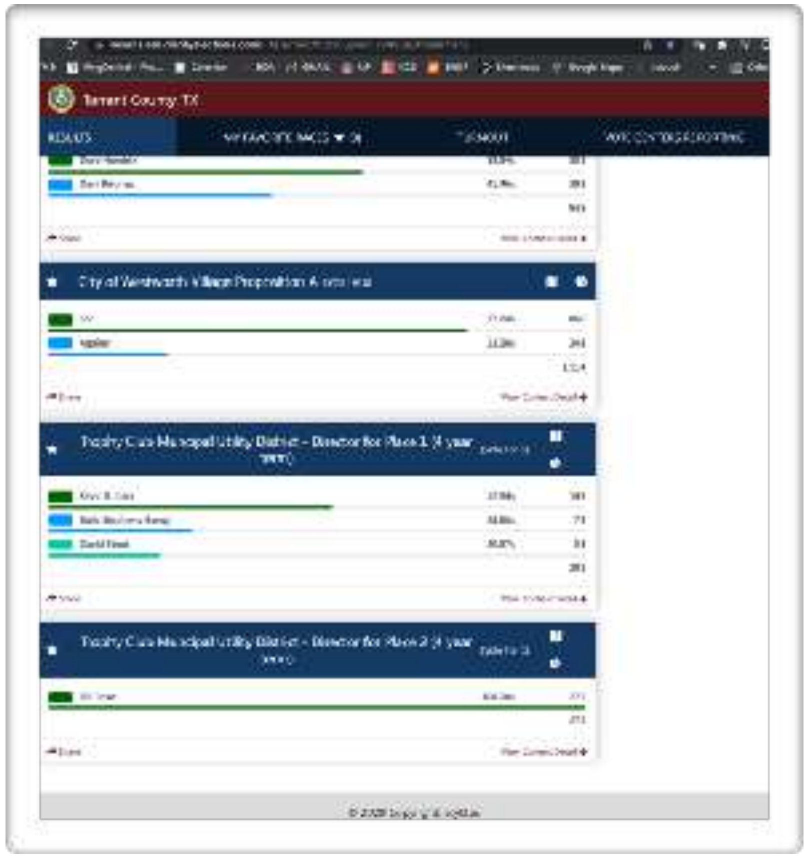
- Graphical Election Night Reporting Tool (ENR) listed on Tarrant's web page

- Click on graphical Election Night Reporting Tool (ENR) listed on Tarrant's web page

- Election Night Reporting Tool (ENR) directs age to ClarityElecitons.com

- Clarity Elections property of scytl.us


Tarrant County, TX
November 3, 2020
Joint, General, and Special Election
RESULTS
Federal
President and Vice President of the United States


Tarrant County, TX
RESULTS
City of Westworth Village Proposition A
Trophy Club Municipal Utility District - Director for Place 1
Trophy Club Municipal Utility District - Director for Place 2

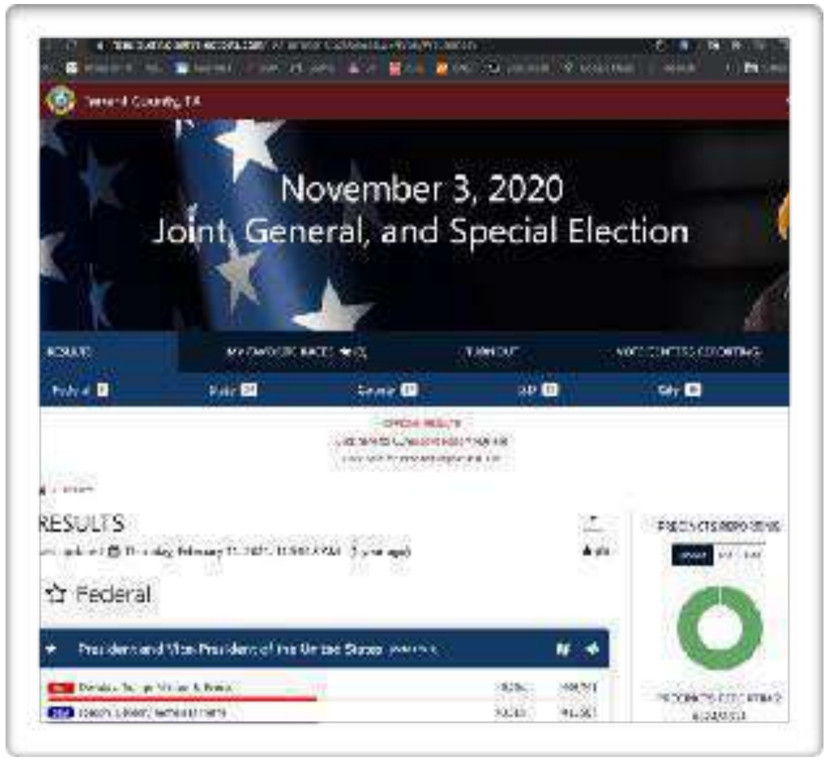
Viewing Official Results from ClarityElections.com | Scytl.us

- From ClarityElections.com | scytl.us voters can view official results from election as a cumulative report PDF file and precinct report PDF file

- Once reports are selected voter is directed back to Tarrant's URLs below

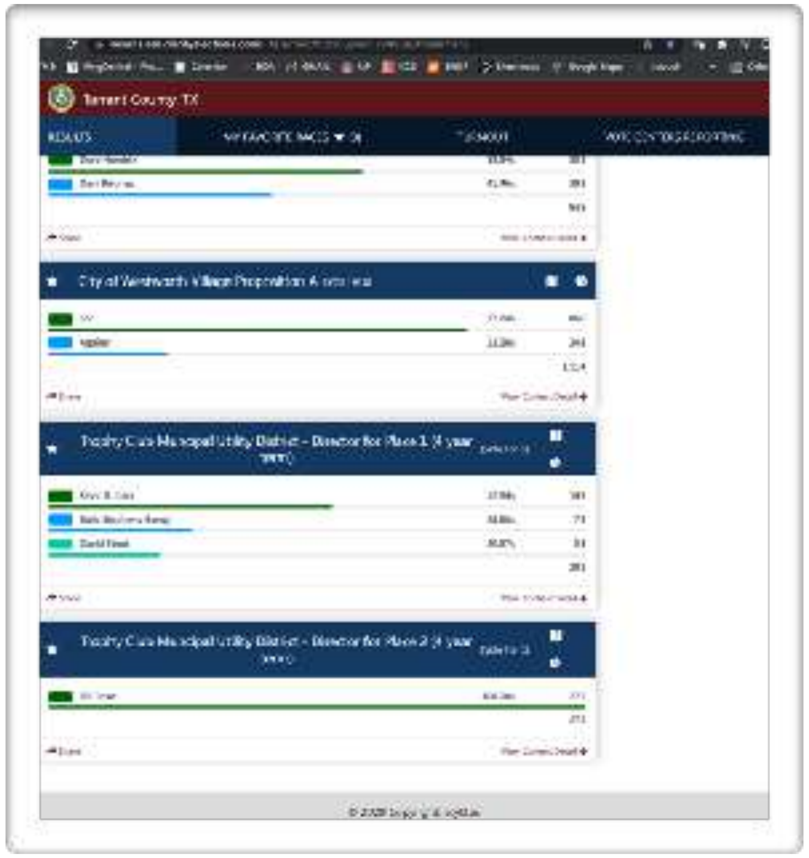
- Cumulative Report: http://access.tarrantcounty.com/content/dam/main/elections/2020/1120/reports/cumulative.pdf

- Precinct Report: http://access.tarrantcounty.com/content/dam/main/elections/2020/1120/reports/precinct.pdf



Tarrant County, TX

November 3, 2020
Joint, General, and Special Election



Tarrant County, TX

Resources

- Tarrant County Archives - https://www.tarrantcounty.com/en/elections/election-archives/2020-archives/November_3_2020-Election_Results.html

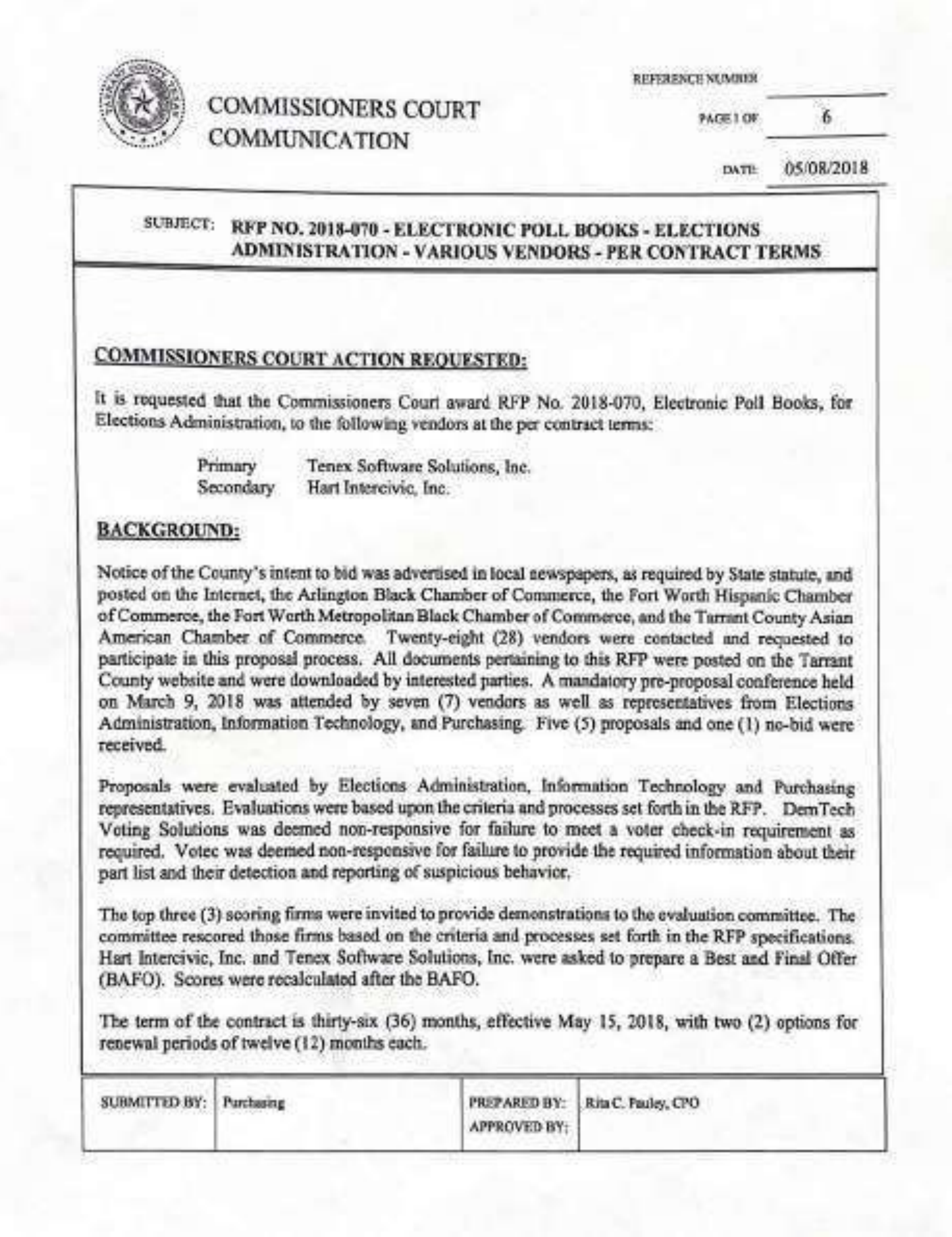
- Election Night Reporting Tool (ENR) - Clarity Elections https://results.enr.clarityelections.com/TX/Tarrant/105205/web.274956/#/summary

- Clarity Elections - Scytl - https://scytl.us/

- Will They Steal the 2020 Elections? https://www.youtube.com/watch?v=pCSAHEOY75E&list=PL6ANpEeO1X_OdGF-Oqm9Oi1xhp0dSNTqR&index=4

EPOLLBOOK

TARRANT ENDS CONTRACT WITH VOTEC;
AND SIGNS WITH TENEX IN 2018



COMMISSIONERS COURT
COMMUNICATION

REFERENCE NUMBER

PAGE 1 OF 6

DATE: 05/08/2018

SUBJECT: RFP NO. 2018-070 - ELECTRONIC POLL BOOKS - ELECTIONS ADMINISTRATION - VARIOUS VENDORS - PER CONTRACT TERMS

COMMISSIONERS COURT ACTION REQUESTED:

It is requested that the Commissioners Court award RFP No. 2018-070, Electronic Poll Books, for Elections Administration, to the following vendors at the per contract terms:

Primary	Tenex Software Solutions, Inc.
Secondary	Hart Intercivic, Inc.

BACKGROUND:

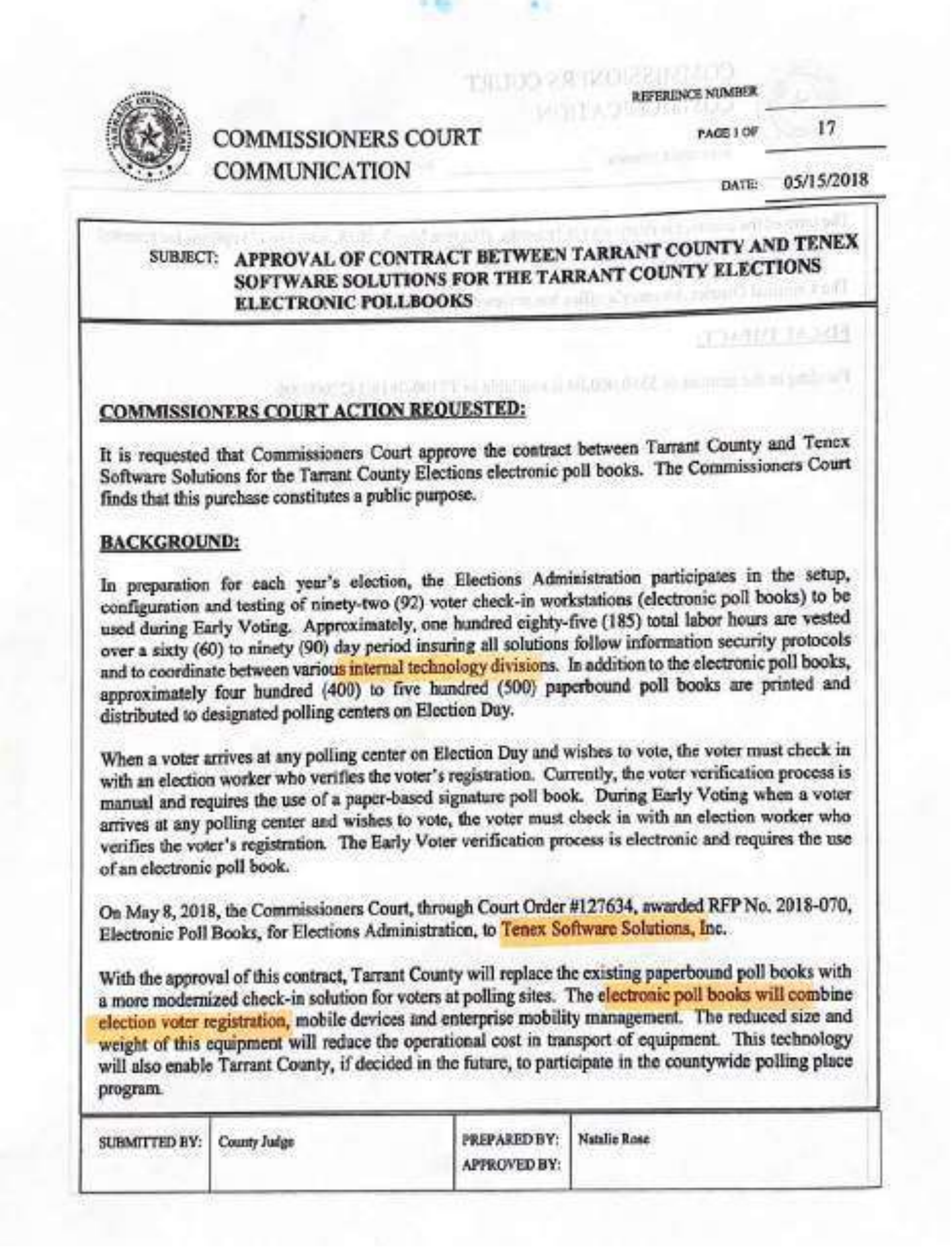
Notice of the County's intent to bid was advertised in local newspapers, as required by State statute, and posted on the Internet, the Arlington Black Chamber of Commerce, the Fort Worth Hispanic Chamber of Commerce, the Fort Worth Metropolitan Black Chamber of Commerce, and the Tarrant County Asian American Chamber of Commerce. Twenty-eight (28) vendors were contacted and requested to participate in this proposal process. All documents pertaining to this RFP were posted on the Tarrant County website and were downloaded by interested parties. A mandatory pre-proposal conference held on March 9, 2018 was attended by seven (7) vendors as well as representatives from Elections Administration, Information Technology, and Purchasing. Five (5) proposals and one (1) no-bid were received.

Proposals were evaluated by Elections Administration, Information Technology and Purchasing representatives. Evaluations were based upon the criteria and processes set forth in the RFP. DemTech Voting Solutions was deemed non-responsive for failure to meet a voter check-in requirement as required. Votec was deemed non-responsive for failure to provide the required information about their part list and their detection and reporting of suspicious behavior.

The top three (3) scoring firms were invited to provide demonstrations to the evaluation committee. The committee rescored those firms based on the criteria and processes set forth in the RFP specifications. Hart Intercivic, Inc. and Tenex Software Solutions, Inc. were asked to prepare a Best and Final Offer (BAFO). Scores were recalculated after the BAFO.

The term of the contract is thirty-six (36) months, effective May 15, 2018, with two (2) options for renewal periods of twelve (12) months each.

SUBMITTED BY:	Purchasing	PREPARED BY: APPROVED BY:	Rita C. Pauley, CPO



COMMISSIONERS COURT
COMMUNICATION

REFERENCE NUMBER

PAGE 1 OF 17

DATE: 05/15/2018

SUBJECT: APPROVAL OF CONTRACT BETWEEN TARRANT COUNTY AND TENEX SOFTWARE SOLUTIONS FOR THE TARRANT COUNTY ELECTIONS ELECTRONIC POLLBOOKS

COMMISSIONERS COURT ACTION REQUESTED:

It is requested that Commissioners Court approve the contract between Tarrant County and Tenex Software Solutions for the Tarrant County Elections electronic poll books. The Commissioners Court finds that this purchase constitutes a public purpose.

BACKGROUND:

In preparation for each year's election, the Elections Administration participates in the setup, configuration and testing of ninety-two (92) voter check-in workstations (electronic poll books) to be used during Early Voting. Approximately, one hundred eighty-five (185) total labor hours are vested over a sixty (60) to ninety (90) day period insuring all solutions follow information security protocols and to coordinate between various internal technology divisions. In addition to the electronic poll books, approximately four hundred (400) to five hundred (500) paperbound poll books are printed and distributed to designated polling centers on Election Day.

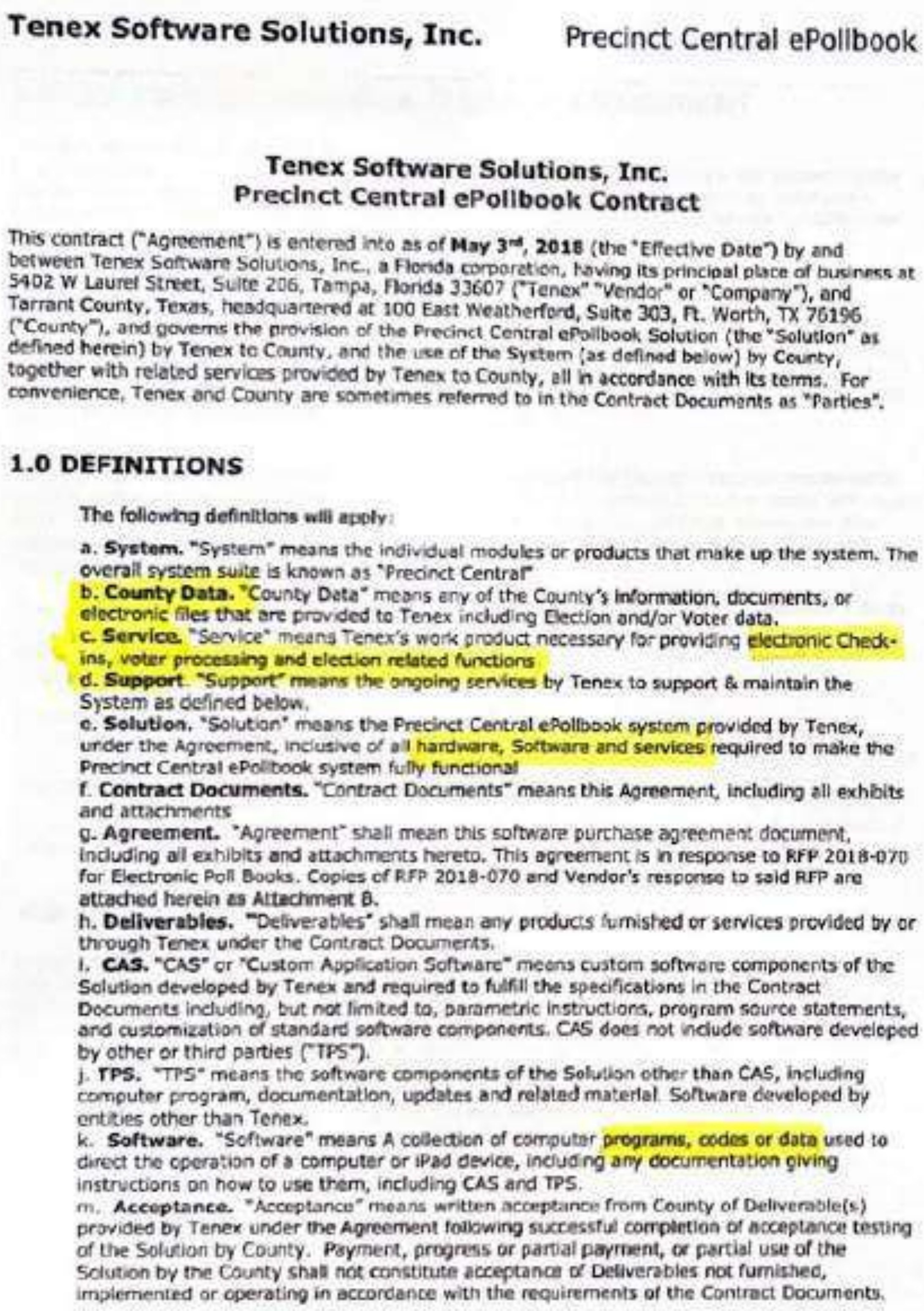
When a voter arrives at any polling center on Election Day and wishes to vote, the voter must check in with an election worker who verifies the voter's registration. Currently, the voter verification process is manual and requires the use of a paper-based signature poll book. During Early Voting when a voter arrives at any polling center and wishes to vote, the voter must check in with an election worker who verifies the voter's registration. The Early Voter verification process is electronic and requires the use of an electronic poll book.

On May 8, 2018, the Commissioners Court, through Court Order #127634, awarded RFP No. 2018-070, Electronic Poll Books, for Elections Administration, to Tenex Software Solutions, Inc.

With the approval of this contract, Tarrant County will replace the existing paperbound poll books with a more modernized check-in solution for voters at polling sites. The electronic poll books will combine election voter registration, mobile devices and enterprise mobility management. The reduced size and weight of this equipment will reduce the operational cost in transport of equipment. This technology will also enable Tarrant County, if decided in the future, to participate in the countywide polling place program.

SUBMITTED BY:	County Judge	PREPARED BY: APPROVED BY:	Natalie Rose

PORTIONS OF 2018 CONTRACT



Tenex Software Solutions, Inc. Precinct Central ePollbook

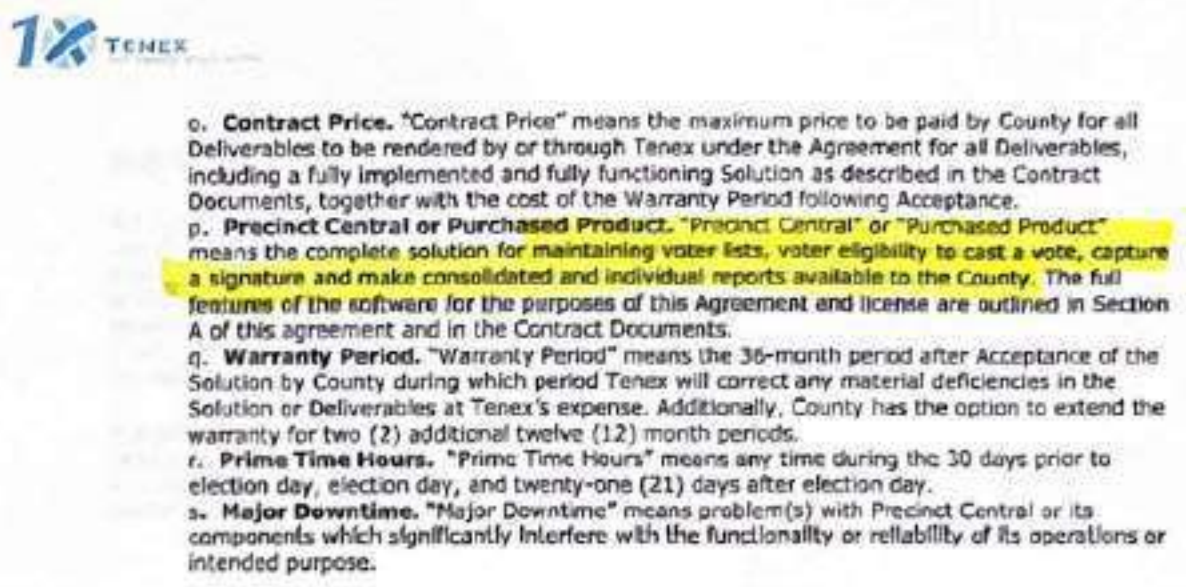
Tenex Software Solutions, Inc.
Precinct Central ePollbook Contract

This contract ("Agreement") is entered into as of **May 3rd, 2018** (the "Effective Date") by and between Tenex Software Solutions, Inc., a Florida corporation, having its principal place of business at 5402 W Laurel Street, Suite 206, Tampa, Florida 33607 ("Tenex" "Vendor" or "Company"), and Tarrant County, Texas, headquartered at 100 East Weatherford, Suite 303, Ft. Worth, TX 76196 ("County"), and governs the provision of the Precinct Central ePollbook Solution (the "Solution" as defined herein) by Tenex to County, and the use of the System (as defined below) by County, together with related services provided by Tenex to County, all in accordance with its terms. For convenience, Tenex and County are sometimes referred to in the Contract Documents as "Parties".

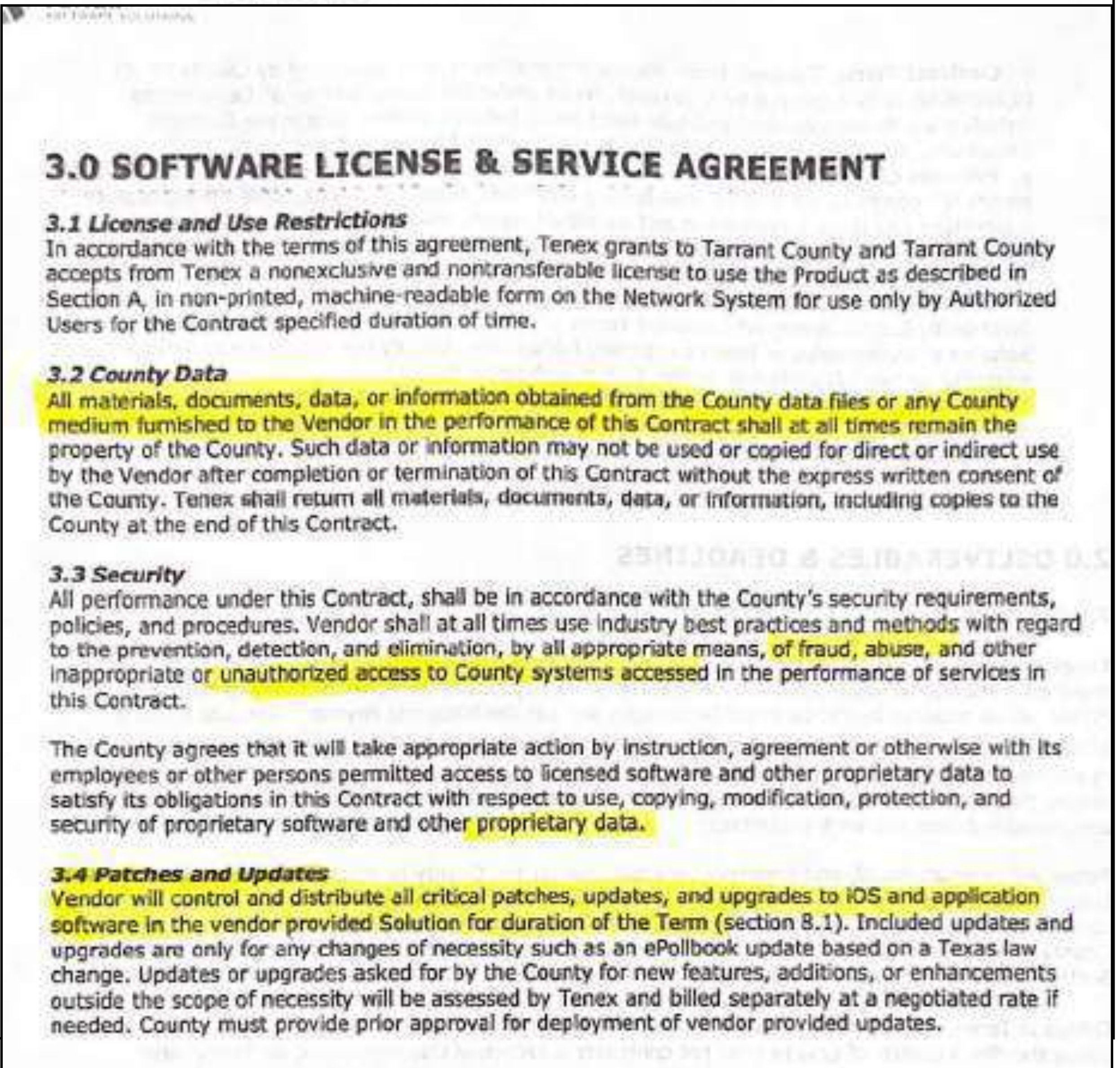
1.0 DEFINITIONS

The following definitions will apply:

a. **System.** "System" means the individual modules or products that make up the system. The overall system suite is known as "Precinct Central"
b. **County Data.** "County Data" means any of the County's information, documents, or electronic files that are provided to Tenex including Election and/or Voter data.
c. **Service.** "Service" means Tenex's work product necessary for providing electronic Check-ins, voter processing and election related functions
d. **Support**. "Support" means the ongoing services by Tenex to support & maintain the System as defined below.
e. **Solution.** "Solution" means the Precinct Central ePollbook system provided by Tenex, under the Agreement, inclusive of all hardware, Software and services required to make the Precinct Central ePollbook system fully functional
f. **Contract Documents.** "Contract Documents" means this Agreement, including all exhibits and attachments
g. **Agreement.** "Agreement" shall mean this software purchase agreement document, including all exhibits and attachments hereto. This agreement is in response to RFP 2018-070 for Electronic Poll Books. Copies of RFP 2018-070 and Vendor's response to said RFP are attached herein as Attachment B.
h. **Deliverables.** "Deliverables" shall mean any products furnished or services provided by or through Tenex under the Contract Documents.
i. **CAS.** "CAS" or "Custom Application Software" means custom software components of the Solution developed by Tenex and required to fulfill the specifications in the Contract Documents including, but not limited to, parametric instructions, program source statements, and customization of standard software components. CAS does not include software developed by other or third parties ("TPS").
j. **TPS.** "TPS" means the software components of the Solution other than CAS, including computer program, documentation, updates and related material. Software developed by entities other than Tenex.
k. **Software.** "Software" means A collection of computer programs, codes or data used to direct the operation of a computer or iPad device, including any documentation giving instructions on how to use them, including CAS and TPS.
m. **Acceptance.** "Acceptance" means written acceptance from County of Deliverable(s) provided by Tenex under the Agreement following successful completion of acceptance testing of the Solution by County. Payment, progress or partial payment, or partial use of the Solution by the County shall not constitute acceptance of Deliverables not furnished, implemented or operating in accordance with the requirements of the Contract Documents.



o. **Contract Price.** "Contract Price" means the maximum price to be paid by County for all Deliverables to be rendered by or through Tenex under the Agreement for all Deliverables, including a fully implemented and fully functioning Solution as described in the Contract Documents, together with the cost of the Warranty Period following Acceptance.
p. **Precinct Central or Purchased Product.** "Precinct Central" or "Purchased Product" means the complete solution for maintaining voter lists, voter eligibility to cast a vote, capture a signature and make consolidated and individual reports available to the County. The full features of the software for the purposes of this Agreement and license are outlined in Section A of this agreement and in the Contract Documents.
q. **Warranty Period.** "Warranty Period" means the 36-month period after Acceptance of the Solution by County during which period Tenex will correct any material deficiencies in the Solution or Deliverables at Tenex's expense. Additionally, County has the option to extend the warranty for two (2) additional twelve (12) month periods.
r. **Prime Time Hours.** "Prime Time Hours" means any time during the 30 days prior to election day, election day, and twenty-one (21) days after election day.
s. **Major Downtime.** "Major Downtime" means problem(s) with Precinct Central or its components which significantly interfere with the functionality or reliability of its operations or intended purpose.



3.0 SOFTWARE LICENSE & SERVICE AGREEMENT

3.1 License and Use Restrictions

In accordance with the terms of this agreement, Tenex grants to Tarrant County and Tarrant County accepts from Tenex a nonexclusive and nontransferable license to use the Product as described in Section A, in non-printed, machine-readable form on the Network System for use only by Authorized Users for the Contract specified duration of time.

3.2 County Data

All materials, documents, data, or information obtained from the County data files or any County medium furnished to the Vendor in the performance of this Contract shall at all times remain the property of the County. Such data or information may not be used or copied for direct or indirect use by the Vendor after completion or termination of this Contract without the express written consent of the County. Tenex shall return all materials, documents, data, or information, including copies to the County at the end of this Contract.

3.3 Security

All performance under this Contract, shall be in accordance with the County's security requirements, policies, and procedures. Vendor shall at all times use industry best practices and methods with regard to the prevention, detection, and elimination, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County systems accessed in the performance of services in this Contract.

The County agrees that it will take appropriate action by instruction, agreement or otherwise with its employees or other persons permitted access to licensed software and other proprietary data to satisfy its obligations in this Contract with respect to use, copying, modification, protection, and security of proprietary software and other proprietary data.

3.4 Patches and Updates

Vendor will control and distribute all critical patches, updates, and upgrades to iOS and application software in the vendor provided Solution for duration of the Term (section 8.1). Included updates and upgrades are only for any changes of necessity such as an ePollbook update based on a Texas law change. Updates or upgrades asked for by the County for new features, additions, or enhancements outside the scope of necessity will be assessed by Tenex and billed separately at a negotiated rate if needed. County must provide prior approval for deployment of vendor provided updates.

26.0 COUNTERPARTS OF THIS AGREEMENT

This Agreement may be executed in counterparts, each of which shall be deemed to be an original of this Agreement.

Section A–Precinct Central Product Description

Precinct Central is the most flexible and comprehensive electronic poll book solution available today. The software runs on the iPad hardware platform and requires no other peripherals for driver license scanning and signature capture. The three modules of Precinct Central are described below.

Precinct Central Touchpad (iPad App)

The Precinct Central Touchpad is the election worker interfacing application that runs on the iPad. The primary function on this module is to facilitate the voter check-in, handle advanced check-in scenarios, such as address changes and provisional voting. The following items describe the features of this module.

- Run in early voting and election day modes
- Voter lookup by scanning a driver license or state issued identification card
- Voter lookup using advanced search features
- Voter lookup using bar-code enabled voter information card or sample ballot
- Searching of state-wide voter registration systems (where available)
- Verifying voter eligibility based on election specific criteria
- Identifying voters that need assistance in voting
- Identifying voters with absentee ballots requests (returned or just requested)
- Identifying voters with any other special circumstances through comments
- Voter electronic signature capture
- Verify current voter signature with the signature on file (where available)
- Identifying ballot type and ballot style
- Validating ballot style issued by scanning a pre-printed ballot stub
- Issuing and *tracking* of provisional ballots
- Ability to issue a manual provisional when needed in unique situations (such, as a challenge to voter eligibility)
- Issuing a provisional in a voter not found situation – allowing complete entry of all relevant information when a voter is not found, identifying the correct ballot style, and issuing a provisional
- Allowing and tracking spoiled ballot information
- Allowing onsite address changes for voters moving within the county
- Allowing onsite address changes for voters moving from other counties
- Ballot-on Demand interface for early voting
- Address lookup for precinct verification and directions
- Tracking voters transferred to correct voting location, with any address changes completed
- Reporting of totals by device and location – including totals by provisional and spoiled ballots
- Reporting of all check-ins on the device or at the location, with various filters
- Printing a voter check-in slip complete voter details and ballot style information
- Printing of voter transfer slip for voters transferred to correct voting location
- Printing of list of voters checked in directly from the iPad – for purposes of posting
- Printing of check-in totals at the beginning of day.
- Printing of check-in totals at the end of the day.
- Side-ways communication for in-precinct communications.

7.0 INTELLECTUAL PROPERTY

7.1 Intellectual Property Ownership

Tenex Software Solutions, Inc. owns the entire copyright, title and interest in the following content ("Content"):

- Precinct Central Suite including the Touchpad, Console, and Data Studio
- Election Response Help Desk Management System

County will own or secure all necessary rights to copyright, trademark or other intellectual property to any materials it submits to Tenex Software Solutions, Inc. for use in the Services.

Nothing in this section will affect ownership of intellectual property created and owned by any entities not a party to this Agreement and not pursuant to an agreement with Tenex. Prior agreements for other products will not be affected by this agreement.

Precinct Central Console

The Precinct Central Console is the IT and Management staff interfacing application that allows Touchpads to be controlled and monitored. The primary function on this module is to aggregate voter check-ins, act as the central repository for databases and perform command and control functions. The following items describe the features of this module.

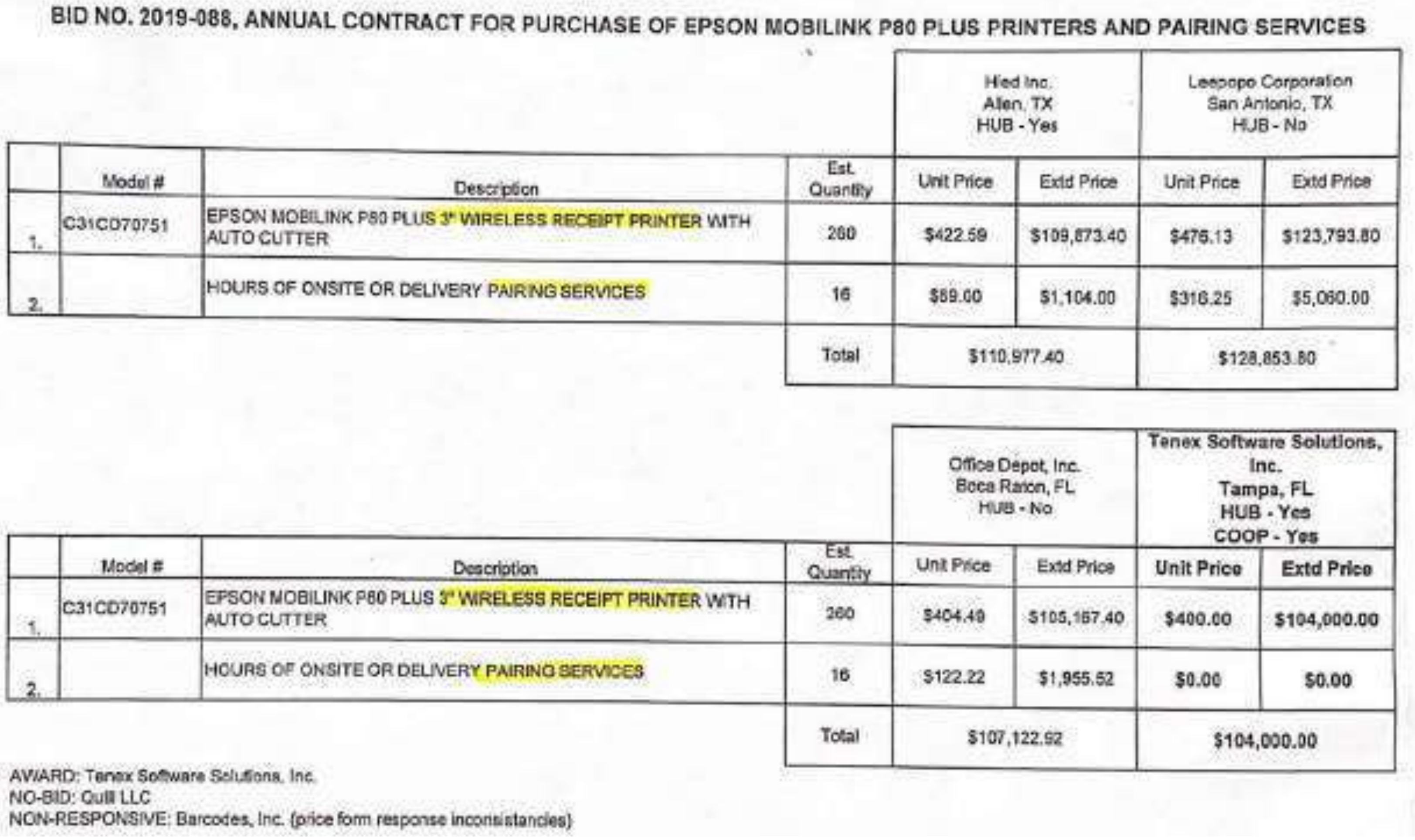
- Device registration and activation
- Device monitoring when idle and non-operational
- Monitoring views of all iPads allowing real-time tracking of any issues
- Reports for voter check-in activity including information on provisional ballots and spoiled ballots
- Auditing views with information on processing times, user activity, and statistics
- Heartbeat monitoring with information on battery status, user status and data status
- Setup and configure data for election
- Pre-election over the air data package loading
- Post-election over the air data package unloading
- Poll worker payroll module

Precinct Central Data Studio

The PC Data Studio module is designed to run at the client site managing the data transfers and providing near real-time updates to Precinct Central for Early Voting and Absentee changes. The following items describe the features of this module.

- Data conversion for level-0 data load into Precinct Central
- Real-time / batch data updates from voter registration system for address changes, name changes, status changes, absentee changes
- Real-time / batch update to voter registration system for voting history and absentee changes
- Real-time / batch cancellation of absentee ballots (mailed or requested)
- All check-in information updated to central server
- All check-in information distributed down to each iPad in real-time from central server
- Voter credit

EPSON PRINTER WITH PAIRING SERVICE

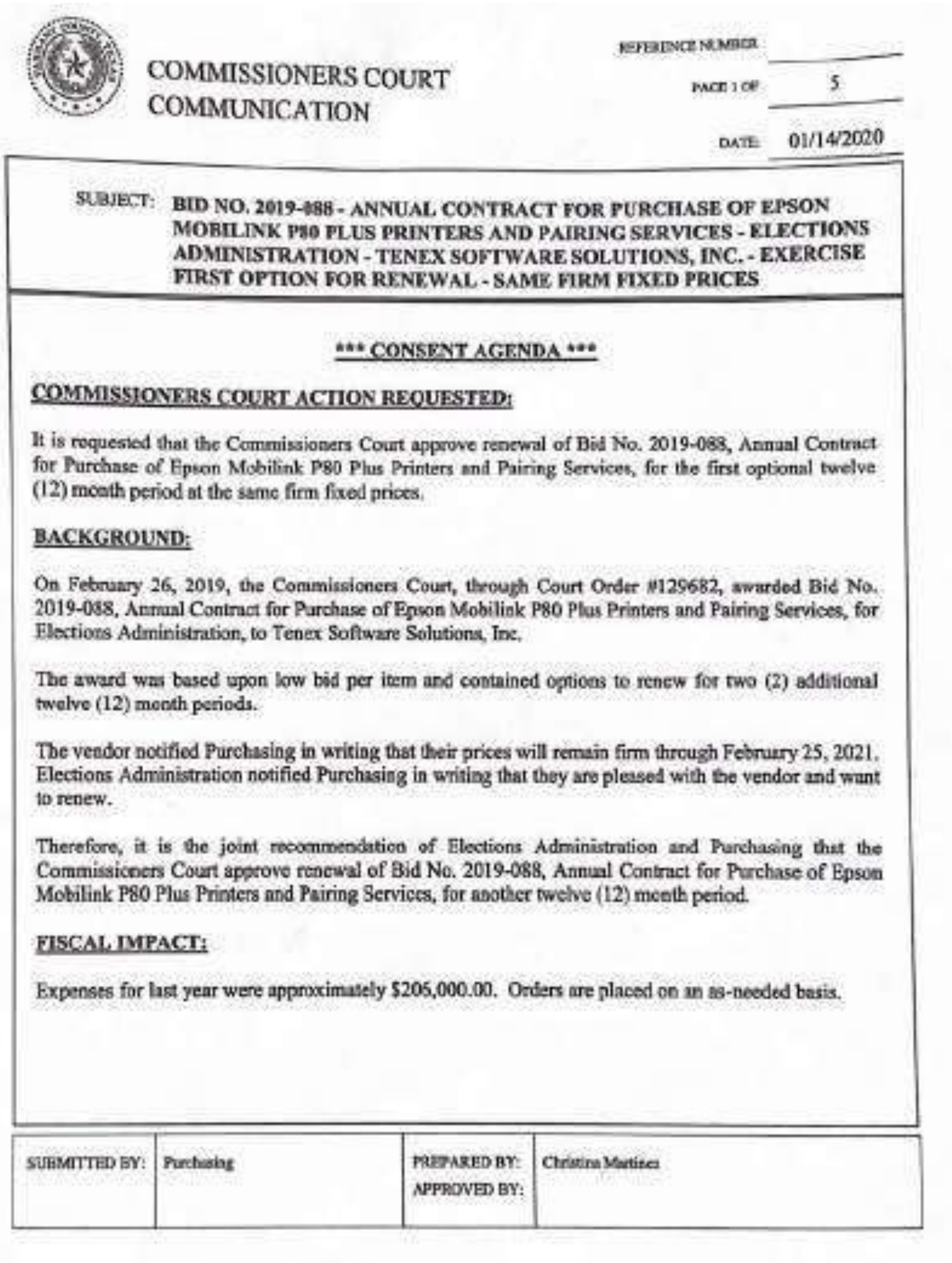


BID NO. 2019-088, ANNUAL CONTRACT FOR PURCHASE OF EPSON MOBILINK P80 PLUS PRINTERS AND PAIRING SERVICES

				Hied Inc. Allen, TX HUB - Yes		Leepopo Corporation San Antonio, TX HUB - No	
	Model #	Description	Est. Quantity	Unit Price	Extd Price	Unit Price	Extd Price
1.	C31CD70751	EPSON MOBILINK P80 PLUS 3" WIRELESS RECEIPT PRINTER WITH AUTO CUTTER	260	$422.59	$109,873.40	$476.13	$123,793.80
2.		HOURS OF ONSITE OR DELIVERY PAIRING SERVICES	16	$69.00	$1,104.00	$316.25	$5,060.00
			Total	$110,977.40		$128,853.80	

				Office Depot, Inc. Boca Raton, FL HUB - No		Tenex Software Solutions, Inc. Tampa, FL HUB - Yes COOP - Yes	
	Model #	Description	Est. Quantity	Unit Price	Extd Price	Unit Price	Extd Price
1.	C31CD70751	EPSON MOBILINK P80 PLUS 3" WIRELESS RECEIPT PRINTER WITH AUTO CUTTER	260	$404.49	$105,167.40	$400.00	$104,000.00
2.		HOURS OF ONSITE OR DELIVERY PAIRING SERVICES	16	$122.22	$1,955.52	$0.00	$0.00
			Total	$107,122.92		$104,000.00	

AWARD: Tenex Software Solutions, Inc.
NO-BID: Quill LLC
NON-RESPONSIVE: Barcodes, Inc. (price form response inconsistancies)



COMMISSIONERS COURT
COMMUNICATION

REFERENCE NUMBER	
PAGE 1 OF	5
DATE:	01/14/2020

SUBJECT: **BID NO. 2019-088 - ANNUAL CONTRACT FOR PURCHASE OF EPSON MOBILINK P80 PLUS PRINTERS AND PAIRING SERVICES - ELECTIONS ADMINISTRATION - TENEX SOFTWARE SOLUTIONS, INC. - EXERCISE FIRST OPTION FOR RENEWAL - SAME FIRM FIXED PRICES**

***** CONSENT AGENDA *****

COMMISSIONERS COURT ACTION REQUESTED:

It is requested that the Commissioners Court approve renewal of Bid No. 2019-088, Annual Contract for Purchase of Epson Mobilink P80 Plus Printers and Pairing Services, for the first optional twelve (12) month period at the same firm fixed prices.

BACKGROUND:

On February 26, 2019, the Commissioners Court, through Court Order #129682, awarded Bid No. 2019-088, Annual Contract for Purchase of Epson Mobilink P80 Plus Printers and Pairing Services, for Elections Administration, to Tenex Software Solutions, Inc.

The award was based upon low bid per item and contained options to renew for two (2) additional twelve (12) month periods.

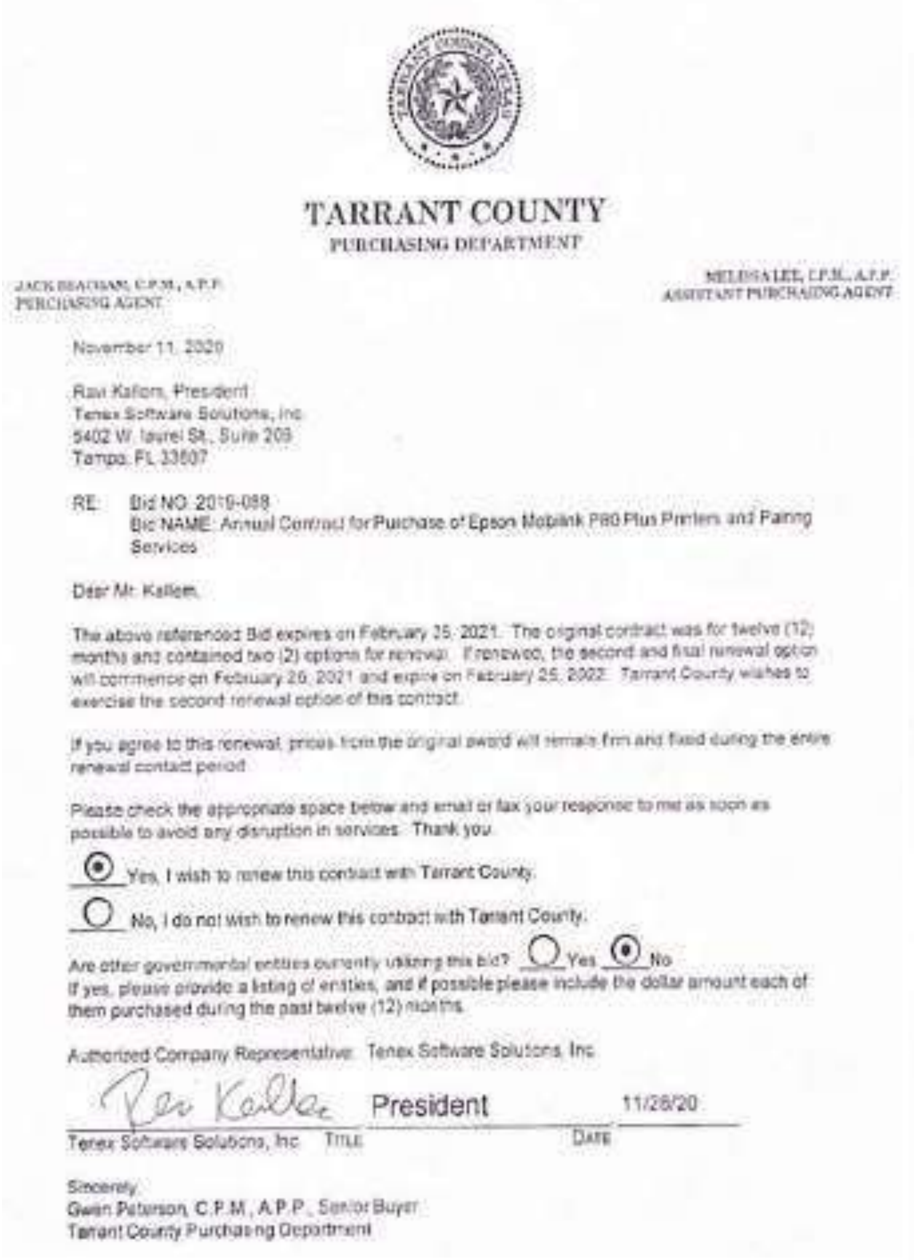
The vendor notified Purchasing in writing that their prices will remain firm through February 25, 2021. Elections Administration notified Purchasing in writing that they are pleased with the vendor and want to renew.

Therefore, it is the joint recommendation of Elections Administration and Purchasing that the Commissioners Court approve renewal of Bid No. 2019-088, Annual Contract for Purchase of Epson Mobilink P80 Plus Printers and Pairing Services, for another twelve (12) month period.

FISCAL IMPACT:

Expenses for last year were approximately $205,000.00. Orders are placed on an as-needed basis.

SUBMITTED BY:	Purchasing	PREPARED BY: APPROVED BY:	Christina Martinez



TARRANT COUNTY
PURCHASING DEPARTMENT

JACK BEACHAM, C.P.M., A.P.P.
PURCHASING AGENT

MELISSA LEE, C.P.M., A.P.P.
ASSISTANT PURCHASING AGENT

November 11, 2020

Ravi Kallem, President
Tenex Software Solutions, Inc
5402 W. laurel St., Suite 209
Tampa, FL 33607

RE: Bid NO. 2019-088
Bid NAME: Annual Contract for Purchase of Epson Mobilink P80 Plus Printers and Pairing Services

Dear Mr. Kallem,

The above referenced Bid expires on February 25, 2021. The original contract was for twelve (12) months and contained two (2) options for renewal. If renewed, the second and final renewal option will commence on February 26, 2021 and expire on February 25, 2022. Tarrant County wishes to exercise the second renewal option of this contract.

If you agree to this renewal, prices from the original award will remain firm and fixed during the entire renewal contact period.

Please check the appropriate space below and email or fax your response to me as soon as possible to avoid any disruption in services. Thank you.

● Yes, I wish to renew this contract with Tarrant County.

○ No, I do not wish to renew this contract with Tarrant County.

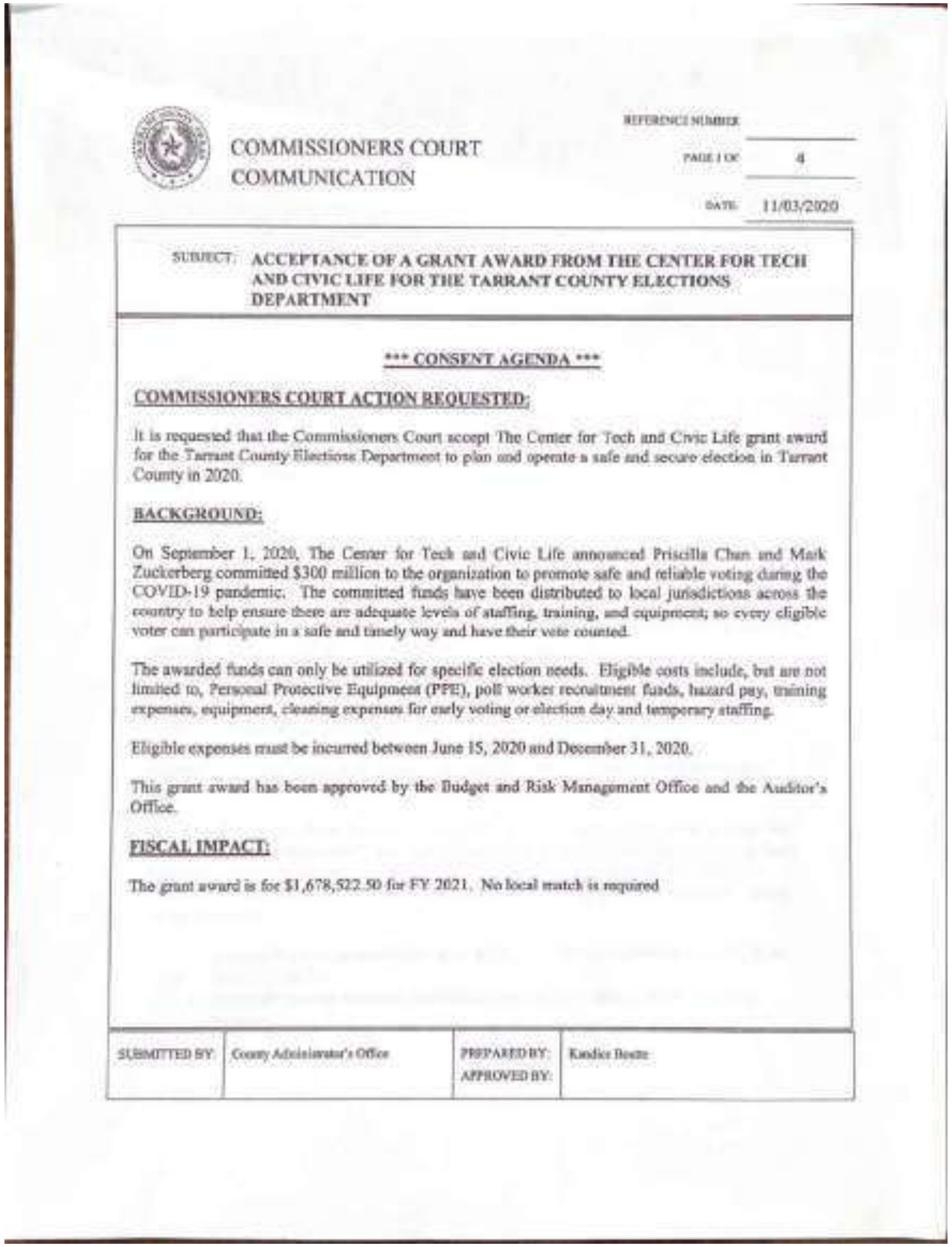
Are other governmental entities currently utilizing this bid? ○ Yes ● No
If yes, please provide a listing of entities, and if possible please include the dollar amount each of them purchased during the past twelve (12) months.

Authorized Company Representative: Tenex Software Solutions, Inc

President 11/28/20
Tenex Software Solutions, Inc TITLE DATE

Sincerely,
Gwen Peterson, C.P.M., A.P.P., Senior Buyer
Tarrant County Purchasing Department

Grants from Big Tech to Purchase Vulnerable Election Infrastructure



COMMISSIONERS COURT
COMMUNICATION

REFERENCE NUMBER	
PAGE 1 OF	4
DATE	11/03/2020

SUBJECT: ACCEPTANCE OF A GRANT AWARD FROM THE CENTER FOR TECH AND CIVIC LIFE FOR THE TARRANT COUNTY ELECTIONS DEPARTMENT

***** CONSENT AGENDA *****

COMMISSIONERS COURT ACTION REQUESTED:

It is requested that the Commissioners Court accept The Center for Tech and Civic Life grant award for the Tarrant County Elections Department to plan and operate a safe and secure election in Tarrant County in 2020.

BACKGROUND:

On September 1, 2020, The Center for Tech and Civic Life announced Priscilla Chan and Mark Zuckerberg committed $300 million to the organization to promote safe and reliable voting during the COVID-19 pandemic. The committed funds have been distributed to local jurisdictions across the country to help ensure there are adequate levels of staffing, training, and equipment; so every eligible voter can participate in a safe and timely way and have their vote counted.

The awarded funds can only be utilized for specific election needs. Eligible costs include, but are not limited to, Personal Protective Equipment (PPE), poll worker recruitment funds, hazard pay, training expenses, equipment, cleaning expenses for early voting or election day and temporary staffing.

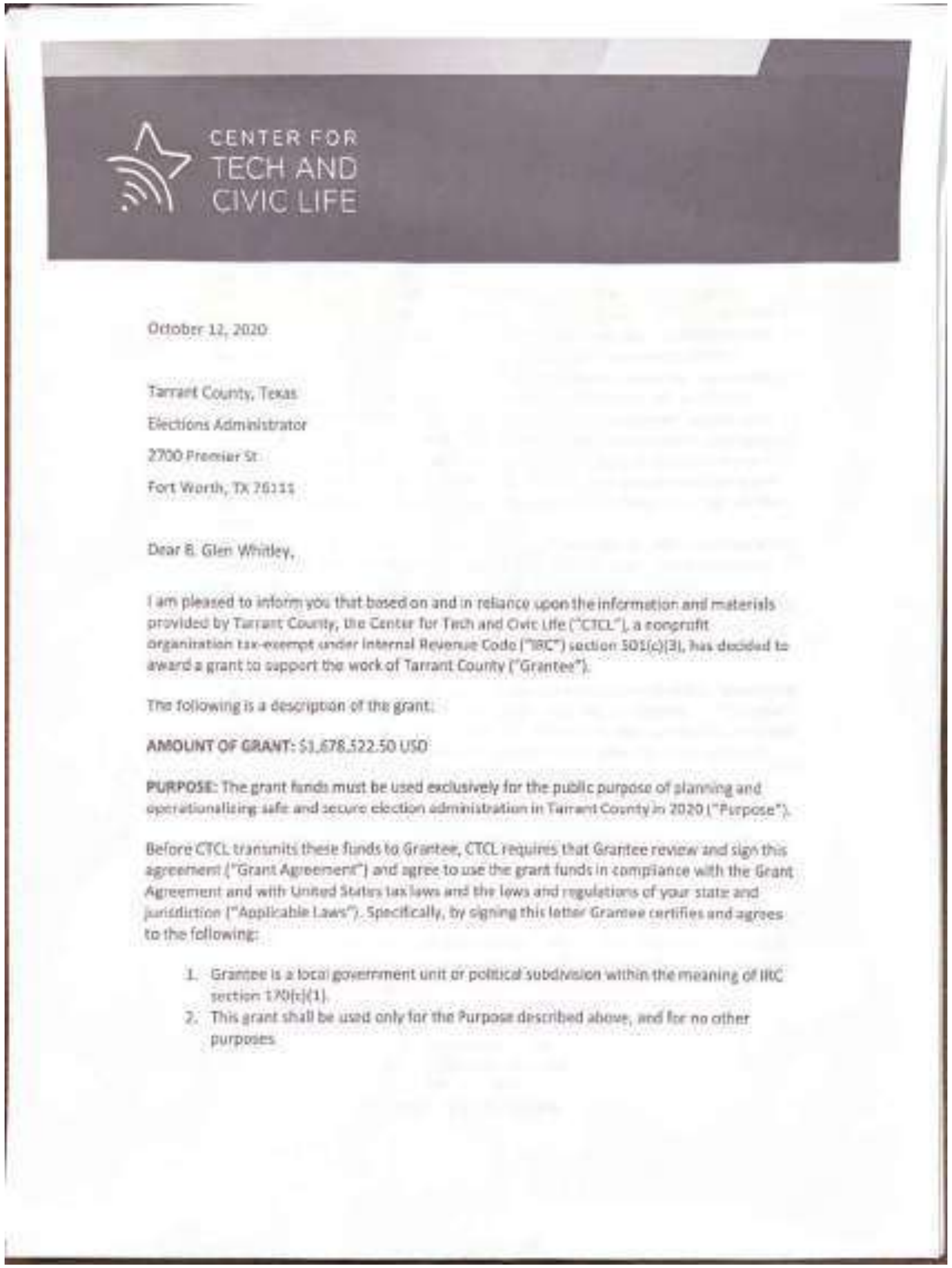
Eligible expenses must be incurred between June 15, 2020 and December 31, 2020.

This grant award has been approved by the Budget and Risk Management Office and the Auditor's Office.

FISCAL IMPACT:

The grant award is for $1,678,522.50 for FY 2021. No local match is required

SUBMITTED BY:	County Administrator's Office	PREPARED BY: APPROVED BY:	Kandice Beste



CENTER FOR
TECH AND
CIVIC LIFE

October 12, 2020

Tarrant County, Texas
Elections Administrator
2700 Premier St
Fort Worth, TX 76111

Dear B. Glen Whitley,

I am pleased to inform you that based on and in reliance upon the information and materials provided by Tarrant County, the Center for Tech and Civic Life ("CTCL"), a nonprofit organization tax-exempt under Internal Revenue Code ("IRC") section 501(c)(3), has decided to award a grant to support the work of Tarrant County ("Grantee").

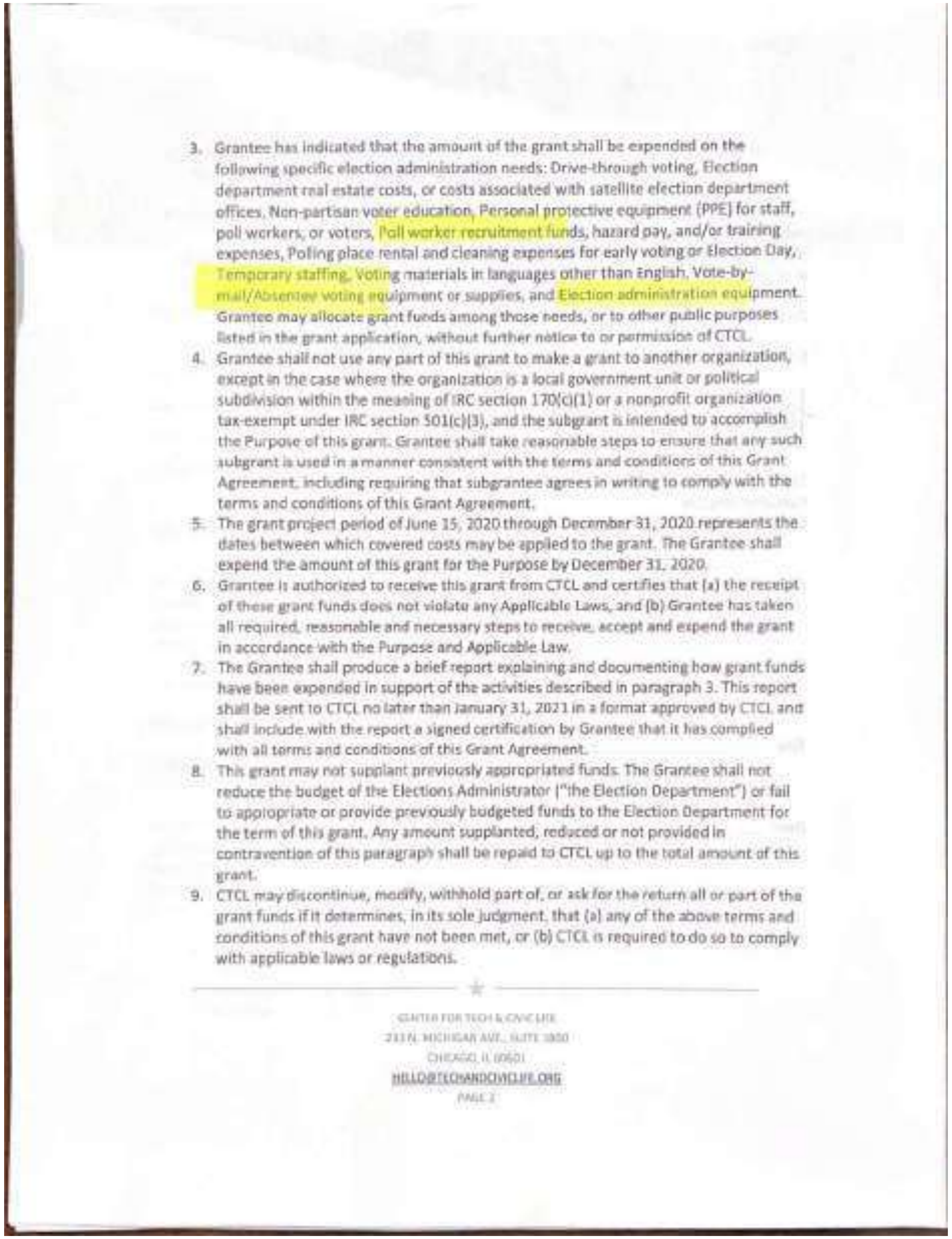
The following is a description of the grant:

AMOUNT OF GRANT: $1,678,522.50 USD

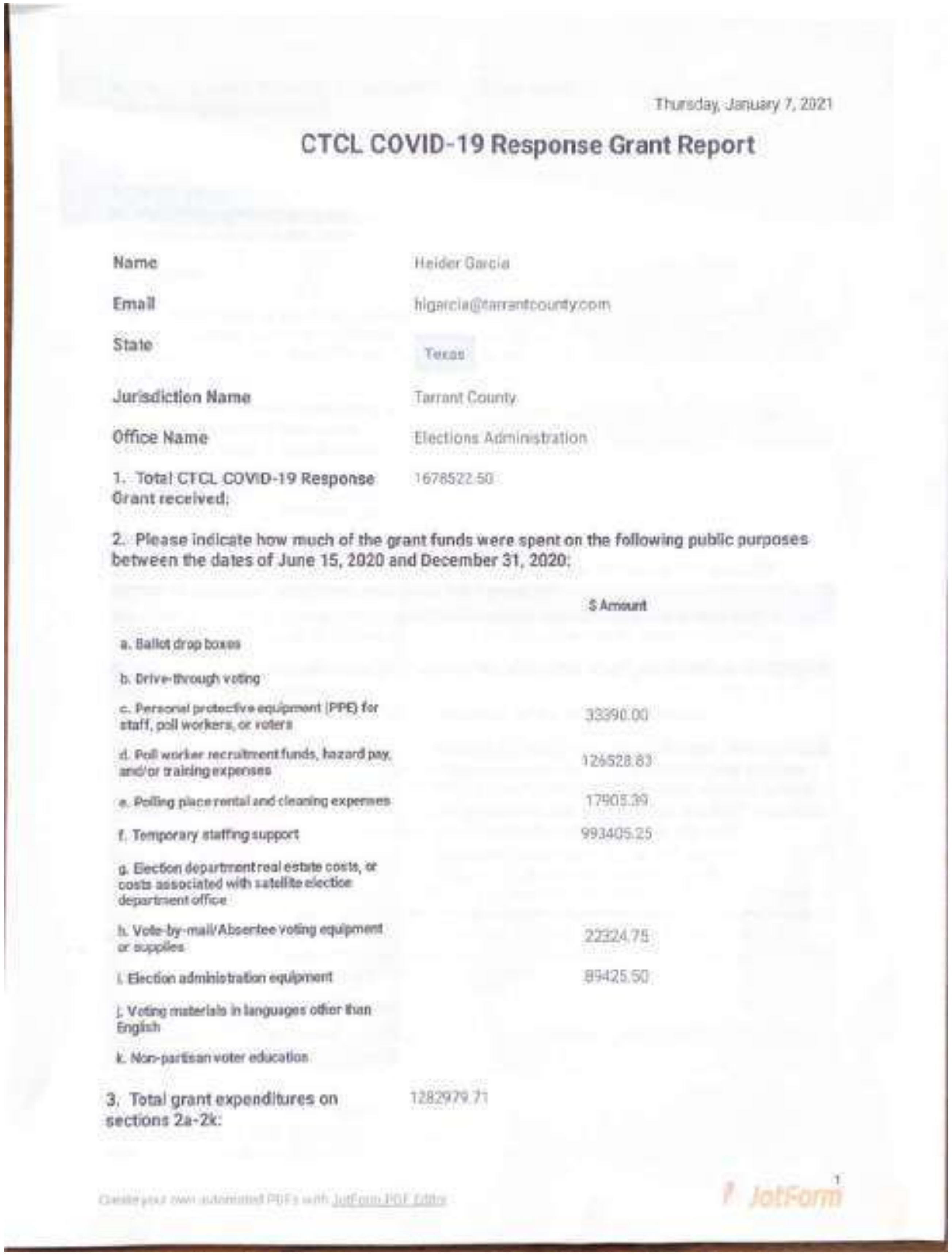
PURPOSE: The grant funds must be used exclusively for the public purpose of planning and operationalizing safe and secure election administration in Tarrant County in 2020 ("Purpose").

Before CTCL transmits these funds to Grantee, CTCL requires that Grantee review and sign this agreement ("Grant Agreement") and agree to use the grant funds in compliance with the Grant Agreement and with United States tax laws and the laws and regulations of your state and jurisdiction ("Applicable Laws"). Specifically, by signing this letter Grantee certifies and agrees to the following:

1. Grantee is a local government unit or political subdivision within the meaning of IRC section 170(c)(1).
2. This grant shall be used only for the Purpose described above, and for no other purposes



3. Grantee has indicated that the amount of the grant shall be expended on the following specific election administration needs: Drive-through voting, Election department real estate costs, or costs associated with satellite election department offices, Non-partisan voter education, Personal protective equipment (PPE) for staff, poll workers, or voters, Poll worker recruitment funds, hazard pay, and/or training expenses, Polling place rental and cleaning expenses for early voting or Election Day, Temporary staffing, Voting materials in languages other than English, Vote-by-mail/Absentee voting equipment or supplies, and Election administration equipment. Grantee may allocate grant funds among those needs, or to other public purposes listed in the grant application, without further notice to or permission of CTCL.
4. Grantee shall not use any part of this grant to make a grant to another organization, except in the case where the organization is a local government unit or political subdivision within the meaning of IRC section 170(c)(1) or a nonprofit organization tax-exempt under IRC section 501(c)(3), and the subgrant is intended to accomplish the Purpose of this grant. Grantee shall take reasonable steps to ensure that any such subgrant is used in a manner consistent with the terms and conditions of this Grant Agreement, including requiring that subgrantee agrees in writing to comply with the terms and conditions of this Grant Agreement.
5. The grant project period of June 15, 2020 through December 31, 2020 represents the dates between which covered costs may be applied to the grant. The Grantee shall expend the amount of this grant for the Purpose by December 31, 2020.
6. Grantee is authorized to receive this grant from CTCL and certifies that (a) the receipt of these grant funds does not violate any Applicable Laws, and (b) Grantee has taken all required, reasonable and necessary steps to receive, accept and expend the grant in accordance with the Purpose and Applicable Law.
7. The Grantee shall produce a brief report explaining and documenting how grant funds have been expended in support of the activities described in paragraph 3. This report shall be sent to CTCL no later than January 31, 2021 in a format approved by CTCL and shall include with the report a signed certification by Grantee that it has complied with all terms and conditions of this Grant Agreement.
8. This grant may not supplant previously appropriated funds. The Grantee shall not reduce the budget of the Elections Administrator ("the Election Department") or fail to appropriate or provide previously budgeted funds to the Election Department for the term of this grant. Any amount supplanted, reduced or not provided in contravention of this paragraph shall be repaid to CTCL up to the total amount of this grant.
9. CTCL may discontinue, modify, withhold part of, or ask for the return all or part of the grant funds if it determines, in its sole judgment, that (a) any of the above terms and conditions of this grant have not been met, or (b) CTCL is required to do so to comply with applicable laws or regulations.



Thursday, January 7, 2021

CTCL COVID-19 Response Grant Report

Name	Heider Garcia
Email	higarcia@tarrantcounty.com
State	Texas
Jurisdiction Name	Tarrant County
Office Name	Elections Administration
1. Total CTCL COVID-19 Response Grant received:	1678522.50

2. Please indicate how much of the grant funds were spent on the following public purposes between the dates of June 15, 2020 and December 31, 2020:

	$ Amount
a. Ballot drop boxes	
b. Drive-through voting	
c. Personal protective equipment (PPE) for staff, poll workers, or voters	33390.00
d. Poll worker recruitment funds, hazard pay, and/or training expenses	126528.83
e. Polling place rental and cleaning expenses	17905.39
f. Temporary staffing support	993405.25
g. Election department real estate costs, or costs associated with satellite election department office	
h. Vote-by-mail/Absentee voting equipment or supplies	22324.75
i. Election administration equipment	89425.50
j. Voting materials in languages other than English	
k. Non-partisan voter education	

3. Total grant expenditures on sections 2a-2k:	1282979.71