> > "This practice is not acceptable. Voting system applications use many operating system functions. Changes to the operating system should only be made after approve by the Texas Director of Elections after appropriate review. Further, safeguards are needed to assure that only the approved update is installed on systems. The current practice potentially allows additional software to be installed under the guise that it is part of the operating system update."
>
> "To assure a secure election system there should never be a point at which individuals from a single organization can change software. At a minimum individuals from two different organizations should approve and verify any changes to the operating system. In the case of operating system upgrades it would be preferable that the vendor recommend and the Director of Elections approve any patches to the operating system. Then that the vendor install the patches and the local jurisdiction have the tools and information to verify that the system delivered to them have only certified software, including the version and updates to the operating system. Further local jurisdictions should have the tools and information to confirm that no additional software has been added to the system."
>
> v. Recommended administrative use procedures for this system are needed.

222.229. Hart InterCivic has a history of issues regarding hash validations to include version 6.2.1 yet the SoS's office did certify without publishing answers regarding if condition had been met.

223.230. Berger's report is listed a multitude of security flaws presented in the Hart InterCivic 6.2.1 voting system.

> **2.2.5.3 COTS General Purpose Computer System Requirements**
>
> Further requirements must be applied to COTS operating systems to ensure completeness and integrity of audit data for election software. These operating systems are capable of executing multiple application programs simultaneously. These systems include both servers and workstations (or "PCs"), including the many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software running on these COTS systems is vulnerable to unintended effects from other user sessions, applications, and utilities, executing on the same platform at the same time as the election software.
>
> "Simultaneous processes" of concern include unauthorized network connections, unplanned user logins, and unintended execution or termination of operating system processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection.

> To counter these vulnerabilities, three operating system protections are required on all such systems on which election software is hosted. First, authentication shall be configured on the local terminal (display screen and keyboard) and on all external connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running.[130]

224.231. These security vulnerabilities provide access to election system in a way in which vote totals may be altered.

225.232. The SoS's office issued a "Preliminary Statement" on April 30, 2009, under conditions the examiners discovered two potential security concerns and advised security protocols to follow to mitigate these vulnerabilities.

226.233. If these security protocols are not followed, then it is theoretically possible to have access to the operating system and run or delete other programs. Jurisdictions are advised to (1) restrict usage of the voting system[131] and (2) restrict what software is loaded onto the voting system computer.

227.234. The SoS's office further "conditioned" the certification of version 6.2.1 by applying procedures for jurisdictions. (1) Two-person access with one person login on Windows 2000 OS and one person to start the

[130] https://www.sos.texasgov/elections/forms/sysexam/stephenberger621.pdf#search=hart%206.2.1 *See* page 25. *ID. See* VVS 2002 Vol. Sec. 2.2.5.3 page 25- Last visited 06/23/22

[131] https://www.sos.state.tx.us/elections/forms/sysexam/hart621cert.pdf *See* Conditions, Election Advisory 2008-09, Sec. 5(f) (i-iii) is no longer available online.

application. (2) Two-person control team on the Tally when open. (3) Windows 2000 audit logs which tracks log-ons and attempts. (4) Windows 2000 to harden operating systems. (5) Jurisdiction must file an initial written confirmation with the SoS that they are in compliance with the procedures.[132]

228.235. By the SoS's current website, there are 37 counties utilizing this version of Hart: Archer, Brown, Burnet, Cass, Castro, Comanche, Crosby, Dawson, Delta, Dickens, Duval, Ector, Falls, Fannin, Foard, Gary, Grimes, Harrison, Hudspeth, Jefferson, Jim Hogg, Kennedy, Kimble, La Salle, Lipscomb, Marion, Matagorda, McLennan, Menard, Mills, Montgomery, Shackelford, Throckmorton, Wichita, Wilbarger, Willacy, and Wood.[133]

D. Foreign Companies in Texas Infrastructure

Scytl and Election Night Reporting (ENR)

205. Scytl Election Technologies S.L.U. is a Spanish provider of electronic voting systems and election technology. Founded in 2001 in Barcelona, its products and services are used in elections and referenda across the world.[134]

[132] https://www.sos.state.tx.us/elections/forms/sysexam/hart621cert.pdf Last visited 06/23/22 - Id. *See* Conditions

[133] https//www.sos.state.tx.us/elections/forms/sysexam/voting-sys-bycounty.pdf Last visited 06/23/22

[134] https://www.forbes.com/sites/rebeccaheilweil1/2017/12/02/eight-companies-that-want-to-revolutionize-voting-technology/?sh=5168353212c1 Last visited 07/16/22

206. Scytl grew out of a cryptography research project[135] at the Autonomous University of Barcelona. The name is a reference to the scytale, an ancient cryptographic tool.[136]

207. In 2017, Scytl divided itself into three companies.

a. Original Scytl Secure Electronic Voting, which develops voting software

b. Scytl Voting Hardware SL, which develops voting hardware (Owned by Scytl and an anonymous Dubai-based investor)

c. Civiti (formerly OpenSeneca) which focuses on civic participation services

208. Paragon Group acquired Scytl in October of 2020.[137]

209. Scytl's products cover the entire election process, including election planning, online voter registration, poll worker management, electronic ballot delivery, online voting, results consolidation, and Election Night Reporting (ENR) and asset tracking.

210. Investors:

a. Venture Capital (Wall Street)

b. Balderton Capital (London, UK)

[135] https: //www.politico.com/story/2018/02/24/elections-vendors-russia-423435 Last visited 07/16/22

[136] https://www.scytl.com/about-us/company-overview/ Last visited 07/16/22

[137] Last visited 07/19/22

c. Nauta Capital (Barcelona, London, and Berlin)

d. Vulcan Capital (Privately held company by Microsoft co-founder Paul Allen and Jody Allen)

e. Sapphire Ventures (Austin, Palo Alto, London and San Francisco)

f. Paul Allen (co-founder of Microsoft with Bill Gates)

211. Scytl is headquartered at Travessera de Gràcia 17-21, 7th floor, 08021 Barcelona, Spain, Tel: +34 934 230 324.

212. Scytl systems have been implemented in numerous countries, but problems have cropped up over the years with its solutions and voting systems, including those used in Australia, Ecuador, Norway and Switzerland.[138]

a. Ecuador: 2014-Bungled regional elections so badly that all the scanned election ballots had to be counted manually at the company's Barcelona headquarters. Several Scytl managers were even temporarily arrested as a result for breach of contract. It took Scytl one month to count all of the ballots. Former employees now say it is strange that the case did not attract international attention.

    i. In some districts the software didn't work at all

[138] https://www.republik.ch/2019/02/07/the-tricky-business-of-democracy Last visited 07/16/22

ii. The program couldn't read and interpret a large portion of the scanned ballots

iii. Vast amounts of data caused several servers to crash completely[139]

b. Australia: Australian state of New South Wales where serious vulnerability was discovered. Researchers Alex Halderman at the University of Michigan and Vanessa Teague at the University of Melbourne examined the system more closely and discovered a serious vulnerability that allowed them to circumvent the encryption between the voter's browser and the e-voting system.[140]

c. Norway: In 2011 when Norway introduced electronic voting, the code was so flawed it was unusable.

i. Reto Koenig, a professor of computer science at the Bern University of Applied Science (BFH) who examined the Norwegian e-voting system at the time, said the <<pile of code>> they received would not have worked to get it up and running.

ii. The group working with Koenig, using simple programs, found <<a bug that had hidden itself deep in the cryptography>>

[139] http://www.ecuadorinmediato.com/index.php?module=Noticias&func=news_user_view&id=2818765879&umt=unasur_entrega_informe_final_observacion_electoral_2014 Last visited 07/16/22

[140] https://arxiv.org/pdf/1504.05646.pdf Last visited 07/16/22

after the voting systems had been used for two years.[141]

iii. Norway has since restricted e-voting and one year later the e-voting project was shelved completely due to the concerns of citizens.[142]

d. Switzerland: In 2019, a cryptographic trap door could let someone change votes cast using Switzerland's online sVote system without being detected.[143]

i. Verification: The specific issue is the way the system receives and counts votes before shuffling them and anonymizing. The trap door means someone could switch all the legitimately cast ballots for fraudulent ones, undetected.

ii. Scytl, who provides electronic voting services to over 35 countries, including the United States, says it's working to fix the flaw.

213. The worrying aspect in the countries mentioned above is how did the "flaws" manage to creep into these systems in the first place. Researchers state

[141] https://www.bfh.ch/ti/de/ueber-das-ti/ Last visited 07/16/22

[142] https://www.technologyreview.com/2019/03/12/136676/a-major-flaw-has-been-found-in-switzerlands-online-voting-system/ Last visited 07/16/22

[143] https://www.technologyreview.com/2019/03/12/136676/a-major-flaw-has-been-found-in-switzerlands-online-voting-system/ Last visited 7/16/22

that they have only tested a fraction of the code base as Scytl has not released source codes.

214. Scytl withholds important information about the testing of its e-voting systems and services (ENR) or requires expansive licenses for those reviews to be carried out.

215. The company had also spent Spanish public funds and EU research money into client acquisition instead of investing them into further development as stipulated (1.5 million euros Spanish Government and 9,000,000 euros EU funds on the Ecuadorian election)[144]

216. In 2008, Scytl made an international breakthrough when it won its first American client: Florida.

217. Researchers at the University of California, Berkeley, wanted to investigate voting-machine software in Florida as early as 2008, but did not have access to the documents that were crucial to their research. As a result, the researchers could not verify whether the system worked properly and weren't able to carry out test attacks on the system.[145]

218. Scytl then began offering software for voting machines as well as infrastructure and on-site support.

219. In 2012, Scytl acquired the American company SOE Software ("Supervisors of Elections")[146]

[144] https://www.republik.ch/2019/02/07/the-tricky-business-of-democracy

[145] https://people.eecs.berkeley.edu/~daw/papers/scytl-odbp.pdf Last visited 07/16/22

[146] http://eon.businesswire.com/news/eon/20120111005636/en/Scytl/SOE/election-software Last visited 07/16/22

220. SOE Software, based in Tampa, FL, has developed Clarity, a suite of 8 software modules.

221. In 2013, Scytl acquired the software division of Gov2U.[147]

a. "Gov2U, based in Brussels, is a non-profit, non-governmental organization by a group of visionary professionals from the field of Legislative Information and Communication Technology (ICT), and community activism who share . . . "

222. The EAC has since posted that SOE Software, A Scytl Company is an inactive voting system registered manufacturer but does not provide dates of when active or inactive.[148]

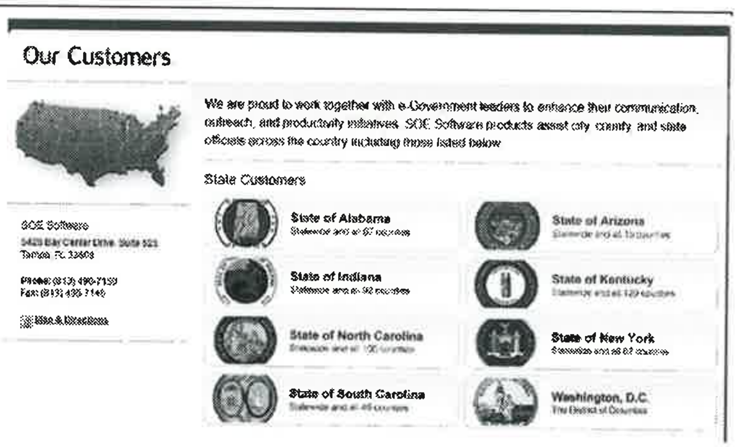
223. In 2020, SOE d/b/a Scytl provided various products and services in over 800 countries and several states in the United States.[149]

224.

[147] https://www.marketwatch.com/story/scytl-acquires-gov2us-software-division-expanding-its-edemocracy-solutions-portfolio-2013-04-30 Last visited 07/16/22

[148] https://www.eac.gov/voting-equipment/registered-manufacturers/soe-software-scytl-company Last visited 07/16/22

[149] https://web.archive.org/web/20120527202144/http://www.soesoftware.com/customers.aspx Last visited 07/16/22



Our Customers

We are proud to work together with e-Government leaders to enhance their communication, outreach, and productivity initiatives. SOE Software products assist city, county, and state officials across the country including those listed below

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

Phone: (813) 490-7150
Fax: (813) 490-7146

Map & Directions

State Customers

State of Alabama
Statewide and all 67 counties

State of Arizona
Statewide and all 15 counties

State of Indiana
Statewide and all 92 counties

State of Kentucky
Statewide and all 120 counties

State of North Carolina
Statewide and all 100 counties

State of New York
Statewide and all 62 counties

State of South Carolina
Statewide and all 46 counties

Washington, D.C.
The District of Columbia

Transcription:

Our Customers: We are proud to work together with e-Government leaders to enhance their communication, outreach, and productivity initiatives. SOE Software products assist city, county, and state officials across the country including those listed below.

225.

Partial Customer List

Arapahoe, CO
Bloomington, IL
Broward, FL
Butte, CA
Charlotte, FL
Chicago, IL
Citrus, FL
Clay, FL
Cochise, AZ
Contra Costa, CA
Cortland, NY
Dallas, TX
Marion, FL
Martin, FL
McHenry, IL
Miami-Dade, FL
Monroe, NY
Nassau, NY
Niagara, NY
Oakland, MI
Okaloosa, FL
Okeechobee, FL
Olmsted, MN
Orange, FL

Dona Ana, NM
Dupage, IL
Dutchess, NY
Duval, FL
Erie, NY
Escambia, FL
Fort Bend, TX
Highlands, FL
Hillsborough, FL
Indian River, FL
Jefferson, CO
Jefferson, TX
Johnson, KS
King, WA
Lake, IL
Lee, FL
Los Angeles, CA
Madison, IL
Manatee, FL
Orange, NY
Palm Beach, FL
Pasco, FL
Pinellas, FL
Putnam, FL
Riverside, CA
Rockford City, IL
Sacramento, CA
Salt Lake, UT
San Diego, CA
Santa Clara, CA
Sarasota, FL
Shasta, CA
St. Lucie, FL
Tarrant, TX
Ventura, CA
Volusia, FL
Will, IL
Williamson, TX
Winnebago, IL

226. In 2018, Scytl became a partner of Amazon Web Services which hosts their services on Amazon's cloud platform.

227.

> **Data Center Security and Compliance**
>
> Scytl products and services are hosted on Amazon Web Services, a secure cloud service platform built on sound network infrastructure. AWS has multiple

> certifications, including SSAE 16, adhering to an extensive list of global security standards. [150]

228. The state of Texas via Department of Information Resources (DIR) has contracted with Amazon Web Services, Inc.[151]

229. Tarrant County contracted with Amazon Web Services via DIR contract #DIR-TSO-4221 which is a statewide contract that is subcontracted out to all Texas counties voluntarily.[152]

230. Our election system infrastructure is currently housed under the same web services as the vendor who reports our election results.

231. Texas counties contracted with SOE d/b/a Scytl are part of its international customers and are as follows: Tarrant, Comal, Gregg, Parker, Denton, Hood, Liberty, Jefferson, and Galveston.[153]

232. The United States has implemented several of Scytl's voting tools.[154]

[150] https://scytl.us/scytl-secure-election-technology/ Last visited 07/16/22

[151] https://acrobat.adobe.com/link/review?uri=urn:aaid:scds:US:70191bd6-f30f-3bbd-92d9-ca55c3115659#pageNum=1 Last visited 07/16/22

[152] https://acrobat.adobe.com/link/review?uri=urn:aaid:scds:US:5ec4ae30-77db-33be-89d2-664d92cfe7ff#pageNum=1 Last visited 17/16/22

[153] https://files.ttttexascom/case/TX_SOS_Election_Violation_References *See* Tarrant, Comal, Gregg, Parker, Denton, Hood, Galveston, Liberty, and Jefferson

[154] https://www.scytl.com/resources-and-references/customers/

a. Election Night Reporting (ENR)

b. Electoral administration: digitizing their training content and making it available to polling station workers through an online training platform.

c. The launching of a voter portal: a tool used to create websites for public administrations in order to provide electoral information before, during and after elections.

233. "Electronic election infrastructure is one example of critical infrastructure[155] which can be subject to remote access operations. Foreign remote access operation capabilities threaten critical infrastructure in the United States, such as election systems."[156]

234. Mills further states that successful " . . . remote access operations conducted against the United States election infrastructure could change vote totals reported by the elections equipment, thereby nullifying the election as an expression of the collective will of the voters."[157]

235. When Scytl was queried about the subject of potential risks, a spokeswoman answered flippantly. "(Voters) don't have the ability to review the source code of their (online) banking either." The company

u-s-elections/ Last visited 07/16/22

[155] https://www.cisa.gov/election-security

[156] https://files.ttttexas.com/static/docs/txsos/John-Mills.pdf *See* Declaration of John Mills 9

[157] *Id.* 10

claims that a public examination of the documentation would jeopardize its business model.[158]

236. How can Scytl's business practices be reconciled with the counties and states in the United States or Texas own government high security and transparency requirements?

237. How secure will Texas elections offerings be?

238. What exactly is the arrangement between Texas and the Spanish voting giant?

239. When it comes to transparency and auditability, Scytl's statements have been contradictory. At a 2017, trade conference called Swiss Cyber Storm, Jordi Puiggali, Scytl's longtime head of technology, gave a presentation.[159] When a participant asked him whether Scytl was prepared to release its source code, he stated it was out of the question of him.[160]

240. Two companies in particular that produce COTS are Huawei and Akamai, the latter of which is partnered with SCYTL and linked to Dominion Software. In the Election Whistleblower Affidavit Ms. Terpsehore Maras attests that the tallied votes on

[158] https//www.parliament.vic.gov.au/images/stories/committees/emc/2010_Election/submissions/14_Scytl_EMC_Inquiry_No.6 pdf Last visited 07/16/22

[159] https://2017.swisscyberstorm.com/2017/09/26/Introducing_Jordi_Puiggali.html Last visited 07/16/22

[160] https://www.republik.ch/2019/02/07/the-tricky-business-of-democracy Last visited 07/16/22

behalf of Dominion and, under contract with the Associated Press (AP), provide the results for reporting.[161]

241. A very similar contractual relationship is noted between several counties in Texas as noted above via SOE d/b/a Scytl.

242. Maras Affidavit corroborates to the vulnerabilities from COTS which are still culpable to domestic, as well as foreign hacking.[162]

MANPULATION AND SECURITY VULNERABILITIES

243. In January of 2021, DNI Ratcliffe issued an unclassified letter to Congress that assessed that China interfered in the 2020 federal elections.[163]

244. CISA also released an Industrial Controls System Advisory (ICSA) detailing vulnerabilities affecting versions of the Dominion Voting Systems.[164]

245. The exploitation of these vulnerabilities would require physical access to individual Election Management System (EMS) or the ability to modify files.

[161] *Id.* 25-26

[162] *Id.* https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Terpsehore Maras Election Software Whistleblower

[163] https://context-cdn.washingtonpost.com/notes/prod/default/documents/6d274110-a84b-4694-96cd-6a902207d2bd/note/733364cf-0afb-412d-a5b4-ab797a8ba154.#page=1

[164] https://www.cisa.gov/uscert/ncas/current-activity/2022/06/03/cisa-releases-security-advisory-dominion-voting-systems-democracy

246. These EMS systems are similar to, or the same as, the Decl. of Halderman detailed a number of these critical vulnerabilities in litigation with the state of Georgia.[165]

247. After the 2016 general elections, then Georgia Secretary of State, Brian Kemp, confirmed that 10 separate cyberattack attempts on Georgia's network had been discovered—all of which were traced back to a U.S. DHS IP address.[166]

248. On December 6, 2019 Democrat Senators (Senators Elizabeth Warren, Ron Wyden, Amy Klobuchar, and Representative Mark Pocan) sent letters[167] to the private equity firms that own the major election machine vendors (Hart InterCivic, Dominion Voting Systems, ES&S) stating their concerns regarding vulnerabilities of election machines, but also requesting disclosure of a range of such information including ownership, finances and research investments, compliance with Election Assistance Commission's (EAC) Voluntary Voting System Guidelines (VVSG), as well as violations of any federal or state laws or regulations.

249. In August of 2020, the Bipartisan Senate Intelligence Committee report[168] was released with the

[165] https://www.documentcloud.org/documents/21069743-2021-09-21-notice-of-filing-dckt-1177_1

[166] https://www.wsbtv.com/news/georgia/georgia-secretary-of-state-says-cyberattacks-linked-back-to-dhs/475707667/

[167] https://www.warren.senate.gov/imo/media/doc/H.I.G.%20McCarthy,%20&%20Staple%20Street%20letters.pdf

[168] https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

findings of the investigation into foreign interference of the 2016 elections. The report disclosed the lack of security in election systems utilized by the vast majority of the nation and warned of the likelihood of fraud and hacking in the November 3, 2020 elections.

250. Other significant findings were reported: regular targeting of numerous election infrastructures, security vulnerabilities with not only all major voting machine vendors, but also of all aspects of other election infrastructure (e.g., election night reporting (ENR), electronic poll book equipment, software, databases and cloud servers), and supply chains, lack of adherence to basic security practices, identification of two components of election infrastructure that required immediate, cybersecurity fixes: voter registration databases, and election night reporting websites, as well as no plausible means to audit elections.

251. Dr. Alex J. Halderman,[169] Professor of Computer Science at the University of Michigan, presented before the committee. He testified "our highly computerized election infrastructure is vulnerable to sabotage and even to cyber-attacks that could change votes." He concluded "Voting machines are not as distant from the internet as they may seem."

[169] https://www.c-span.org/video/? c4674512/user-clip-j-alex-halderman-voting-structure-vulnerable-sabotage-attacks-change-votes

252. Both the FBI[170] and CISA[171] issued two alerts regarding Iranian interference in the U.S. November 3, 2020, election in October of 2020.

253. The FBI and CISA reported targeting of state election websites with "intentional effort to influence and interfere with the 2020 U.S. presidential election".[172]

254. "The exploitation of key supply chains by foreign adversaries – especially when executed in concert with cyber intrusions and insider threat activities – represents a complex and growing threat to strategically important U.S. economic sectors and critical infrastructure".[173]

255. Several attacks on local, county and state government agencies have been reported over a short course of time. Texas was not and is not immune to these hacks, including in our own election systems[174].

a. "The U.S. intelligence community developed substantial evidence that state websites or voter registration systems in seven states

[170] https://www.fbi.gov/news/pressrel/press-releases/iranian-cyber-actors-responsible-for-website-threatening-us-election-officials

[171] https://www.ncsc.gov.uk/files/NCSC%20CISA%20Alert%20-QNAP%20NAS%20Devices.pdf

[172] https://www.cisa.gov/uscert/ncas/alerts/aa20-304a Last line of Summary Paragraph

[173] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Shawn Smith 15

[174] https://www.nbcnews.com/politics/elections/u-s-intel-russia-compromised-seven-states-prior-2016-election-n850296

were compromised by Russian-backed covert operatives prior to the 2016 election — but never told the states involved, according to multiple U.S. officials.

b. Top-secret intelligence requested by President Barack Obama in his last weeks in office identified seven states where analysts — synthesizing months of work — had reason to believe Russian operatives had compromised state websites or databases.

c. Three senior intelligence officials told NBC News that the intelligence community believed the states as of January 2017 were Alaska, Arizona, California, Florida, Illinois, Texas and Wisconsin."

256. According to the Declaration of John R. Mills; the "U.S. Government has pioneered and advanced the art and techniques of remote access operations targeting critical infrastructure."[175]

257. Based on his personal experience, Mr. Mills states that the U.S. Government has the capability to project significant effects[176] toward critical infrastructure worldwide. This would include Texas' own election systems. The capability to project "effects" exists in China, Russia, Iran, North Korea, and Venezuela as well as other countries. These foreign powers now use these same or similar, and improved remote access operation methodologies to advance

[175] https://files.ttttexas.com/static/docs/txsos/John-Mills.pdf

[176] "Effects" an operator's and planner's term of art which implies the ability to degrade, exfiltrate, manipulate, change, or destroy *See* Mills Declaration 15-footnote 4

their own national agendas. A growing talent base of personnel, software, and network enabled capabilities that are becoming global in the hands of companies and personnel outside of the U.S. Government.[177]

258. The Texas Election Systems are not the only state systems to have been hacked since 2016 even as recently as this year are the Texas Department of Agriculture, Public Utility Commission of Texas, Office of Court Administration, Department of Transportation, Texas Health and Human Services Commission and Texas Medicaid – in which information exposed included names, addresses, dates of birth, social security numbers and more – were compromised The state's answer was to pay a ransom to bad actors in an attempt to restore systems.[178]

259. Local county and city agencies reported – in some cases our tax dollars were paid to hackers – Brooks County, Bexar County Appraisal District, Harris County US Port, City of Austin, Aransas County, Bowie County, Parker County, City of Odessa, George W. Bush Presidential Center in Dallas County, Nacogdoches County, Calhoun County, Grayson County Government Systems, Burnet County Government Systems, City of Waco in McLennan County, City of Fort Worth in Tarrant County, City of College Station in Brazos County, Travis County Appraisal District , Lubbock

[177] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of John R. Mills 15-16

[178] https://www.dallasnews.com/news/politics/2021/03/05/terminated-texas-medicaid-subcontractor-dumped-after-data-breach-in-ransomware-attack-from-russia/

County Government Systems, and other state agencies[179].

260. If the state of Texas or any federal agencies cannot secure itself or our health and personal data from security breaches and exposure how are our elections safe or secure from manipulation? How do Plaintiffs know that our votes cast are not free from manipulation and dilution due to the former? The short answer is we cannot be sure. Plaintiffs know the electronic systems/machines are susceptible due to network connections and vulnerabilities of the electronic voting systems/machines themselves.

261. CISA acknowledged as early as October 2020 that hackers targeted not only Federal government, but also state, local, tribal, and territorial government—that is critical infrastructure, and election organizations including unauthorized access to election support systems.[180]

262. "However, CISA has no evidence to date that integrity of elections data has been compromised . . . CISA's credibility in their conclusion must be tempered by the knowledge that this was during the same period that CISA was unaware that its own networks had been compromised."[181] *Id.*

263. In the litigation case of Curling and at its conclusion the federal court stated,

[179] https://www.seculore.com/resources/cyber-attack-archive/texas

[180] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Shawn Smith Line 35

[181] https://www.cisa.gov/uncert/ncas/alerts/aa20-283a

a. "Evidence presented in this case overall indicates the possibility generally of hacking or malware attacks occurring in the voting systems and this particular system through a variety of routes-whether through physical access and use of a USB flash drive or another form of mini-computer, or connection with the internet. As discussed in the declarations and testimony of the proffered national cybersecurity experts in this case, a broad consensus now exists among the nation's cybersecurity experts recognizing the capacity for the unobserved injection of malware into computer systems to circumvent and access key codes and hash values to generate fraudulent codes and data. In these experts' views, these risk issues are in play . . . " *Curling v. Raffensperger*, 493 F. Supp. 3d 1264, 1280 (N.D. Ga. 2020)

SUPPLY CHAIN VULNERABILITIES

264. The Affidavit of Terpsehore Maras highlights voting systems rely on foreign made Commercial Off The Shelf (COTS) components rather than custom components manufactured in the United States.[182]

265. While this presents an affordable and economic solution to meet the voting demand, it also means these COTS components introduce vulnerabilities into the Voting Systems. These vulnerabilities can

[182] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of Terpsehore Maras Election Software Whistleblower Line 20

take the form of proprietary hardware and software that has not been through vulnerability testing.[183]

266. The components are manufactured in countries that have strained political and economic relations with the United States. There are numerous intelligence reports, both US Government and Commercial-sourced, highlighting the vulnerabilities in hardware and software components manufactured by foreign countries.[184]

a. "In the light of CISA's inability to defend even its own computer systems from nation-state level supply chain attacks from March through December 2020, little credence can be given to CISA's July declaration that the 2020 election would be 'the most secure election in modern history, and its declaration in November 2020 that the 2020 election was the "most secure in American history".[185]

b. "In fact, the EAC's "test assertions" for the Voluntary Voting System Guidelines (VVSG) "which are meant to translate each VVSG requirement into unambiguous, specific, testable condition so that the Voting System Testing Lab (VSTL) may verify the conformance of a given voting system to the VVSG standard. Here is what the EAC's VVSG Test

[183] *Id.* Line 22-24

[184] *Id.* Line 22, 25

[185] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of Shawn Smith Line 21

Assertions state for supply chain security of voting system components:"[186]

c. 2.1.1-A – General build quality . . . TA211A-2: "If components from third-party suppliers are used for their intended purpose within the voting system, THEN the voting system manufacturer MUST ensure that third-party suppliers document the quality assurance procedures used to ensure components supplied from third-parties are free from damage or defect".[187]

267. This is the proverbial fox guarding the hen house situation in which we trust third-party vendors in our supply chain. As the VSTL's are now to verify their conformance with Voting System Standards and VVSG, and that their tests ensure the security and integrity of voting systems but do not address the supply chain attack threats or their mitigation or assessment.[188]

268. Terpsehore Maras emphasized the significance of a VSTL's role in the certification process, stating the significance of VSTLs being accredited and examining the hardware is key.[189]

269. COTS software updates are the avenues of entry. While the use of outsourced COTS, manufactured

[186] *Id.* 47

[187] *Id.* 47

[188] *Id.* 46-48

[189] https://files.ttttexas.com/case/TX_SOS_Election_Violation_ References *See* Declaration of Terpsehore Maras Election Software Whistleblower Line 22

outside the US presents an affordable and economic solution to meet the voting demand, it also means these COTS components introduce vulnerabilities into the Voting Systems.[190]

270. These vulnerabilities can take the form of proprietary hardware and software, which lack vulnerability testing and are outsourced for manufacturing in countries that have strained political and economic relations with the United States.[191]

271. COTS components by voting system machine manufactures can be used as "Black Box" and due to changes to their specs and hardware make up change continuously. Some changes can be simple upgrades to make them more efficient, cost effective, end of life extension and or even complete reworks to meet new standards. The key issue is that MOST of the COTS are outsourced to China and makes us vulnerable to "Black Box" antics and backdoors.[192]

272. "The proprietary voting system software is done so and created with cost efficiency in mind and therefore relies on 3rd party software that is AVAILABLE and HOUSED on the HARDWARE. This is a vulnerability. Exporting system reporting using software like Crystal Reports, or PDF software allows for vulnerabilities with their constant updates."[193]

[190] *Id.* 22-23

[191] *Id.* 23

[192] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of Terpsehore Maras Election Software Whistleblower Line 22

[193] *Id.* 23

273. " . . . country of manufacture or origin for a representative sampling of computers and computer hardware components used in those voting systems . . . The voting systems used in these counties represent three of the top four U.S. voting systems vendors, whose voting systems are used to cast and or tabulate over 80% of votes in the U.S. elections." The third largest voting system vendor is Hart InterCivic, which unlike Dell used by ES&S, used Hewlett-Packard (HP) computers. It is a difference without distinction, as HP computers are manufactured and assembled primarily in the People's Republic of China by foreign workers with no U.S. government oversight. Effectively, there are no safeguards in the entirety of testing or EAC certification for these electronic voting system/ machines. All electronic voting systems/machines utilize COTS software with thousands of known vulnerabilities which can be exploited both before and after delivery.[194]

274. One such component was found in the ES&S contracts for Collin County and Bexar County.[195]

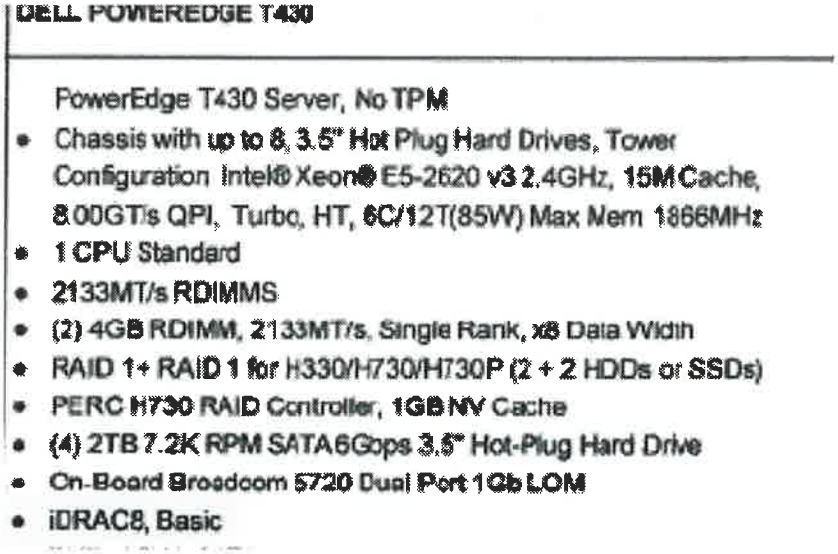
275. Listed under Dell PowerEdge T430 is listed a component "iDRAC8" which is installed in the EMS.

276.

Dell Poweredge T430

[194] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of Shawn Smith Line 79

[195] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Collin and Bexar County ES&S Contract

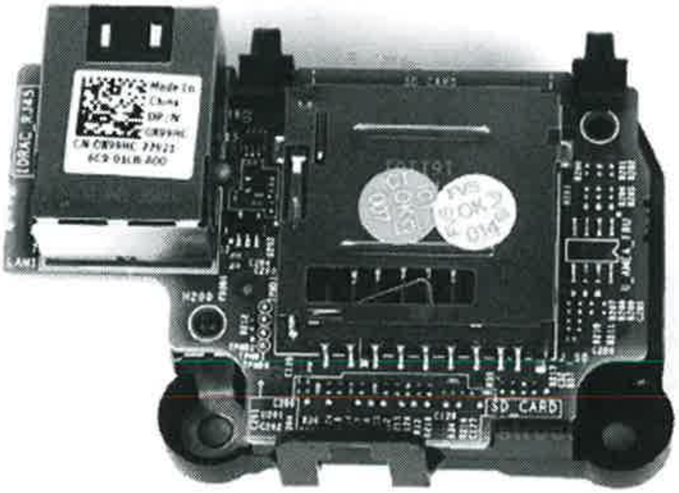


DELL POWEREDGE T430

PowerEdge T430 Server, No TPM

- Chassis with up to 8, 3.5" Hot Plug Hard Drives, Tower Configuration Intel® Xeon® E5-2620 v3 2.4GHz, 15M Cache, 8.00GT/s QPI, Turbo, HT, 6C/12T(85W) Max Mem 1866MHz
- 1 CPU Standard
- 2133MT/s RDIMMS
- (2) 4GB RDIMM, 2133MT/s, Single Rank, x8 Data Width
- RAID 1+ RAID 1 for H330/H730/H730P (2 + 2 HDDs or SSDs)
- PERC H730 RAID Controller, 1GB NV Cache
- (4) 2TB 7.2K RPM SATA 6Gbps 3.5" Hot-Plug Hard Drive
- On-Board Broadcom 5720 Dual Port 1Gb LOM
- iDRAC8, Basic

277.



278. iDRAC is a Dell Remote Access Controller. "iDRAC . . . . is part of a larger datacenter solution that helps keep business critical applications and workloads available at all times . . . allows administrators to deploy, monitor, manage, configure, update,

troubleshoot and remediate Dell servers from any location, and without the use of agents."

279. "Leveraging the incomparable agent-free capabilities of the embedded, integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller technology, server deployment, configuration and updates are streamlined across the OpenManage portfolio and through integration with third-party management solutions."[196]

280. "Remote management: iDRAC8 with Lifecycle Controller, iDRAC8 Express (default), iDRAC8 Enterprise (upgrade), 8GB vFlash media (upgrade), 16GB vFlash media (upgrade)"

281. The Declaration of John R. Mills describes remote access operations as generally " . . . activities used to access computer networks, data centers, and other equipment, conducted in a manner to avoid leaving behind forensic evidence of the access. Remote access operations are often enabled by planted malware, enabling software, and/or algorithms in the targeted computer system."[197]

282. "Remote access operations are different from remote maintenance monitoring which is intended by network designers for transparent and auditable access to network enabled devises for maintenance and updates." These remote maintenance monitoring can be subverted or co-opted for reasons that do not

[196] https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/aa/Dell-PowerEdge-T430-Spec-Sheet.pdf Last visited 06/23/22

[197] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of John R. Mills 4

involve or are in accordance with remote maintenance monitoring tenets, design or intent, network owners/ operators, or for lawful access or purposes.[198]

283. The iDRAC8 modem creates a serious security breach and violates a multitude of election and penal codes.[199]

284. Bruce Sherbet, an Elections Administrator, stated via email that the county must receive an approval from the SoS's office prior to purchasing a voting system.[200]

285. If electronic systems are continued to be used in any Texas elections and are compromised, which there is opportunity, then it is more than reasonable to conclude that U.S. elections are compromised through our voting system vendors' supply chains. What resource is more valuable to this country than the vote of the American people?

a. "Without access to comprehensive real-time and post-election data, and a cadre of cyber expertise that exceeds U.S. workforce quantity and quality resources, we may never know. This is true not only because supply chain attacks can be extraordinarily difficult to detect, but also because the safeguards inherent in the U.S. voting system testing and certification regime are practically non-existent, and because the nation in which

[198] *Id.* 5

[199] *See* Tex. Elec Code 122.001(a)(4), TEX. PEN. CODE § 16.02, § 33.05, 18 U.S.C. § 1030

[200] *See* Line 447 of this document, Tex. Elec Code 122.005(a)

most of the systems and their components are manufactured and assembled is engaged in a decades-long campaign to infiltrate, corrupt, and compromise Western, and especially U.S., computers and computer-based systems, including government and election systems."[201]

b. "The employment of machine-based algorithms to access electronic voting systems in the United States to impose a pre-determined election outcome through remote access operations is well within the capabilities of many nation-state actors such as China, Russia, Iran, and Venezuela, as well as even non-nation state actors."[202]

E. Declaration of Terpsehore Maras Election Software Whistleblower

286. The Affidavit of Terpsehore Maras attesting the 2017 elections is null and void due to lack of Election Assistance Commission (EAC) certifications of Voting Systems and the Voting System Test Laboratories (VSTL) used to certify the Voting Systems. (Exhibit Q)[203]

RULE: Section 231(b) of the Help America Vote Act (HAVA) of 2002 (*42 U.S.C. § 15371(b)*) requires

[201] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of Shawn Smith Line 80

[202] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of John R. Mills 11

[203] https://files.ttttexas.com/static/docs/txsos/Exhibit-Q.pdf *See* Declaration of Terpsehore Maras Election Software Whistleblower

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

287. To meet its statutory requirements under HAVA § 15371(b), the EAC has developed the EAC's Voting System Test Laboratory Accreditation Program. The procedural requirements of the program are established in the proposed information collection, the EAC Voting System Test Laboratory Accreditation Program Manual. Although participation in the program is voluntary, adherence to the program's procedural requirements is mandatory for participants. The procedural requirements of this Manual will supersede any prior laboratory accreditation requirements issued by the EAC. This manual shall be read in conjunction with the EAC's Voting System Testing and Certification Program Manual (OMB 3265-0018).

288. The person filing the affidavit is over the age of 21 and under no legal disability which would prevent them from giving this declaration. The election software whistleblower has extensive experience gathering foreign intelligence in support of operations which took place within the Continental United States (CONUS) and Outside the Continental United States (OCONUS). She is a trained Cryptolinguist, holds a

completed degree in Molecular and Cellular Physiology with formal training in other sciences such as Computational Linguistics, Game Theory, Algorithmic Aspects of Machine Learning, and Predictive Analytics. Terpsehore Maras possess more than two decades of experience in mathematical modeling and pattern analysis as well as lesser experience in network tracing and cryptography. Additionally, she has extensive involvement in overseeing OCONUS elections and the HAVA Act for CONUS elections. The information presented in the affidavit is her personal, first-hand account.

289. Voting Systems rely on foreign made Commercial Off The Shelf (COTS) components rather than custom components manufactured in the United States. While this presents an affordable and economic solution to meet the voting demand, it also means these COTS components introduce vulnerabilities into the Voting Systems. These vulnerabilities can take the form of proprietary hardware and software that has not been through vulnerability testing. The components are manufactured in countries that have strained political and economic relations with the United States. There are numerous intelligence reports, both US Government and Commercial-sourced, highlighting the vulnerabilities in hardware and software components manufactured by foreign countries. (*See* Exhibit Q for a detailed explanation of COTS)

290. Two companies in particular are Huawei and Akamai, the latter of which is partnered with SCYTL, which is linked to Dominion Software. SCYTL receives the tallied votes on behalf of Dominion and, under contract with Associated Press (AP), provides the results for reporting. This shows that voting

information is under the control of the companies that provide the Voting Systems.

291. A further vulnerability are the algorithms which, under the guise of posing as encryption methodologies, provide a means by which votes can be changed. This process will be summarized below.

292. Observation made during the 2020 election:

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

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

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

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

293. This means that SCYTL can read the contents of each ballot because it uses the same key as Dominion to encrypt/decrypt. This key provides access to the "commitments" which are the values of the votes cast. In the 2020 Presidential election there would have been commitments for Trump and for Biden. Those commitment values can be altered by SCYTL, re-encrypted using the same key and appear as though nothing has been changed. When challenged they fake a proof of ciphertexts.

294. The issue with this is randomness of votes. During the 2020 election, there were periods where

blocks of votes for Biden were seen without any votes for Trump. That is statistically improbable and points to block allocation of votes to one candidate by the algorithm. This was witnessed when there were massive spikes of votes for Biden in certain geographical locations instead of the natural progression.

295. It is further attested of first-hand knowledge by the Obama-Biden administration to deploy this same election software in [redacted] in 2013. Further, on or about April 2013, a one-year plan was set to fund and introduce elections in [redacted]. Joe Biden was designated by Barack Hussein Obama to ensure the [redacted] accepted assistance. John Owen Brennan and James Clapper were responsible for the ushering of the intelligence surrounding the elections in [redacted]. Under the guise of Crisis support the US Federal Taxpayers funded the deployment of the election software and machines in [redacted] signing on with SCYTL.

296. Using the same process outlined above, SCYTL was allowed to tally the votes rather than the election machines. The elections were held on May 25, 2014, but the results were delayed allowing the election results to be modified in favor of [redacted]. There was a false claim of Russian DDoS when in fact it was an injection of block votes.

297. In the case of the US elections, Dominion, ES&S, Smartmatic, Hart InterCivic would have to manually deploy keys if remote access to Voting Systems failed. This occurred nationwide for days and in the case of Alaska, with a mere 300,000 registered voters was stuck at 56% reporting for nearly a week. This indicates a failed deployment of a script to block allocate votes remotely from one location. This would

also justify the presence of the election machine software representatives making physical appearances in states where election results are being contested.

298. This is why accredited VSTLs are so important to the election process. This also underscores why it is imperative VSTLs maintain their accreditation to ensure compliance with and adherence to updated standards.

299. There are only two accredited VSTLs: Pro V&V and SLI Compliance.

300. Pro V&V is owned and operated by Ryan Jackson "Jack" Cobb and headquartered out of Huntsville, AL, USA. (*See* Exhibit Q regarding ties to Aerospace Defense Contracting Entity and address discrepancies)

301. SLI Compliance is a Division of Gaming Laboratories International, LLC and headquartered out of Wheat Ridge CO, USA.

302. Pro V& V and SLI Compliance both lack evidence of EAC Accreditation as per the Voting System Testing and Certification Manual. Certifications expired in 2017 for VSTLs and for Voting Systems as well. This means the Voting Systems used in the 2020 elections were not certified.

303. CONCLUSION: This affidavit presents unambiguous evidence of:

a. Foreign interference

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

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

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

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

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

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

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

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

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

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

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

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

305. "Those responsible within the Intelligence Community directly and indirectly by way of procurement of services should be held accountable for assisting in the development, implementation, and promotion of GEMS" (Dominion Software Foundation)

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

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

308. Currently a defamation complaint has been filed, Case. No. 1:21-cv-00317-DCLC -CHS in the United States District Court for the Eastern District of Tennessee Chattanooga presiding Judge Clifton L. Cocker. Terpsehore Maras has filed this complaint in regards defamation in which several defendants have been named regarding the affidavit summarized above.

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

F. Declaration of Halderman

309. This is a summary of the Declaration of Mr. J. Alex Halderman in regard to the case of Curling et al v. Raffensperger et al.[204] Mr. Halderman makes these claims under oath and this summary will neither make inferences from nor inflate his statements.

310. Mr. Halderman claims the 2016 presidential election was subject to multiple attempts to interfere with and undermine the election process through cyberspace. He cites incidents such as compromised email accounts belonging to the Democratic National Committee and John Podesta. He also cites attempted intrusions into election-related systems via cyberspace in at least 18 States. Voter data was successfully exfiltrated in two states and in a subset of those 18, attackers could have altered or deleted voter registration data.

311. Mr. Halderman states Russia has sophisticated offensive cyber capabilities as well as intent to use them to hack elections in other locations. He goes on to cite published reports of Russian involvement in hacking the Ukrainian election in 2014. He states that countries other than Russia have similar offensive cyber capabilities.

312. The U.S. Senate Select Committee on Intelligence reported findings and recommendations based upon its investigation into cybersecurity threats to U.S. election infrastructure. Mr. Halderman cites this report as evidence of vulnerabilities in the existing election system used in the United States. Further he

[204] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of Halderman

quotes DNI Coats and DHS Secretary Nielsen of Russia's continuing goal to interfere in the elections within the U.S. to achieve a variety of outcomes favorable to Russia. He specifically calls out the Paperless Direct Recording Electronic (DRE) voting machines as being particularly vulnerable to exploit.

313. The DRE machines do not create a paper record of each vote. Paperless DRE machines are notoriously vulnerable to cyber attacks that can cause a multitude of issues. Votes can be changed or erased. Extra votes can be cast, and machines can be made to not work at all. He goes on to state that paperless DRE machines do not provide even adequate security against cyber attacks.

314. He points out Dominion voting systems as being exclusively used in the State of Georgia and that over the past 15 years he, and others, have repeatedly warned of the vulnerabilities in this system. These vulnerabilities include both hardware and software flaws. There are also network architectural weaknesses that cannot be repaired through software updates.

315. These types of voting systems use software that can be reprogrammed. Any attacker gaining privileged access to that software can modify it to do anything. He has proven through multiple demonstrations how easy it is to install malware on these systems.

316. Mr. Halderman cites the first major study of voting systems conducted in 2003 where it was discovered the source code contained multiple errors and vulnerabilities. The States of Maryland and Ohio commissioned independent studies and the resulting

assessments confirmed the vulnerabilities in the Dominion voting systems.

317. In 2006, another independent security researcher also identified vulnerabilities, primarily in the software update mechanism that would allow upload of malware. That same year, Mr. Halderman and others reverse engineered a Dominion voting system and identified multiple additional vulnerabilities.

318. As part of this study, they developed malware that would modify all the vote records, audit logs, and protective counters, preventing any forensic examination from discovering the crime. The malware was also designed to spread automatically to other voting machines. This was propagated by the removable memory cards used to program the ballot design.

319. In 2007, Mr. Halderman participated in two independent studies for the States of California and Ohio. In both studies, additional vulnerabilities were discovered that would allow malware to be installed and propagated to cause even more harm than the virus created during the 2006 test. Mr. Halderman states that some of the vulnerabilities could be resolved by improving the underlying software. Other vulnerabilities are more serious and require hardware and software changes. As a result, California, despite having a paper ballot trail, decided to decertify the Dominion voting system in use at that time.

320. Mr. Halderman points out there are a variety of techniques available to sophisticated attackers to compromise non-internet connected systems. One of those techniques is the removable media cards being exploited via the Election Management System (EMS) prior to insertion in the voting machine. He also states

the EMS has recently had remote access software installed which creates another means of exploitation. The physical security measures in place to secure the removable memory cards are also weak and can be easily compromised.

321. Mr. Halderman goes on to describe how a potential attack might take place. The attacker would gain access to the election management computers via weak cyber security. The attacker would then target the pre-election ballot programming with malware that would spread from machine to machine. This malware would automatically shift "a few percent of the vote" to a particular candidate.

322. Mr. Halderman then describes the inadequacy of certain physical security measures, such as tamper evident seals. These would be less than adequate when the memory card is inserted with the malware already loaded. Furthermore, logic and accuracy tests only validate the ballot design or counting logic. Such tests would fail to detect malware as it could be programmed to detect and circumvent logic and accuracy tests or only perform on election day.

323. Mr. Halderman states the existing measures to defeat election and voting fraud do not provide a way to determine if fraud occurred during the election or afterward. Malware could be programmed to make it appear statistically probable despite the countermeasure testing taking place. In fact, the malware would delete itself and all log files, thereby preventing any kind of forensic evidence.

324. Mr. Halderman states the only way to reliably safeguard a voting system from future cyber attacks

is to generate and examine physical evidence of voter intent, in the form of a voter-verifiable paper trail. Optical scan paper ballots are the most widely used and secure technology available for casting votes, according to Mr. Halderman. The manipulation of both paper and electronic ballots could still be compromised but would require more extensive resources.

325. Mr. Halderman points out that with the monies associated with the Help America Vote Act (HAVA) 2002 in conjunction with the U.S. Senate Select Committee on Intelligence recommendation that States replace outdated voting systems with newer systems that have a verified paper trail. He also states the use of all DRE type machines should be discontinued.

G. Declaration of Shawn Smith

326. Shawn Smith, retired Military officer with a Master's degrees in National Security Affairs and in Aeronautical Science, filed a declaration on 6/8/22 into *Kari Lake, et al. v. Karie Hobbs*, Arizona Secretary of State (case 2:22-cv-00677-JJt)[205].

327. In this declaration, he states that his military occupational specialty was space and missile operations, and he has extensive experience in operating, planning, training, testing, and commanding the employment of complex, computer-based military weapons systems.

328. He states that 'I have been asked to testify about the threat of the compromising of our supply

[205] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of Shawn Smith

chain and attack(s) to U.S. national security systems and critical infrastructure, in particular to election related systems, including voting systems and consequently, to elections." As noted in other expert affidavits and declarations, Smith describes the vulnerability of the U.S.'s critical systems, resulting from compromised supply chains, to include elections. He states that it is his, "conclusion that U.S. elections are critically vulnerable to exploitation by foreign adversaries through compromising of our computerized election systems through supply chains."

329. He goes on to say, that despite this fact, the U.S. Government appears to be keenly aware of the risk of supply chain compromise to the nation's critical systems. This same awareness does not appear to extend to any agency responsible for the "procurement, security, certification or use of election and voting systems, nor to imbue them with any capacity to respond effectively."

330. The targeting of U.S. voting and election systems must be an extraordinarily high priority for foreign powers and bad actors.

331. Smith demonstrates that supply chain compromise is pervasive, sophisticated, widespread and can take place at any stage of the supply chain including: Manipulation of development tools, development environment, source code repositories (public or private), source code in open-source dependencies, software update/distribution mechanisms, compromised and/or infected system images (multiple cases of removable media infected at the factory), replacement of legitimate software with modified versions, sales of modified/ counterfeit products, and shipment interdiction.

332. Smith explains that the public lacks awareness of the severity and pervasiveness of threats to supply chain compromise from malicious cyber activity commonly being portrayed by media as an opportunistic hacker, rather than nation state operated or sponsored advanced persistent threat (APT) groups.

333. Smith identifies a multitude of such APT groups that have in the past and are currently utilizing supply chain attacks, as well as evidence of many investigations and reports. Prosecutions have occurred by several U.S. entities including the DOJ, Department of Commerce, National Counterintelligence and Security Center, Office of the Director of National Intelligence, National Institute of Standards and Technology, CISA, and the FBI. Smith demonstrates that the institutions, measures, laws, and guidelines intended to secure U.S. elections are grossly inadequate:

a. Supply chain threats for critical computer-based infrastructure, such as election ecosystems, are so severe and extensive that the "computer networks of the Cybersecurity and Infrastructure Security Agency (CISA), the very U.S. government institution responsible for critical infrastructure security, were compromised by software supply chain attacks in 2020, the SolarWinds, SUNBURST and SUPERNOVA attacks, for ten months or more without detection and, even then, that compromise only became known to CISA due to the intervention of a private company."

b. "In the light of CISA's inability to defend even its own computer systems from nation-state level supply chain attacks from March through December 2020, little credence can be given to CISA's July declaration that the 2020 election would be 'the most secure election in modern history, and its declaration in November 2020 that the 2020 election was the "most secure in American history.' "

c. "CISA has acknowledged, as early as October 2020, that APRs have targeted not only the Federal government, but state, local, tribal, and territorial (SLTT) governments, critical infrastructure, and elections organizations, including successful APT establishment of unauthorized access to election support systems."

d. Despite repeated warnings and recommendations from NIST, the technical body and agency identified in TITLE 52, USC to advise the EAC, to take measures to secure against supply chain attacks since 2012, the EAC has effectively provided no standards, procedure or safeguards to implement those recommended protections for election systems and elections.

e. To date, nearly all the systems certified and in use in the United States have no supply chain security, nor any testing or verification of the security as a result of the EAC's failures to implement protections. Although the latest version of the VVSG acknowledges supply chain risk manages as a necessity, no real safeguards were added. Smith states, "these standards are barely better than the EAC's non-existent standards for electronic poll books, centralized statewide voter registration systems, and election auditing systems.

f. According to VVSG, security testing guidelines do not even require VSTLs to review common vulnerabilities and exploits that are publicly available.

g. "The EAC's standards of accreditation for VSTLs do not even ask, let alone require, awareness in the VSTLs of supply chain vulnerabilities in computerized voting systems, much less awareness or proficiency in the detection of supply chain compromises, or in their assessment of effective mitigation, where even possible, by voting system vendors."

h. The Technical Guidelines Development Committee (TGDC) is the advisory body established by HAVA to "assist the (EAC) in the development of (VVSG)", includes far more "lawyers, politicians, public affairs, and psychology grads than computer scientists or software expert, at a 4:1 ratio." In addition, of those few committee members that are computer scientists and software experts included the director for software development at one of the largest US voting system vendors.

i. Although NIST recommended to the TGDC that no wireless devices be permitted on voting systems as early as 2006, the "TGDC" in 2020 still held a "compromise position" with no prohibition on wireless devices for the latest 2021 VVSG. Smith states, "permitting wireless devices in computerized voting systems is irrational and indefensible in light of the known and persistent threats to those systems."

j. "The EAC has demonstrated inadequate awareness, comprehension, and response to the clear and present danger posed by foreign nation states, supply chain attacks against the computers and components used in U.S. voting systems." Furthermore, the EAC "can't be relied upon to protect U.S. elections by competently examining voting systems, prior to use, for indicators of compromise and vulnerability."

k. Laboratory Director, and corporate principal, for the VSTL Pro V & V, stated that he had no "specialized expertise in cybersecurity testing or analysis or cybersecurity risk analysis," in a federal court testimony in 2020.

l. Furthermore, the same VSTLs, despite lacking specialized expertise in cybersecurity testing or cybersecurity risk analysis, are responsible to not only conduct initial and modification testing, but are also responsible to recommend to the EAC whether those changes may be implemented without testing, as "de minims." Smith describes several other factors that further negatively impact the security of elections

m. "Even if states and localities could afford the caliber of cybersecurity expertise needed to defend voting systems, the U.S. workforce of qualified cyber professionals is too small to staff voting systems offices in 50 states, much less over our 3,000 U.S. Counties. Hart InterCivic appears to use Hewlett-Packard computers, which are remanufactured and assembled overseas, containing overseas-manufactured components, built by foreign workers, and all without U.S government oversight and "effectively no safeguards in the entirety of the testing and certification regime for voting systems"

n. "ES&S is owned by the private equity firm McCarthy Group, which doesn't disclose the information of investors, including if any other investments or financial interests, have a controlling interest in ES&S."

H. Declaration of John R. Mills

This is a summary of the Declaration of John R. Mills. It is provided without amplification or supposition.[206]

334. Mr. Mills is a retired Colonel in the United States Army Reserve. He has also served as Former Director of Cybersecurity Policy, Strategy, and International Affairs, as a Senior Civilian in the Office of the Secretary of Defense. This afforded nearly 40 years of service to the United States of America and gave him extensive experience in the employment of cyberspace capabilities. He has held a Top Secret Sensitive Compartmented Information (SCI) security clearance since approximately 1988. Mr. Mills has

[206] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Declaration of John R. Mills

also been an Adjunct Professor teaching graduate level cybersecurity law and policy at the University of Maryland, Global Campus since 2013. His final uniformed position within DoD was as liaison to DHS where he coordinated the national response to emergencies and threats to the United States.

335. The testimony of Mr. Mills regarding the use of remote access operations for the unlawful entry and purposes into computer networks was requested. The information is unclassified and based on his personal experience, publicly available reporting and open source information.

336. Remote access operations are designed to gain access to computer networks to avoid detection and residual forensic evidence. This is accomplished via implanted malware, other software and/or algorithms that facilitate access to the targeted system.

337. Remote access is not the same as remote maintenance. Remote access is intended as a legitimate activity subject to active or passive monitoring and logging of the event. Remote maintenance can be compromised to suit the needs of remote access operations given discoverable vulnerabilities.

338. The capabilities to conduct remote access have greatly expanded since the 1980s. The primary user of remote access is the U.S. Intelligence Community in close partnership with the Department of Defense and Federal Law Enforcement.

339. Remote access operations capability is not limited to the United States. Several countries, organizations, and individuals have developed skillsets with varying degrees of sophistication. These actions have accelerated over the last 20 years and have

become commonplace among nation state and private actors.

340. Electronic election infrastructure is considered critical infrastructure and can be subjected to remote access operations. A successful remote access operation could change vote totals rendering elections null and void.

341. Employment of machine-based algorithms to enhance remote access operations is well within the skillset of nation-state actors such as China, Russia, Iran, and Venezuela. This capability also exists with non-nation state actors.

342. Mr. Mills states his review of the Mesa County Forensic reports are consistent with remote access operations.

343. He has served as a sworn election official and understands the U.S. election process at the county level. Due to this and his previous experience mentioned, he states he has very low confidence in the security of American election critical infrastructure.

344. Mr. Mills contradicts the claims of the U.S. Intelligence Community, Homeland Security, and Law Enforcement Agencies that they have the ability to defend election infrastructure from remote access operations. He states, their high level of confidence is not supported, and in some cases, may be false. He goes on to relate the breach of the Office of Personnel Management which, despite the resources available to stop such an attack, failed to do so.

345. In his professional opinion, the statement, "The November 3rd election was the most secure in

American history" asserted by CISA, had little, if any, basis in fact.

346. Mr. Mills continues by highlighting the statements made by CISA would require assessment of the indicators used by the National Intelligence Collection priorities to track, monitor, and collect during the 2020 election. Furthermore, he states, the capability of CISA to detect, assess, and respond to remote access operations in a timely manner, with high confidence, is unrealistic and they have a poor track record to back up this statement.

347. Mr. Mills states the Mesa County findings are consistent with publicly known intrusion sets, that are likely nation state level, with intimate insider knowledge of the infrastructure. He likens the actions taken by the actors be so deeply technical that anyone monitoring the activity would be unable to detect what was happening given the level of complexity.

348. Throughout Mr. Mills career he has received a variety of training, some of which includes work in the Special Operations community. Part of that work included planning, implementing, observing, and recommending during elections both in the United States and in foreign countries.

349. Mr. Mills had the opportunity to provide advice for the January 2020 elections in Taiwan. Among his many recommendations were to keep the process as simple as possible. This included reliance upon paper ballots, hand counting, and minimization of election machines as well as any connectivity components or sub-components. In addition, he advised that any tabulation of ballots (when not hand-counted) be performed as transparently as possible, and on

machines with no other features other than to tabulate the ballot. This would limit the ability to conduct remote access operation methods to the power cord used to power the tabulating machines.

350. As a result, the Taiwanese elections were conducted flawlessly. The counting of ballots was done live with multiple observers from both parties. As the ballot was verified and passed through the tabulator, the counts were changed automatically for all to see.

351. Mr. Mills then provides a history of remote access operations from post World War II to the present.

352. Mr. Mills states there is no independent third party review of electronic voting systems. The level of expertise by those officials who review or access these systems is woefully inadequate.

353. He states contractors use intellectual property rights or contractual terms to deny any third party review of the election systems they provide.

354. Mr. Mills further states that the culture within the U.S. Intelligence Community actively stifled any findings from analysts that concluded China interfered in the 2020 U.S. elections. Even going so far as to pressure analysts to change or withdraw their support proof of Chinese actions.

355. Mr. Mills goes on to state that while federal government officials are well meaning, they simply do not understand U.S. election infrastructure.

356. He points out anomalies in various statements made Mr. Chris Krebs, then Director of CISA, who claimed the election of 2020 was secure. Mr. Mills

highlights the inaccuracies in multiple statements made by Mr. Krebs.

357. Mr. Mills points out that ES&S has admitted to building in remote access to their machines. He goes on to state that many of the security procedures designed to restrict the ability of remote access operations, are not being used.

358. Mr. Mills concludes by assessing the current voting process has become over-sophisticated; and asks why it would need to this way. He raises legitimate questions of why counties are spending inordinate amount of resources on a technology environment without an evaluation of whether it is truly necessary. He further assesses there are no checks and balances on sworn elected officials and that the entire notion of electronic voting machines needs to be revisited.

I. Texas County Failures

HOOD COUNTY

359. Hood County Commissioners, in addition to election officials, have failed to confirm if the voting equipment in Hood County is properly certified.

360. On July 28, 2021, Michele Carew was questioned about the issue of non-sequential ballots.[207]

361. November 9, 2021, Plaintiff Karen Towell addressed the Hood County Commissioner's court regarding the lack of accredited VSTLs and thereby

[207] https://www.texastribune.org/2021/10/01/texas-election-official-hood/ (Last visited 5/20/22)

the lack of state certifications. Plaintiff provided evidence similar to the evidence in this case.[208]

362. Michele Carew resigned shortly after the November 2021 meeting.

363. ES&S was the voting system employed within Hood County.[209]

a. ES&S was first utilized for elections in Hood County in 2008 and continued to be used through the November 2020 election.

b. According to Melissa Welborn, H. R. Director or Hood County, ES&S version 3.4.1.0 was utilized for the November 2020 elections.

c. The last certification on file indicates that ES&S version 3.4.1.0 was certified in April 2014.

364. On February 9, 2021, a contract was signed with Hart InterCivic voting systems for use in elections in Hood County.[210]

[208] https://duckduckgo.com/?q=hood+county+commissioner+meeting&iax=videos&ia=videos&iai=https%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DuguFcPW7P_A (Lasted visited 5/20/22)

[209] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Hood County ES&S Contract

[210] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Hood County Hart Contract

a. Certification for Hart InterCivic Verity Voting software version 2.4[211] is on file with the Secretary of State website.[212]

b. Hood County records indicate that Hart InterCivic software version 2.4.2 was utilized for the November 2, 2021, elections.

c. During inspection of the Hart InterCivic Verity Voting 2.4.2, conducted on April 14-17, 2020, one examiner noted an "over-vote" issue and yet still recommended the version for certification.[213]

4. In the voting process, an "over-vote" bring up a warning when more than one candidate can be voted for in a specific race. However, when you make your selection to continue, there is an automatic de-selection of another candidate chosen rather than allowing the voter to decide who gets deselected. This could lead to voter confusion and a casting of an unintended vote without the voter's knowledge.

d. Another note in the Hart InterCivic Certification Test Report Modification document states that Verity Voting version 2.4 is Hart InterCivic Verity Voting 2.4.2. No other version of any Hart modified software/firmware is certified under an original version number as modified versions are not the same as the

[211] https://www.sos.state.tx.us/elections/forms/sysexam/hart-verity-2.4-certification-order.pdf (Last visited on 5/18/22)

[212] *See* Tex. Elec Code § 122.036

[213] https://www.sos.texas.gov/elections/forms/sysexam/brandon-hurley-hart-2.4.pdf#search=hart%202.4.2 (Last visited 5/18/22)

original. The original version is also not decertified for use in Texas.[214]

e. In an "Electrical Hardware Test Plan" Verity Voting 2.4 Discrepancies, conducted by SLI Compliance, issues arose with the "*proposition text not saving properly during election creation*" and "*loss of audio clarity when audio speed set to high*". (*Emphasis added*)[215]

> HV24-13 — Verity Data/Build – Proposition Text Not Saving Properly During Election Creation
>
> HV24-12 — Loss of Audio Clarity When Audio Speed Set to High
>
> HV24-8 — Insufficient information to set up the Relay wireless network
>
> HV24-7—Verity Relay Implementation Guide missing from TDP

f. Listed discrepancies by SLI Compliance for Hart InterCivic Verity Voting version 2.4 were "repaired" by updating to Hart InterCivic Verity Voting firmware version 2.4.2.

g. All state of Texas certifications for these versions are currently approved under version 2.4.

365. SLI Compliance is not an accredited laboratory in accordance with the Voting System Test

[214] *See* Tex. Elec Code § 122.031(a)

[215] https://www.eac.gov/sites/default/files/voting_system/files/Attachment%20G%20-%20Verity%20Voting%202.4%20Discrepancy%20Report.pdf Last visited 07/22/2022

Laboratory Program Manual ver. 2.0 effective May 31, 2015, page 38, Sec 3.6.1.

366. On May 3, 2021, Hood County Attorney, Matthew Mills, sent a letter to Attorney General, Ken Paxton, requesting clarification of ballot numbering issues associated with the use of election machines in Hood County.[216] [217]

367. A letter from Roger B. Borgelt of Borgelt Law dated July 29, 2021, to the Attorney General, Ken Paxton, outlines the questions that Hood addressed in the cited letter above from Matthew Mills, May 3, 2021, concerning the ballot numbering for Hart Inter-Civic currently in use in Hood County.

a. "Secretary of State claims that TEX ELEC § 122.001 provides authority for the Secretary to prescribe "operating procedures" related to voting systems,[218] nothing in the Election Code grants the Secretary the authority to provide advice to ignore specific sections of the Election Code – laws and procedures are not equal."

b. Several times, in the letter from Borgelt Law, it is noted that inconsistent numbering violates several Texas Election Codes (TX Election Code § 52.062, § 51.006, § 51.007, § 51.008, § 51.010, § 62.007, § 62.009).

[216] https://katychristianmagazine.com/wp-content/uploads/2021/12/Request-for-Opinion-on-Ballot-Numbering_RQ-0405-KP_status-Borgelt-letter.pdf (Last visited 5/18/22)

[217] *See* Tex. Elec Code § 52.062

[218] *See* Tex. Elec Code § 31.003

> "The Secretary is the Chief Election Officer of the State of Texas.[219] Among other duties, the Secretary has been tasked by the Legislature with "obtain[ing] and maintain-[ing] uniformity in the application, operation, and interpretation of [the Election] code."[220] As part of performing this duty, the Secretary is required to "prepare detailed and comprehensive written directives and instructions relating to and based on [the Election] code and the election laws outside this code."[221] The Secretary must "distribute these materials to the appropriate state and local authorities having duties in the administration of these laws."
>
> "The Secretary's deficient guidance to counties violates the Separation of Powers clause of Art. 2, Sec. 1 of the Texas Constitution. Further, because the Secretary is providing counsel to counties to ignore Tex. Elec. Code §§ 52.062, 51.006, 51.007, and 51.008, this is a violation of the Suspension of Laws provision in Art. 1, Sec. 28 of the Texas Constitution. The Constitution provides that only the Legislature can suspend laws - not the Secretary, a member of the Executive Branch. These actions by the Secretary are contrary to the Legislature's intent that the Election Code be interpreted and applied

[219] *See* Tex. Elec Code § 31.001

[220] *See* Tex. Elec Code § 31.003

[221] *Id.*

> uniformly across this State for voting systems. *See* Tex. Elec. Code § 122.032. By suspending laws and authorizing exceptions to Tex. Elec. Code § 52.062, and other statutes, the Secretary is failing to perform his ministerial duty. Surely the Legislature did not intend for any of these provisions to be waived, ignored, or violated."

368. The SoS recommendations for ballot numbering procedures for Hart InterCivic System and correctly notes that Tex. Elec Code § 52.062 requires ballots to be prepared with

> The first option, ordering blank ballot stock with preprinted numbers, complies with § 52.062, as the ballots can be numbered consecutively beginning with " one. " this plainly satisfies both the letter and spirit of § 52.062 and thus ensures counties adherence to other election laws, such as those cited supra, that relate to ballot numbering the second option purports to provide an alternative to § 52.0624 counties using the ES&S and Hart InterCivic systems. According to the secretary, the Hart InterCivic "ballot is assigned a unique identifier when printed." however, the secretary acknowledges in appendix a that the lack of consecutively numbered ballots renders it impossible for election officials to fully comply with portions of the election code:
>
> "the ballot shall be tracked, distributed, and retained just as you would with the traditional preprinted full ballot in accordance with §§ 51.006, 51.007, 51.008 with the exception of notated serial number of the ballot ranges. " (emphasis added.)

The alternative randomize ballot numbering procedure will cause counties to violate, at a minimum, Tex. Elec. Code §§ 52.062, 51.006, 51.007, and 51.008

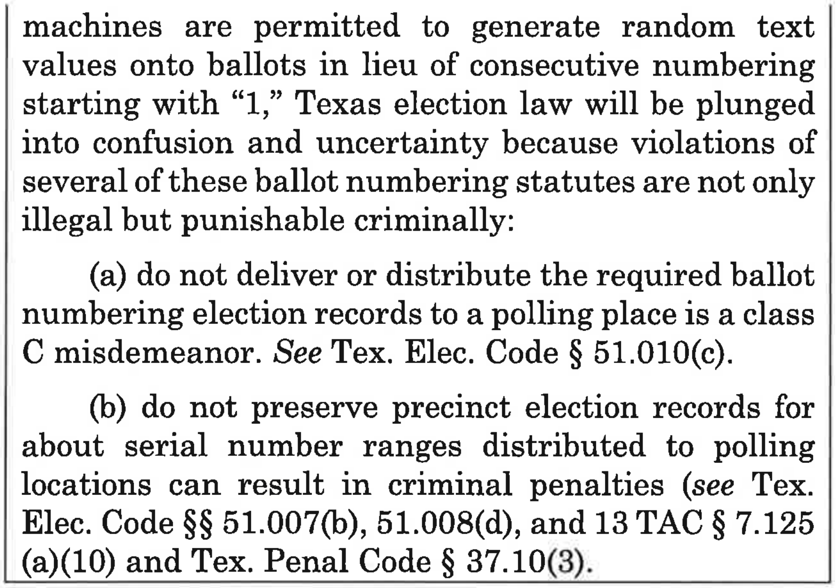
consecutive numbers to begin with "1". The two options for meeting this requirement.

369. On November 1, 2021, Virginia Hoelscher, Chair of the Opinion Committee for Attorney General Ken Paxton, sent the following letter to Matthew Mills, Hood County Attorney:

> "Re: Procedure for numbering election ballots and which officials are authorized to select the method for numbering ballots (RQ-0405-KP) Dear Mr. Mills: Thank you for requesting a written opinion from this office. Section 402.042 of the Government Code requires this office to issue an opinion within 180 days of receiving a request for one unless we explain to the requestor in writing before the deadline why the opinion will be delayed. Accordingly, we are notifying you that we will not issue an opinion on your

Does not provide sufficient instructions for how officials may comply with Tex. Elec. Code 51.010 (how will officials deliver serial number ranges according to polls), 62.007 (how will officials that pulls determine if ballots are properly numbered) and 62.009 (how election judges placed numbered ballots FaceTime for voters to choose their ballot). In short, the secretaries permission to ignore § 52.062 cause a chain reaction in which counties may violate at least six other laws.

Should Gen. Paxton determine the Tex. Elec. Code 52.062 is discretionary and that computerized



machines are permitted to generate random text values onto ballots in lieu of consecutive numbering starting with "1," Texas election law will be plunged into confusion and uncertainty because violations of several of these ballot numbering statutes are not only illegal but punishable criminally:

(a) do not deliver or distribute the required ballot numbering election records to a polling place is a class C misdemeanor. *See* Tex. Elec. Code § 51.010(c).

(b) do not preserve precinct election records for about serial number ranges distributed to polling locations can result in criminal penalties (*see* Tex. Elec. Code §§ 51.007(b), 51.008(d), and 13 TAC § 7.125 (a)(10) and Tex. Penal Code § 37.10(3).

> request within 180 days of the date received because we need more time to review the law, complete the analysis that your request requires, and finalize the formal opinion. We will make every effort to issue this opinion as soon as possible."

370. To our knowledge, non-sequential ballots have been used in all Hood County elections since the Hart InterCivic equipment was first employed in 2021.

371. By Defendants' own admission via the State of Texas' Secretary of State website regarding education of the HAVA 2002; knowingly certified voting software, systems and modification without a valid VSTL accreditation via the EAC.

PARKER COUNTY

372. Parker County Commissioners, County Judge and election officials, have failed to confirm and properly certify the voting equipment in Parker County.

373. October 6, 2021, Plaintiff Jennifer B. Edwards met with Larry Walden, Parker County Commissioner, Precinct 3, regarding the lack of accredited VSTLs and thereby the lack of state certifications for the November 3, 2020, elections in Parker County.

374. October 13, 2021, Plaintiff Jennifer B. Edwards met with Larry Walden, Parker County Commissioner, Precinct 3 and John Forrest, Parker County Attorney regarding the lack of accredited VSTLs and thereby the lack of state certifications.

375. October 20, 2021, Plaintiffs Jennifer B. Edwards and Jennifer Williams met with Larry Walden, Parker County Commissioner, Precinct 3, Crickett Miller, Parker County Elections Administrator and John Forrest, Parker County Attorney regarding the lack of VSTL's and thereby the lack of state certifications.

376. October 23, 2021, Plaintiff Jennifer B. Edwards sent letter via email to Pat Deen, Parker County Judge requesting an emergency meeting of the Parker County Election Commission be called to present findings regarding the lack of accredited VSTLs and thereby the lack of state certifications.

377. November 1, 2021, Plaintiffs, Jennifer Williams and Jennifer B. Edwards emailed Elections Administrator Crickett Miller; County Commissioners Steve Dugan, George Conley, Craig Peacock, and Larry Walden; County Attorney John Forrest; County

Judge Pat Deen; and Sheriff Russ Autheir alerting them to fact that the election machines have not been certified as is required by law. Certified letters with evidence were sent to the District Attorney Jeffrey Swain and the District Judges Craig Townson and Graham Quisenberry.

378. March 25, 2022, Plaintiffs Jennifer B. Edwards and Jennifer Williams submitted sworn affidavits to Jeffrey Swain, Parker County District Attorney in accordance with Tex. Elec. Code § 273 regarding the lack of accredited VSTLs and thereby the lack of state certifications.

379. Hart InterCivic Voting System 2.4 was utilized in Parker County for the November 3, 2020, election.

a. According to Crickett Miller, Parker County Election Administrator, Hart version 2.4 was utilized for the November 2020 general elections.

b. Certification for Hart InterCivic Verity Voting software version 2.4 is on file with the Secretary of State website.[222] (Judicial Notice: Parker County regarding 2.4)

c. Inconsistent numbering violating several Texas Elections Codes (TX Election Code § 52.062, § 51.006, § 51.007, § 51.008, § 51.010, § 62.007, § 62.009).[223]

[222] https://www.sos.state.tx.us/elections/forms/sysexam/hart-verity-2.4-certification-order.pdf (Last visited 5/25/22)

[223] *See* Parker County page 91of this case

380. SLI Compliance is the VSTL that certified Hart InterCivic voting systems and equipment.

381. SLI Compliance is not an accredited laboratory in accordance with the Voting System Test Laboratory Program Manual ver. 2.0 effective May 31, 2015, page 38, Sec 3.6.1.[224]

382. By Defendants' own admission via the State of Texas' Secretary of State website regarding education of the HAVA 2002; knowingly certified voting software, systems and modification without a valid VSTL accreditation via the EAC.

COMAL COUNTY

383. Comal County Commissioners, in addition to election officials, have failed to confirm the voting equipment in Comal County was/is properly certified.

384. Comal County removed the Elections Administrator position due to malfeasance.

385. The County Clerk is the responsible elections official. There is a Deputy under the County Clerk named the Elections Coordinator.

a. Bobbie Koepp, Comal County Clerk

b. Cynthia Jaqua, Deputy under the Clerk - Elections Coordinator

386. Comal County used KNOWiNK Poll Pads that were updated the night before the November 3, 2020, General Election.

[224] https://www.eac.gov/sites/default/files/eac_assets/1/28/VSTLManual%207%208%2015%20FINAL.pdf (Last visited 5/25/22)

387. Comal County has not provided the version of KNOWiNK poll pad software that was utilized during the November 3, 2020.

388. KNOWiNK Poll Pads version 2.4.9 was certified by the SoS on January 23, 2020.[225] What version of software were the poll pads upgraded to the night before the November 3, 2020, General Election?

389. The purchase of these pads was contracted via Hart InterCivic under contract in 2018 with software, maintenance, and upgrade options.

390. The SoS's office did not inspect the KNOW-iNK Poll Pad updated/modified changes as required by law.[226]

a. Defendants Koepp and Jaqua did not address the violation of Tex. Elec Code with the SoS's office and or make the voters aware of lack of certification.

b. Defendants Koepp and Jaqua authorized the update/modification of poll books with clear knowledge of Tex. Elec Code.

391. KNOWiNK performed an update the night before the election of November 3, 2020, similar to how an iPhone updates via a network connection.[227]

[225] https://www.sos.texas.gov/elections/forms/sysexam/knowink-poll-pad-certification-letter.pdf Last visited 06/10/22

[226] *See* Tex. Elec Code 31.014

[227] https://www.ksat.com/news/local/2020/11/03/polling-pads-down-at-comal-county-voting-locations/ Last visited 06/10/22

392. Election officials throughout the country-from North Texas to Georgia-reported issues with poll pads from St. Louis-based KNOWiNK.

393. In some locations; the poll pads also activated ballots on voting machines which forced some voters to fill out selections on paper ballots.

394. The Defendants proceeded to utilize the paper forms and provided pencils.[228]

395. KNOWiNK poll pads went down November 3, 2020, across the state affecting Comal County elections.

a. Marcia Ridley, Spalding County Board of Elections, attributed the problem to a vendor's 11th hour update per a representative for the election technology vendor, dominion Voting Systems, told her office that it had uploaded some kind of "***update***" the night before the election and that this had created the glitch.[229] (*emphasis added*)

396. As a result, "three reports of races not being included on a ballot,":[230]

[228] https://www.ksat.com/news/local/2020/11/03/polling-pads-down-at-comal-county-voting-locations/ Last visited 06/10/22

[229] https://www.politico.com/news/2020/11/04/georgia-election-machine-glitch-434065 Last visited 06/10/22

[230] https://www.kens5.com/article/news/community/hill-country-reporter/comal-county-investigates-scope-of-election-day-tech-issues/273-603cef42-e93a-483b-aa4d-60edde2db052 Last visited 06/10/22

a. Contests seats on the New Braunfels ISD Board of Trustees

b. District 2 (Nancy York claiming victory over incumbent Michael Calta by 12 votes)

c. District 4 (John Tucker claiming victory over incumbent Matthew Sargent by 251 votes)

d. Lake Dunlap Proposition not being on the appropriate ballot.

397. Impacted precincts due to failure of poll pads include 301, 302, 303 and 201.

398. This resulted in County Judge to extend voting hours due to poll pad failures.

399. Defendant Bobby Koepp's statement to Kens5 in which she offers only a partial responsibility, "It's part of my duties to make sure that everybody gets what they're supposed to get when they come to vote, and I do take responsibility for that"; in which the Defendant continues placing blame at KNOWiNK. "But in my defense, I honestly feel [KnowInk] needs to make it right. They need to make a statement and need to tell everybody what happened."

400. Defendant Bobby Koepp believes it is up to the candidates to request a do-over. "We are doing everything in our power to . . . try to figure out exactly how many votes were cast that didn't get the opportunity to vote the way they needed to."

401. The day prior Defendant Bobby Koepp stated to one candidate, Sargent, that reported his name and race not on the ballot but submitted in error; "If this had been brought to our attention before the vote was

submitted, we could have canceled out the vote and reviewed the problem . . . "[231]

402. Sargent is left wondering and . . . "waiting for the county to step up and say there is a problem or to let us know what they are going to do to fix it. . . . . Or to make us feel all warm and fuzzy that every vote got counted."[232]

403. Sargent's complaint to the SoS Office states . . . potential violation from the handbook for Election Judges and Clerks 2020, which in part requires presiding election judges to cease using malfunctioning equipment installed at polling places "immediately after discovering that the equipment is not functioning properly."[233]

404. Sargent's continues, "The county knew about the problem no later than 10:41 am and continued to utilize the equipment without shutting the polling places(s). Even though this was a software issue, and the ballots were not loading correctly the machines were not properly functioning. The equipment should have been shut down until the software issue could have been corrected."

[231] https://www.kens5.com/article/news/politics/elections/election-day-glitches-led-to-reports-of-absence-of-races-and-propositions-on-some-ballots-comal-co-says/273-308a3fae-49a9-41e4-a4bf-711266c28310 Last visited 06/10/22

[232] https://www.kens5.com/article/news/politics/elections/election-day-glitches-led-to-reports-of-absence-of-races-and-propositions-on-some-ballots-comal-co-says/273-308a3fae-49a9-41e4-a4bf-711266c28310 Last visited 06/10/22

[233] https://herald-zeitung.com/community_alert/article_862bdcaa-2483-11eb-9728-fb0da9e3734c.html Last visited 06/10/22

405. Defendants Koepp and Jaqua authorized and continued to use Hart InterCivic voting systems and equipment after many reported malfunctions including but not limited to lack of paper ballot and ballot numbering.

406. After multiple PIA requests, Comal County did not provide the Letter of Approval from the SoS to Comal County approving the contract for the purchase of Hart Verity Voting 2.4. as pursuant to Tex. Elec Code.[234] Making the election null and void if the document does not exist.

407. By Defendants' own admission via the State of Texas' Secretary of State website regarding education of the HAVA 2002; knowingly certified voting software, systems and modification without a valid VSTL accreditation via the EAC.

TARRANT COUNTY

408. Tarrant County Commissioners, in addition to election officials, have failed to confirm and properly certify the voting equipment in Tarrant County.

409. Hart InterCivic Verity Voting 2.3, 2.4 and 2.5 contain numerous COTS components,[235] and that all three versions lack proper EAC certifications according to HAVA 2002.

410. Halderman's statement with regard to close proximity of the voting system to the internet rings true. There are several components of the election

[234] *See* Tex. Elec Code § 123.035 (a), (b), (c), (d).

[235] https://www.eac.gov/voting-equipment/registered-manufacturers/hart-intercivic-inc (Last visited 5/23/22)

infrastructure ecosystem utilized by Tarrant County for all three elections that give cause for concern.

a. November 3, 2020, election contained one or more of these aspects/components but not limited to:

411. Verity Touch Writer DUO are daisy chain configurations comprised of a Verity controller device and up to twelve Ballot Marking Devices[236] (BMDs). The Implications of the utilization of these types of election systems will be addressed in a following section.

412. Verity Scan equipped with a Relay Kit[237] enables direct transmission of cast vote records from Verity Scan (precinct ballot counter or tabulator) via a preferred telecommunications carrier, to a central election office.

413. Per the contract obtained between Tarrant County and Hart InterCivic 9 Relay Kits (COTs modems) were acquired[238]

[236] https://www.stat.berkeley.edu/~stark/Preprints/bmd-p19.pdf (Last visited 5/23/22)

[237] https://www.michigan.gov/documents/sos/071B7700128_Hart_Exhibit_2_to_Sch_A_Tec_Req_556894_7.pdf

[238] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendices C & E

414. Hart InterCivic,[239] as well as Dominion Voting Systems, and ES&S, have disclosed[240] that some tabulators have wireless modem capabilities, offered as an add-on to base model kits. Add-on modem kits (e.g., Relay Kits) not only put elections at heightened vulnerability,[241] but also decertify[242] EAC certification[243] of the system, according to Kevin Skoglund, Senior Technology Advisor at the National Election Defense Coalition.

415. The Master Agreement between Tarrant County and Hart InterCivic was signed on August 13, 2019. However, the Relay Kits do not appear as a component included within the 2.3 version of Verity

[239] https://www.eac.gov/sites/default/files/voting_system/files/Attachment_G_-__As_Run_Hart_Verity_Voting_2.2.2_EAC_Modification_Test_Plan_v1.21.pdf *See* page 15, 20 (Last visited 5/23/22)

[240] https://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436 (Last visited 5/23/22)

[241] https://www.vice.com/en/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials (Last visited 5/23/22)

[242] https://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436 (Last visited 5/23/22)

[243] https://www.documentcloud.org/documents/6602861-EAC-ESS-Letter-01-07-20.html (Last visited 5/23/22)

Voting per the EAC Certificate for Conformance,[244] nor is it mentioned in the Memorandum[245] of the SoS.

416. Relay Kits are listed as components of Verity Voting 2.2.2,[246] and as an option for Verity 2.4. Moreover, the application acceptance[247] date for version 2.4 (including the Relay kit) is after the contract for 2.3 was signed, on August 15, 2019, by Tarrant County[248].

417. The EAC later issued certification of Verity Voting 2.4 (despite the lack of examination by an accredited VSTL) on February 21, 2020[249]

418. The Relay Kit is never mentioned in the TX SoS Memorandum of certification, and yet somehow Tarrant County purchased 9 Relay Kits (modems) outside of the scope of 2.3 that also had not even begun the EAC certification process.[250]

[244] https://www.eac.gov/sites/default/files/voting_system/files/Cert_of_Conformace_and_Scope_Verity_Voting_2.3_3.15.193.pdf Last visited 06/13/22

[245] https://www.sos.state.tx.us/elections/forms/sysexam/Chuck-Pinney-Voting2.3.pdf Last visited 06/13/22

[246] https://www.eac.gov/sites/default/files/voting_system/files/Cert._of_Conformace_and_Scope_Verity_Voting_2.2.2_5.22.18.pdf Last visited 06/13/22

[247] https://www.eac.gov/voting-equipment/verity-voting-24 Last visited 06/13/22

[248] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendix C

[249] https://www.eac.gov/voting-equipment/verity-voting-24 Last visited 06/13/22

[250] https://files.ttttexas.com/case/TX_SOS_Election_Violation_

419. Brandon Hurley, an SoS appointed examiner, cited the connectivity capabilities of this make and version of voting system in his examination report. He reported that Hart InterCivic representatives stated this capability was only available in the state of Michigan.[251]

a. He did not identify the component(s) that would allow internet connectivity, nor evidence that the systems sold to Texas counties were absent of this capability.

b. He also expressed concerns regarding this system adhering to the ballot numbering requirements of Texas, as well as issues with paper jams in the scanner.

420. Brian Mechler's, Technical Examiner Report, noted paper feed issues that resulted in spoiled ballots. He also concluded his report with, "In order to fully comply with the EAC Voluntary Voting System Guidelines (VVSG) Vol 1.0, Hart needs to ensure that their documentation recommends hash verification software that uses a FIPS 140-2 level or higher validated cryptographic module."[252]

421. Lesley French, General Counsel for the office of the Texas Attorney General, stated in a letter to Keith Ingram, Director of Elections, Texas SOS, that "Both during and after the examination, the examiners

References *See* Appendix C

[251] https://www.sos.texas.gov/elections/forms/sysexam/brandon-hurley-hart-2.4.pdf *See* page 2 Last visited 06/13/22

[252] https://www.sos.texas.gov/elections/forms/sysexam/brian-mechler-hart-2.4.pdf *See* page 9 Last visited 06/13/22

raised specific concerns about the legal compliance of Verity 2.4." No further information in which these concerns were addressed to warrant the recommendation of certification was given.[253]

422. James Sneering, a Designee of the Attorney General, noted the presence of "some security risk in the polling places due to passcodes are the same throughout an election across all precincts for all voting stations and other precinct devices."[254]

423. The Relay Kit is never mentioned in the TX SoS Memorandum of certification Tarrant County purchased 9 components outside of the scope of 2.4 that also had not even begun the EAC certification process.[255]

424. As is demonstrated by the Election Judge and Clerk educational materials from Tarrant County's Elections website, the epollbooks are connected to a Mifi.[256]

425. 260 Epson Mobilink[257] P80 Plus 3" Wireless Receipt Printers with auto cutters, with blue tooth

[253] https://www.sos.texas.gov/elections/forms/sysexam/lesley-french-hart-2.4.pdf Last visited 06/13/22

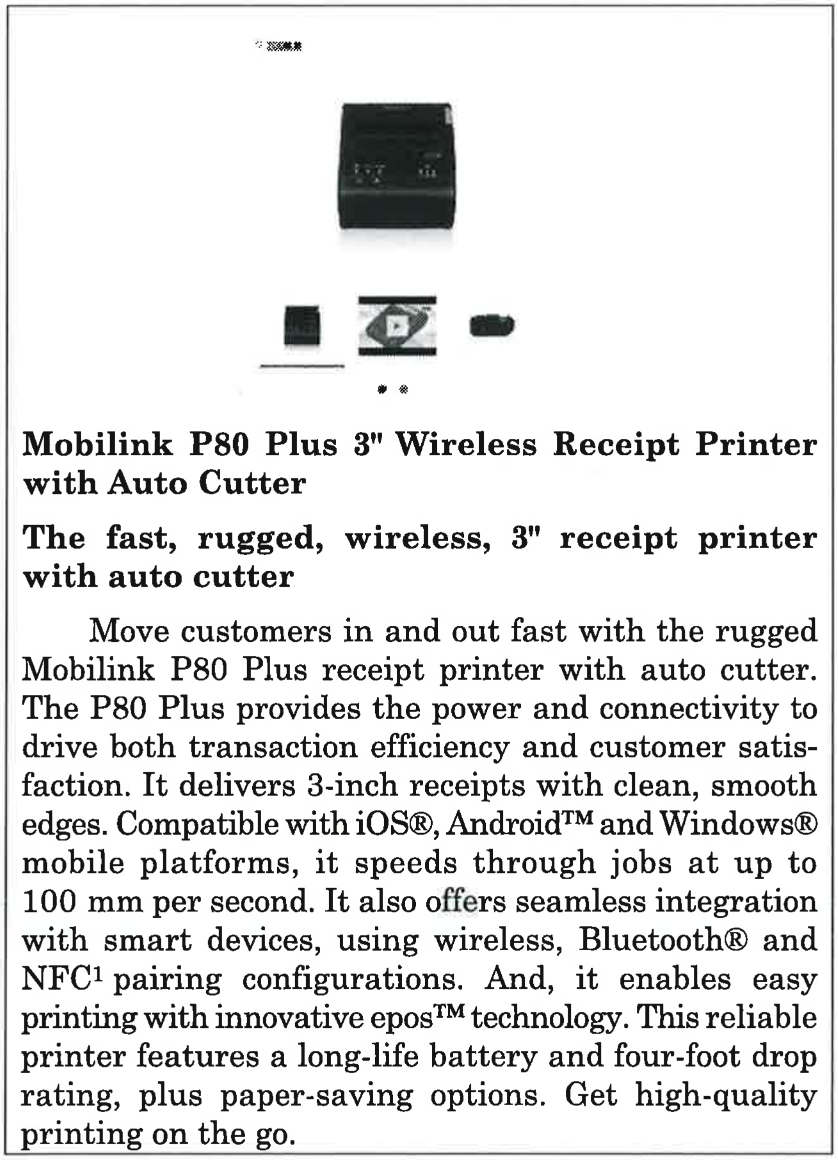
[254] https://www.sos.texas.gov/elections/forms/sysexam/jim-sneeringer-hart-2.4.pdf *See* page 2 Lasted visited 06/13/22

[255] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendix C

[256] https://access.tarrantcounty.com/content/dam/main/elections/Poll_Worker/TC_Election%20_Handbook.pdf *See* page 30

[257] https://epson.com/For-Work/Printers/POS/Mobilink-P80-Plus-3%22-Wireless-Receipt-Printer-with-Auto-Cutter/p/

capability along with 16 hours of pairing services were purchased in January of 2020 by Tarrant County.



Mobilink P80 Plus 3" Wireless Receipt Printer with Auto Cutter

The fast, rugged, wireless, 3" receipt printer with auto cutter

Move customers in and out fast with the rugged Mobilink P80 Plus receipt printer with auto cutter. The P80 Plus provides the power and connectivity to drive both transaction efficiency and customer satisfaction. It delivers 3-inch receipts with clean, smooth edges. Compatible with iOS®, Android™ and Windows® mobile platforms, it speeds through jobs at up to 100 mm per second. It also offers seamless integration with smart devices, using wireless, Bluetooth® and NFC[1] pairing configurations. And, it enables easy printing with innovative epos™ technology. This reliable printer features a long-life battery and four-foot drop rating, plus paper-saving options. Get high-quality printing on the go.

C31CD70751 Last visited 06/13/22

426. In a response[258] to a news story, identifying Hart Verity Voting systems as "highly vulnerable," the company stated, "As part of the EAC certification, systems go through the "trusted build process" performed by accredited Voting System Testing Laboratories (VSTLs)." Ironically, Hart Intercivic went onto say, "Hart's Verity Voting system has passed multiple federal and many state certifications and has never failed." Without the establishment of proper certification, one could argue quite the opposite.

427. Communications between Pat Geppert,[259] with Hart InterCivic, Jerome Lovato, Director of Voting System Testing and Certification of the EAC, and Jonathon Panek, SLI Compliance, during the application for certification for Hart Verity Voting 2.4 system, indicate that Hart InterCivic selected SLI Compliance as the lead VSTL for testing.

a. Jerome Lovato, clearly defined the process of certification by stating "testing will be conducted to the VVSG 1.0. If the system meets the criteria for a grant of certification, the system will be assigned number "HRT-Verity-2.4" per your request on the application form."

428. In several instances in which Tarrant County Elections Administrator, Heider Garcia, indicated that he possesses extensive experience with imple-

[258] www.hartintercivic.com/hartstatement-securityreporting/ Last visited 06/13/22

[259] https://www.eac.gov/sites/default/files/voting_system/files/ HRT-Verity-2.4_Application_Approval_Letter.pdf Last visited 06/13/22

menting systems compliant to VVSG. One such example is: Garcia was a speaker in the webinar[260]"What City and County Officials Need to Know About Modernizing and Securing Campaign Finance".

429. Garcia' s introduction, it is said, "In 2009, he was selected as the Election Systems Manager for the Project Team that ran the 2010 Automated Elections in the Philippines. In a country of over 50 million registered voters, Heider was responsible for customizing the technology, certifying the solution under VVSG standards in the United States, and ensuring 100% compliance with the local legislation."

430. Two companies in particular that produce COTS are Huawei and Akamai, the latter of which is partnered with SCYTL and linked to Dominion Software.

431. A very similar contractual relationship is noted per Tarrant County's contracts between SOE D/B/A Scytl (a foreign headquartered company located in Spain) and Hart InterCivic.[261]

432. Emails, certified mail, as well as affidavits attesting to the aforementioned were sent to officials.[262]

433. The extent of examinations, certifications, regulations, and oversight of the exact manner of how

[260] https://webinars.govtech.com/What-City-and-County-Officials-Need-to-Know-About-Modernizing-and-Securing-Campaign-Finance-127158.html (Last visited 5/23/22)

[261] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendix E

[262] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendix G

Tarrant County's election infrastructure ecosystem functions as a whole, in real-time (e.g., ePollbooks, election night reporting, aggregation, databases and servers) lacks transparency.

434. As for 2020, and the primaries of 2022, significant irregularities occurred throughout the entire process in Tarrant County.[263]

435. Tarrant County contracted with SOE D/B/A SCYTL for such ENR purposes described previously in Terpsehore Maras' Affidavit.

436. Tarrant County's election system, combined with the aforementioned published opinions/presentations of numerous experts, and the irregularities observed in previous elections bring the Affidavit of Terpsehore Maras into the forefront; specifically, yet not limited to, lines: 9-12, 33-34, 50, 89, 112-118.

437. Vulnerabilities do not end with Tarrant County's ENR contracts, but rather extend across the entire election ecosystem (e.g., Hart InterCivic, ePollbook contracts, servers, and databases) and into the security and autonomy of private/personal information.[264]

438. Tarrant County has entered its citizens contractually into abominable circumstances extending beyond elections:

[263] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendices B & E

[264] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendix E

a. ENR services through a company with foreign ties[265]

b. ePollbook and pairing services that allows those with malicious intent to make significant changes to the voting process[266]

c. provides vendors access to, the collection of, and the transfer (over the air) of private sensitive data[267]

d. the "hosting" of sensitive data on servers belonging to/rented by vendors[268]

e. grants and/or contracts that entrust personal information to corporations historically vulnerable to cyberattacks[269]

f. the exposure of the election process to the influence of big tech and corporations[270]

g. contracts with stipulations that violate the ability of citizens to request information

[265] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendices D & E

[266] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendix E

[267] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendix E

[268] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendix E

[269] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendices A & E

[270] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendix E

regarding virtually any aspect of voting equipment their taxes funded[271]

h. contracts giving vendors complete control over updating, upgrading, maintaining and enhancing security[272]

439. On September 23, 2021, the TX SoS announced that a forensic audit would occur in Tarrant County along with four other counties.

440. Many have pointed to hybrid voting systems (i.e. BMDs) as a means to provide a paper trail should the need for an audit arise.

441. A legitimate forensic audit, in the sense that we see in other industries (e.g, financial), is impossible within the current electronic voting/elections industry.

442. The reasoning revolves around two key foundational requirements of elections:

a. the protection of privacy (of voters, ballots, and proprietary information)

b. protection of voters' intentions.

443. The realm of an electronic system, the ability to ensure and provide proof of protections from manipulation, as well as evidence of votes being casted as intended, would require some breach of privacy with regard to a voter, ballot, and/or proprietary protections.

[271] https://files.ttttexas.com/case/TX_SOS_Election_Violation_ References *See* Appendix G

[272] https: //files.ttttexas.com/case/TX_SOS_Election_Violation_ References *See* Appendix E

444. In effect, without sacrificing privacy for increased transparency, it is impossible to ever have the security our elections require.

445. Many states performed audits are essentially "self-audits," where the county and the SoS are essentially auditing themselves utilizing the same equipment, and the same methods, which brought about the need for an audit, absent the conditions present in a real-time election (e.g., voting day epollbook activity and transmission of election results).

446. Findings of experts that studied the Swiss Post/Scytl system[273] further increases doubt that the results of any audit would be transparent, reliable, or accurate.

447. Tex. Elec. Code § 43.007(j) authorizes the implementation of Community Voting Centers[274], substantially enhancing the risk of security breaches and vote manipulation by increasing the need for technology with internet connectivity: all for the sake of perceived convenience.

448. Community Voting Centers require wide-spread use of epollbooks and internet connectivity.

449. They also further complicate the ability to audit elections due to the significant strain added to the maintenance of chain of custody protocols (secondary to the injection of county-wide ballots and the shuffling of voters across precincts).

[273] https://link.springer.com/chapter/10.1007%2F978-3-030-30625-0_6 Last visited 06/13/22

[274] https://www.tarrantcounty.com/en/elections/Election-CAC/VC-FAQ-QA.html Last visited 06/13/22

450. Given the described environment, summoning one's ballot would be nearly impossible considering the chain of custody breaks which were evident in Tarrant County[275].

451. Locating an individual's ballot and determining the manner in which it was cast and counted is further complicated by the laws designed to protect proprietary information. This gives rise to further possible violations with regard to the ballot numbering[276] protocols currently in place.

452. TX SoS's audit as a potential waste of time, effort, and taxpayer funds; as it appears that investigation of proper EAC certification and many other irregularities are not within the scope of the SoS' audit.

453. The audit in Tarrant County, approximately 1/3 (estimated to be up to 33,000 ballots) of Tarrant County's mail in ballots for the November 3, 2020, election, purchased from Runbeck,[277] were not scannable.

454. Adjudication on this large of scale, affected thousands of votes; and brings other Texas Election Code violations into view.

[275] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Appendix F

[276] https://blackboxvoting.org/the-case-of-dr-laura-pressley/#fn-3370-2 Last visited 06/13/22

[277] https://www.survivethenews.com/maricopa-county-relegated-election-processes-to-a-printer-who-didnt-provide-accurate-counts-of-ballots-received-by-election-day-nor-chain-of-custody-details/ Last visited 06/13/22

455. The exact manner, and who personally adjudicated thousands of mail in ballots over the course of several days lacked transparency, and warranted immediate investigation following the November 3, 2020 election.

456. This occurrence was not mentioned by Heider Garcia, Tarrant County Elections Administrator, in his response to the SoS, found within the Phase 1 audit report[278]

457. He did disclose Tarrant County Elections Administration is currently engaged in litigation and his access to equipment is limited.

458. Given the administration's restricted access to evidence requested by the SoS, the absence of an investigation into proper EAC certifications, and the many points of vulnerabilities across all aspects of the Tarrant County election ecosystem it is apparent that this audit lacks integrity.

459. An audit that lacks transparency, as well as thoroughness, will render invalid and incomplete results, leaving citizens with little faith in the outcome, and less confidence in the validity of future election results.

460. By Defendants' own admission via the State of Texas' Secretary of State website regarding education of the HAVA 2002; knowingly certified voting software, systems and modification without a valid VSTL accreditation via the EAC.

[278] https://www.sos.state.tx.us/elections/forms/phase1-progress-report.pdf Last visited 06/13/22

BEXAR COUNTY

461. Bexar County Commissioners, in addition to election officials, have failed to confirm the voting equipment in Bexar County are properly certified.

462. Beginning on October 18, 2021, Plaintiff Amanda Eubanks requested multiple responses through the Bexar County PIA portal the information regarding the version of ES&S software used in the 2020 election. Defendant Jacquelyn Callanen responded to one PIA request by referring the plaintiff to the Secretary of State's website for current information. As of June 5, 2022, multiple PIA requests remain unanswered beyond the required 10 business day response window.

463. ES&S was selected as the voting system to be employed within Bexar County.

a. A new ES&S contract was signed for elections in Bexar County in 2019 and continued to be used through the November 2020 election.

b. According to Jacquelyn Callanen and her direction to the Texas SOS website, ES&S version 6.0.2.0 was utilized for the November 2020 elections.

c. The last certification on file indicates that ES&S version 6.0.2.0 was certified in October of 2018.

d. Certification for ES&S Voting software version 6.0.2.0 is on file with the Secretary of State website.[279]

[279] https://www.sos.state.tx.us/elections/forms/sysexam/voting-

e. Bexar County records indicate that ES&S software version 6.0.2.0 was utilized for the November 2, 2021 as well as the May 7, 2022 joint amendment elections.

f. Another note in the ES&S Certification Test Report Modification document states that EVS version 6.0.2.0 is actually ES&S EVS 6.0.0.0 with modifications in software. The original version is not decertified for use in Texas.

g. ES&S made a modification of their system that caused hash tag validations to fail. In October 2020, this technical issue was deemed an administrative error and ruled a de minimus change, therefore neither certification nor testing were required. The EAC sent a memo to all 50 states and explained the hash tag discrepancy during an update when using a USB thumb drive.

    i. The build did not match the "CERTIFIED" version because a file named SYSLOAD.BMP (image file) was not part of the update so the old SYSLOAD.BMP remained on the system causing the hash tag discrepancy. (Emphasis added)

    ii. The issue with a bitmap file is that it should not be considered "minor in nature and effect"; a bitmap file has been known to contain malware.[280]

sys-bycounty.pdf (Last visited 6/5/2022)

[280] https://www.zdnet.com/article/obliquerat-trojan-now-hides-

iii. Brian Mechler, SOS examiner, stated in September 2020 voting system examination report, "It was disclosed during the concurrent EVS 6.0.3.0 exam that ES&S personnel have performed the hash verification process instead of their customers. Jurisdiction should always perform this process themselves. To have the vendor perform a required component of acceptance testing creates, at best, a conflict of interest."[281]

iv. This method of introducing or keeping malware on a voting system lends support to researchers[282] and a witness explaining how code containing an algorithm can impact elections. We do not have assurance that the SYSLOAD.BMP file was not updated.

v. The Secretary of State (Ruth R. Hughs) authorized the continued use of this system with alleged malware. Respondents acquiesce in the matter and neglected enforcement of the "law of the land".

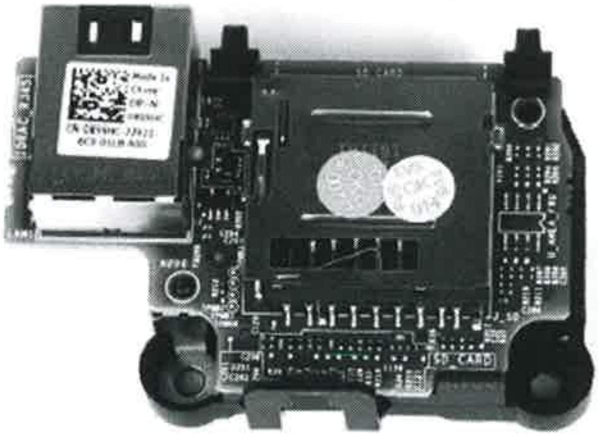
464. On May 21, 2019, Bexar County executed an ES&S voting equipment and system contract that listed the Dell Poweredge T430 with a "iDRAC8"

in-images-on-compromised-websites/

[281] https://www.sos.state.tx.us/elections/forms/sysexam/brian-mechler-ESS-exam-report-EVS6110-aug.pdf

[282] https://www.digitalegesellschaft.ch/uploads/2019/03/UniversalVerifiabilitySwissPost.pdf

component which is listed in the Election Night Reporting Network (ENR).[283]



a. Dell touts the (iDRAC) as an integrated Dell Remote Access Controller. "iDRAC . . . . is part of a larger datacenter solution that helps keep business critical applications and workloads available at all times . . . allows administrators to deploy, monitor, manage, configure, update, troubleshoot and remediate Dell servers from any location, and without the use of agents."

b. "Leveraging the incomparable agent-free capabilities of the embedded, integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller technology, server deployment, configuration and updates are streamlined across the OpenManage portfolio and

[283] Need web address *See* page 23

through integration with third-party management solutions."[284]

c. "Remote management: iDRAC8 with Lifecycle Controller, iDRAC8 Express (default), iDRAC8 Enterprise (upgrade), 8GB vFlash media (upgrade), 16GB vFlash media (upgrade)"

d. The iDRAC8 modem creates a serious security breach and violates a multitude of election and penal codes.[285]

e. Defendant Keith Ingram signed a letter of authorization for purchase on April 18, 2019 which included the iDRAC8 remote access controller.[286] [287]

f. This is a supply chain security issue according to the Declaration of Shawn Smith and Terpsehore Maras and Bexar County's voting system/machine is vulnerable.[288]

[284] https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/aa/Dell-PowerEdge-T430-Spec-Sheet.pdf Last visited 06/23/22

[285] *See* Tex. Elec Code 122.001(a)(4), TEX. PEN. CODE § 16.02, § 33.05, 18 U.S.C. § 1030

[286] Need web page for Bexar contract *See* page 27

[287] *See* Tex. Elec Code 122.031(a), Tex. Elec Code 122.001(a)(4), Tex. Elec Code 123.035 (a), (1)

[288] https://files.ttttexas.com/case/TX_SOS_Election_Violation_ References *See* Declaration of Shawn Smith, Election Software Whistleblower, Tex. Elec Code 122.005(a)

465. SLI Compliance is not an accredited laboratory in accordance with the Voting System Test Laboratory Program Manual ver. 2.0 effective May 31, 2015, page 38, Sec 3.6.1.

466. The election department order for adopting a voting system to be used in elections since 2019 in Bexar County have reflected that, for each election excluding the primary and general election in 2020 and the primary and runoff elections in 2022, Bexar County has used EVS 6.0.2.0. Jacquelyn Callanen's direction to the Texas SOS website seems to conflict with the available information in Bexar County Commissioners Court documents which do not specify an approved EVS for use in the 2020 and 2022 elections.

467. By Defendants' own admission via the State of Texas' Secretary of State website regarding education of the HAVA 2002 they knowingly certified voting software, systems and modification without a valid VSTL accreditation via the EAC.

Bexar County Voting Signed Certifications

{ Images too small for reproduction }

TRAVIS COUNTY

468. Travis County Commissioners, in addition to election officials, have failed to confirm the voting equipment in Travis County are properly certified.

469. On May 12, 2020, Modification No. 3 was approved in the Travis County Commissioners Court

for the purchase of services for the version 6.1.0.0 election management system upgrade[289].

470. 6.1.1.0 was only "certified" by the Election Assistance Commission (EAC) on July 27, 2020 by Pro V&V which did so with an expired EAC VSTL accreditation and was not certified to do the examination at the time[290].

471. On August 21, 2020, Election Systems & Software ("ES&S" or the "Vendor") presented the EVS 6.1.1.0 system for examination and certification by the Texas Secretary of State[291].

472. Travis county officials have confirmed that Election Systems & Software's EVS 6.1.1.0 system was used to conduct the November 3, 2020, elections[292].

473. On December 9, 2020, pursuant to TEX ELEC § 122.0371 of the Texas Election Code, the Office held a public hearing, by telephone, for interested persons to express views for or against the certification of the EVS 6.1.1.0 system[293].

[289] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* MODIFICATION OF CONTRACT: 4400003924, Voting System and Services

[290] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* ES&S EVS 6.1.1.0. Certificate and Scope of Conformance

[291] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* EVS 6.1.1.0 system examination and certification

[292] https://files.ttttexas.com/case/TX_SOS_Election_Violation_References *See* Travis County FOIA/ PIA Request and Response

[293] https://files.ttttexas.com/case/TX_SOS_Election_Violation_

474. On January 8, 2021, The Secretary of State's office pursuant to Section 122.039 wrote and filed their official report certifying Election Systems & Software's EVS 6.1.1.0 system for use in Texas elections.

475. EVS 6.1.1.0 was NOT CERTIFIED for use in any election prior to the state certification on January 8, 2021. (*Emphasis added*)

476. Defendants did not seek as stated per TX statutes temporary restraining order, or a writ of injunction obtained through the attorney general to prevent the use of any part of a voting system or voting system equipment that had not been approved per TX ELEC § 122.031(b). Thereby, committing an offense by providing a voting system or voting system equipment that the Defendants knew has not been approved. An offense under this subsection is a Class A misdemeanor. TX ELEC § 122.031(c)

477. By Defendants' own admission via the State of Texas' Secretary of State website regarding education of the HAVA 2002; knowingly certified voting software, systems and modification without a valid VSTL accreditation via the EAC.

HAYS COUNTY

478. Hays County Commissioners, in addition to election officials, have failed to confirm if the voting equipment in Hays County is properly certified.

479. Cliff Ormiston, Technology Coordinator confirmed via email that Hays County used Hart

References *See* ESS EVS 6.1.1.0. Certification Order

InterCivic Verity Duo version 2.4 for the November 3, 2020, election.

480. On July 10, 2020, Peter Lichtenheld Senior VP of Customer Success contacted the SoS's to inform the states that Hart was working with the below counties to upgrade them from their current Verity voting system version to the latest Texas certified version of 2.4.

Hart InterCivic

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

July 10, 2020

Dear Christina,

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

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

{ dense illegible data table omitted }

481. Hart InterCivic with non-subsequent ballot numbers violated several Texas Election code.[294]

482. SLI Compliance was the VSTL that certified Hart InterCivic Verity 2.4[295]

483. SLI Compliance is not an accredited laboratory in accordance with the Voting System Test Laboratory Program Manual ver. 2.0 effective May 31, 2015, page 38, Sec 3.6.1.

484. The Election Code specifically assigns the SoS duties[296] to ensure uniform compliance but does NOT provide the SoS with "discretion" to advise any jurisdictions to ignore or refuse to comply with the Election Code.[297]

485. The SoS Defendants and County Officials disregard for Tex. Elec Code in their guidance to jurisdictions violates the Separation of Powers clause of Art. 2 Sec. 1 of the Texas Constitution.

486. The Texas Constitution provides that only the Legislature can suspend laws – not the SoS whom is a member of the Executive Branch.

[294] *See* Tex. Elec Code § 52.062, § 52.006, § 51.007, § 51.008, § 51.10, § 62.007 and § 62.009

[295] https://www.eac.gov/sites/default/files/voting_system/files/HRT-VERITY-2.4%20Certificate%20and%20Scope%2002-21-2020.pdf

[296] *See* Elec. Code § 31.003

[297] *See* Elec. Code § 52.062, § 51.010(c), § 51.007(b), 51.008 (d)

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

a. under false pretense[298]

b. prevent a cast of a legal vote in which Plaintiff(s) are eligible to vote.[299]

c. Cause the ballot not to reflect the intent of the Plaintiff(s)/voter[300]

d. Defendants committed the offense while acting in the capacity of an elected official.[301]

MONTGOMERY COUNTY

488. July 27, 2004, the SoS's office certified Hart eSlate Voting System Version 3.3. for use in Texas elections without the required EAC certification.[302]

489. On or around November 2005, Montgomery County purchased Hart eSlate Voting System Version 3.3.

490. Hart eSlate Voting System Version 3.3 was "decertified" for use in the State of Texas by the Secretary of State's office on October 1, 2007.

[298] *See* Tex. Elec Code 2736.013(1)

[299] *See* Tex. Elec Code 2736.013(2)

[300] *See* Tex. Elec Code 2763.013(6)

[301] *See* Tex. Elec Code 2736.013(b)(1)

[302] https://www.sos.state.tx.us/elections/forms/sysexam/hart.pdf

491. On July 15, 2009, Montgomery County purchased Hart eSlate Voting System Version 6.2.1.

492. April 30, 2009, the SoS's office certified Hart eSlate Voting System Version 6.2.1. for use in Texas elections without the required EAC certification.[303]

493. There is no indication as to when the Hart InterCivic 6.2.1 equipment was placed into service for county, state and federal elections in Montgomery County.

494. This indicates an approximate 2-year gap (from 2007, when Version 3.3 was decertified, until 2009, when Version 6.2.1 was purchased) in which Montgomery County used an election system that did not even have certification from the SoS's office, much less meet the legal requirements of the State of Texas or HAVA 2002.[304]

495. Montgomery County's and the SoS's illegal negligence impacted local, state, and federal elections held on November 6, 2007, March 4, 2008, April 8, 2008, May 10, 2008, June 21, 2008, November 4, 2008, and May 9, 2009.

496. Depending on when the new equipment was placed into service, the elections of November 3, 2009, March 2, 2010, April 13, 2010, May 8, 2010, June 26, 2010, and November 2, 2010, may also have been affected.

[303] https://www.sos.state.tx.us/elections/forms/sysexam/hart621cert.pdf Last visited 06/23/22

[304] *See* Tex. Adm Code § § 81.60, 81.61, Tex. Elec Code § 122

497. This system was not certified by an EAC accredited VSTL nor did it comply with the requirements of the Voting System Standards.[305]

498. During the SoS's examination dated March 7, 2008, for Hart eSlate Voting System Version 6.2.1. Paul Miles, a staff attorney, and examiner; notated the following issues.[306]

a. "On January 17 and 18, 2008, Hart Intercivic presented modifications . . . The submitted versions of the voting system had undergone review at an independent testing authority ("ITA") and a copy of the ITA reports along with the NASED certification numbers were included with the application to the Secretary of State."

b. "Under current examination standards, all changes to a voting system required review both at the federal level, now through the Elections Assistance Commission (EAC) and at the state level by the Secretary of State."

c. Tally 4.3.10 " . . . . technical examiners were able to exit Tally and enter access the operating system while Tally running. "

499. The Hart eSlate Voting System Version 6.2.1 was never examined/tested by an EAC accredited VSTL and did not receive the certification required by

[305] *See* Tex. Adm Code § § 81.60, 81.61, Tex. Elec Code § 122

[306] https://www.sos.texas.gov/elections/forms/sysexam/paulmiles.pdf Last visited 06/23/22

Texas in compliance with HAVA 2002 as noted by an attorney as a SoS examiner Paul Mills.[307]

500. SoS's certification letter of the Hart eSlate Voting System Version 6.2.1 identified 2 security concerns in the system.[308]

a. Examiners discovered that if existing security protocols are not followed, then it is theoretically possible to access the operating system and run or delete other programs while Tally is tabulating results.

b. Examiners expressed concern that Version 6.2.1 does not have a secure OS configuration.

501. The certification letter from the SoS's office states ". . . certification of Hart InterCivic Voting System 6.2.1, is conditioned on a political subdivision employing the following procedures:

502. Based on these security concerns the SoS's office *conditioned "certification"* of the Hart eSlate Voting System Version 6.2.1 *on the following procedures being employed* by each county (political subdivision) using this system:[309] (*Emphasis added*)

a. "Two-person access for all Version 6.2.1 computers and servers is required: one person to log on to start the Windows 2000 OS and

[307] *See* Tex. Adm Code § § 81.60, 81.61

[308] https://www.sos.state.tx.us/elections/forms/sysexam/hart621cert.pdf Last visited 06/23/22

[309] https://www.sos.state.tx.us/elections/forms/sysexam/hart621cert.pdf Last visited 06/23/22

a second person to log on to start the specific application (e.g., BOSS, Tally, Ballot Now, eCM Manager)."

b. "A two-person control team must be present any time the Tally application is open."

c. "Version 6.2.1 Application Logs and Windows 2000 Audit Logs, which track user log-ons and log-on attempts, must be regularly reviewed by the local election officer. The Office of the Secretary of State may inspect these logs or may require the logs to be copied and mailed to this office."

d. "Hart *Windows 2000 "Hardened" Operating System* Security Settings is *required.* Hart Windows 2000 "Hardened" Operating System Security Settings presents a table of Win2K system settings installed to achieve the "hardened" configuration. The format of the settings closely approximates that used in the applicable NIST checklist." (*Emphasis added*)

e. "*Each political subdivision* which adopts Version 6.2.1 *must file an initial written confirmation with the Office of the Secretary of State that they are in compliance with Condition Numbers 1 through 4, above, and subsequent to the initial confirmation filing, must file annual, updated confirmations.*" (*Emphasis added*)

503. Although the Secretary of State placed some conditions on the certification of this vulnerable system a very important condition recommended by Stephen Berger (Berger) was ignored.

504. In his report (Berger Report) dated March 3, 2008, Berger asserts[310]

> "All files installed with the system must be filed with the NIST (National Institute of Standards and Technology) and NSRL (National Software Reference Library).
>
> "Hart InterCivic's response is egregiously Deficient"
>
> "To support incoming inspections of new systems a list of all files installed is need so that the new system can be verified as having only the system as certified."
>
> "Pre and post election checks to confirm that software has not been changed or tampered with are recommended. To do this local jurisdictions must have HASH codes of all static files. Further to avoid the system having a single point vulnerability the non-static files, that change with use, should be evaluated by an entity other than the vendor. Why non-static files change should be understood by state and local authorities. Election officials should make their own independent determination that files that change with use and are not included in pre and post election checks are appropriate and do not represent a security vulnerability"
>
> "The Hart software makes 'broad use of Windows resources, including hundreds of DLLs and other executable files'. Each of

[310] https://www.sos.state.tx.us/elections/forms/sysexam/stephenberger621.pdf *See* pages 1-2 Last visited 06/23/22

> those files represents a potential vulnerability, an opportunity to introduce malicious code into the system. For that very reason it is essential that the information be available to verify these files both in the certification process and pre and post election."
>
> "Being able to confirm that the software certified at the national and state level is identical to that installed and used in elections is one of the most significant improvements to total election system security that can be made. Implementing such checks requires not modification or recertification of a voting system, unlike many changes. The tools to verify HASH codes are readily available and do not require extensive training to use. It is hard to imagine why a change that is this beneficial is being resisted."

505. To clarify why the HASH codes are so important Berger goes on in his report to say "Further, safeguards are needed to assure that only the approved update is installed on systems. The current practice potentially allows additional software to be installed under the guise that it is part of the operating system update."

506. And that, "It has been reported in reviews of this system in other states that it is possible to bypass the Hart software security settings. This item was discussed in the California evaluation of the Hart 6.2.1 system."

507. HASH code validation practices would have mitigated these risks.

508. The most alarming statement in the Berger report is a quote from a California expert report that states: "Some of the findings from previous studies on precinct count optical scanners were replicated on the eScan, and they allowed the Red Team to maliciously alter vote totals with the potential to affect the outcome of an election. These attacks were low-tech and required tools that could be found in a typical office."[311]

509. Berger[312] recommended that this system NOT be certified and repeatedly states throughout his report that there are serious concerns with the security of this voting system and that those concerns should be addressed, and the system should be reevaluated to ensure they were addressed before the system was certified for use in Texas.

510. Montgomery County is using Windows 7 operating system with the Hart eSlate Voting System Version 6.2.1 and not the required Windows 2000 "hardened" Operating System.

511. A change in the type of operating system used with an election system would have required a new certification, especially when the operating system used was clearly spelled out in the certification process as vital to the security of the system.

512. "Hart InterCivic 6.2.1 system should have been denied certification until these serious issues were addressed by Hart and once addressed should

[311] https://www.sos.state.tx.us/elections/forms/sysexam/stephenberger621.pdf *See* page 19

[312] https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/red-hart-final.pdf

have been required to be fully reevaluated to ensure that the issues were resolved specifically via the legal route of the EAC.

513. In fact, according to the Berger Report "Operating systems have many configuration options and depending on the options selected can range from relatively secure to very vulnerable.

514. For this reason the VSS (Voting System Standards) 2002 and the VVSG (Voluntary Voting System Guidelines) 2005 require that the vendor specify the operating system configuration and that the security of the recommended by evaluated by the ITA, now VSTL (Voting System Test Laboratories).

515. If the configuration of the operating system is not controlled many other security safeguards are of little value. The configuration of the operating system is a foundational piece essential to the overall security of the operating system. This fact is recognized and results in multiple requirements in the VSS 2002."

516. Not only have multiple Secretaries of State knowingly "certified", or failed to decertify, an insecure election system, they have also failed to monitor and enforce the conditions they placed upon the contingency of certification of the equipment and the usage in the counties that utilized it.

517. A Public Information Act request sent to the Secretary of State's office seeking to obtain the annual filings by Montgomery County for years 2018, 2019, 2020 and 2021, that were required by the Secretary of State to maintain "certification" of this election system, returned no results.

518. To be clear, in at least the last 4 years, the Secretary of State's office received none of the filings from Montgomery County that were required to obtain at least the appearance of certification of the election system they were using.

519. According to Suzie Harvey, she has been the Elections Administrator for Montgomery County since 2011. She stated that she has never seen the conditioned certification letter from the Secretary of State's website and has therefore never filed an annual report related to the conditioned certification. She further stated that she has never received any communication from the Secretary of State's office in her 11 years notifying her that she was out of compliance with those requirements even though she receives many communications from their office detailing requirements.

520. Montgomery County has used equipment that would have been considered uncertified even by the terms of the Secretary of State's "certification" letter since at least 2018.

521. The Secretaries of State holding office from 2008 to today had the legal and moral duty under Texas Election Code[313] to monitor and ensure receipt of the annual reports required for "certification" of Hart eSlate Voting System 6.2.1 and that all of the other 4 conditions for "certification" were met as they understood the system was vulnerable to manipulation.

522. We have filed a Public Information Act request with the Secretary of State's office to obtain

[313] *See* Tex. Elec Code § 31.005

the annual reports for Montgomery County for the years 2009-2017 but have not yet received an answer to that request.

523. Montgomery County was still using this uncertified election equipment as recently as the runoff election held on March 24, 2022, the Secretary of State has failed to protect the voting rights of the People of Montgomery County violating the election code.[314]

524. The SoS violated the Election Code in regards to uniformity as the people of Montgomery County were forced to vote on vulnerable equipment that was never certified by an EAC accredited VSTL.[315]

525. We contend that due to these actions and lack of action by the Secretary of State, the elections in Montgomery County have been illegal, unreliable, and therefore uncertifiable since at least January 1, 2006.

526. Currently, according to the SoS's website; 35 counties in the state of Texas in addition to Montgomery County are conducting illegal and uncertifiable elections due to the illegal "certification" of Hart eSlate Voting System 6.2.1 by the Secretary of State in 2009.[316]

f. Archer, Brown, Burleson, Burnet, Cass, Coke, Comanche, Crosby, Dawson, Delta, Duval, Ector, Falls, Fannin, Foard, Gray,

[314] *See* Tex. Elec Code § 31.005

[315] *See* Tex. Elec Code § 31.003

[316] https://www.sos.state.tx.us/elections/forms/sysexam/voting-sys-bycounty.pdf Last visited 06/23/22

> Grimes, Harrison, Hudspeth, Jefferson, Jim Hogg, Karnes, Kennedy, Kimble, LaSalle, Lipscomb, Marion, Matagorda, Mclennan, Menard, Shackelford, Wichita, Wilbarger, Willacy and Wood.

527. We have filed a Public Information Act request with the Secretary of State's office to obtain the annual reports for these counties for the last 4 years but have not yet received an answer to that request.

528. Texas Certification Procedures for Electronic Pollbooks states: "Election Code 31.014 requires an electronic pollbook system that is used in Texas elections to be certified annually by the Secretary of State's Office. Accordingly, vendors will need to seek recertification of their system on an annual basis which will become effective on January 1 of the year in which the system will be used."[317]

529. Through a Public Information Act request with the Secretary of State's office we were able to determine that Montgomery County, as an Electronic Pollbook vendor, has failed to obtain recertification of its electronic pollbook for the election year 2022 in violation of Election Code.[318]

530. In the state of Texas for the years 2021 and 2022 only 3 of the 6 electronic pollbook vendors were certified by the Secretary of State.

[317] https://www.sos.texas.gov/elections/laws/certification-pollbooks.shtml *See* Tex. Elec Code § 31.014 Last visited 06/23/22

[318] *See* Tex. Elec Code § 31.014

531. April 1, 2021, the SoS's office certified Hart Verity Voting System Version 2.5 for use in Texas elections without the required EAC certification

532. While Hart Verity Voting System Version 2.5 has an illusion of certification by an EAC accredited VSTL, that certification is fraudulent because the Voting System Test Laboratory, SLI Compliance, that approved the certification is not an accredited laboratory in accordance with the Voting System Test Laboratory Program Manual ver. 2.0 effective May 31, 2015, page 38, Sec 3.6.1.

533. On October 26, 2021, Montgomery County purchased Hart Verity Voting System Version 2.5. This system was not certified by an EAC accredited VSTL and should have never been "certified" by the Secretary of State's office.[319]

534. The Hart Verity Voting System Version 2.5 has not yet been placed into service in Montgomery County but will affect future elections.

WILLIAMSON COUNTY

535. Williamson County Commissioners, in addition to election officials, have failed to confirm if the voting equipment in Williamson County is properly certified.

536. The Williamson County Elections Administrator since 2019 is Christopher Davis.

537. According to responses to Public Information Requests (PIR) for electronic voting system versions, Williamson County said:

[319] *See* Tex. Elec Code § § 81.60, 81.61

a. 2018 – Not applicable.

b. System purchased in Summer 2019

c. 2019 – ES&S EVS 6.0.2.0

d. 2020 – ES&S EVS 6.1.0.0

e. 2021 – ES&S EVS 6.1.1.0

f. 2022 – ES&S EVS 6.1.1.0

538. Elections Administrator Chris Davis received approval from the SoS's office on April 23, 2019, for the purchase of ES&S's EVS 6.0.2.0.

539. According Davis via email, ES&S's EVS 6.1.0.0 was utilized for the November 3, 2020.

540. Chuck Pinney, Staff Attorney, Elections Division submitted a memorandum to Keith Ingram, Director of Elections notating. "At the time of the examination, the system was somewhat limited in its ability to comply with the non-sequential ballot serialization requirement in particularly large counties . . . Despite this issue, I would recommend certification."

541. Williamson County has not answered my PIA request of the election ware used in the past few years.

542. Williamson County commenced with a recount 235,000 of early voting ballots where vote totals were accurately recorded but could not be separated by voting precinct, as required by state law. Williamson County has 94 voting precincts.

543. A computer programming issue also caused ballots not to be separated by precinct.[320]

a. On November 12, 2020, Williamson County still had 3,400 provisional ballots to be presented to the county's ballot board to determine how many should be accepted.

b. The county on this date currently had 1,000 provisional votes had been accepted but not yet counted.

c. Per Davis the county usually only receives 1,000 to 1,500 provisional votes in an election. The election of 2020 was double the amount.

d. Included in these provisional ballots were ballots cast by people who had requested mail-in ballots but cast in person instead.

e. Due to these issues Davis said it is possible that outcomes may change for some races.

f. The reasons there are so many provisional ballots, Davis said, is that poll workers are trained to never turn a voter away, even if they're not registered in the county poll book.

g. "As a consequence of that, a provisional voter could be one that isn't registered at all," he said, "or is still registered in another state or county but could only vote in WilCo as a last resort."

[320] https://www.statesman.com/story/news/local/2020/11/12/williamson-county-still-sorting-through-3400-provisional-ballots/43092675/ Last visited 06/23/22

h. "So they voted provisionally," Davis said. "Most likely, if they didn't register in WilCo by the (Oct. 5) deadline, their ballot won't be accepted and counted. Same for voters that voted provisionally for lack of a voter ID and didn't come in to cure that deficiency within the state-mandated six days. Their ballot will most likely not be accepted."

544. "Will most likely not be accepted" is not acceptable as the election code requires all voters be registered by October 5, 2020 of the election year.

545. Brandon Jenkins, Voting System Analyst for Williamson County Elections sent an email to Darren Znamenacek and employee of ES&S regarding "wildly incorrect" precinct results.[321]

From: Brandon Jenkins

Sent: Monday, November 2, 2020 5:26 PM

To: Zha**** (not legible), Darren

Cc: Crhistopher J. Davis, Moody, Chris

Subject: precinct by precinct results importance: high

Darren, as we discussed on the phone, I'm seeing the following issues. Our precinct by precinct results for our "in person early voting" reporting group are wildly incorrect. We have some precincts that are showing over well 10,000 ballots cast we know precinct has more than 8000 voters. We have other precinct that are showing zero ballots cast I don't understand what could be causing this, please

[321] https://dl.airtable.com/.attachmentThumbnails/2e2a50d0c22985075d6bfa7465289821/409bb881 Last visited 06/23/22

> escalate this as high as it can be escalated. I'm currently uploading a backup of my election, the results summary that shows the precinct returns, and a copy of my ballot on demand file please let me know who I should reach out to about this, and if there's anything you can find that is causing this.
>
> Brandon Jenkins
> Voting Systems Analyst
> Williamson County Elections

546. Williamson County decided to do a second recount by hand of early voting ballots due to inaccuracies.

547. Davis presented the results of the first count of the early voting by precinct to commissioners and state, but he could not say how accurate the results were because 235,000 early votes had to be sorted manually into 94 precincts to meet a state deadline of November 16, 2020.[322]

a. The county's election office had to count the early voting ballots for precinct results by hand because a bar code that would have sorted them by each of the county's 94 precincts was not on the ballots.

b. Davis said it was caused by the county's vendor and was discovered and fixed before votes were cast on Election Day.

[322] https://www.statesman.com/story/news/local/2020/11/18/williamson-commissioner-asks-for-possible-recount-of-precinct-by-precinct-election-results/114981050/ Last visited 06/23/22

c. "It wasn't a mistake we made," said Gravell. "It was a mistake the vendor made and we are going to ger the right data."

548. According to Commissioner Court minutes, Williamson County plans to canvas the 2020 election.

549. ProV&V was the VSTL that certified EVS 6.1.0.0.[323]

550. ProV&V is not an accredited laboratory in accordance with the Voting System Test Laboratory Program Manual ver. 2.0 effective May 31, 2015, page 38, Sec 3.6.1.

551. It is unclear if Williamson County was affected by the HASH validation failure as the SoS has not released specific information regarding the affected counties that utilized ES&S for their elections.

COLLIN COUNTY

552. Collin County Commissioners, in addition to election officials, have failed to confirm if the voting equipment in Collin County is properly certified.

553. Cheryl Gorena via email confirmed EVS 6.1.01.0 was utilized for the November 3, 2020, election. The SoS's website states 6.0.0.0.

554. Bruce Sherbet, Elections Administrator confirms that per Election Advisory 2016-12, "All voting systems in use for Texas elections must be federally certified by the Texas Secretary of State . . . To execute a contract to sell, lease or otherwise provide a voting

[323] https://www.eac.gov/voting-equipment/evs-6100 Last visited 06/23/22

system that has not been approved by the Texas Secretary of State is a Class A Misdemeanor."

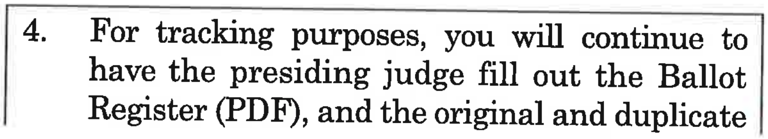
555.

{ Letter not legible for reproduction }

556. Chuck Pinney, Staff Attorney, Elections Division of SoS noted in memorandum from the examination of EVS 6.1.1.0; "The technical examiners identified concerns regarding the complexity of the hash validation process for this system and regarding the password reset requirements authorized by the system. Those concerns do not affect the reliability, accuracy, or security of the system if proper procedures are followed. I would recommend that the vendor make adjustments to these procedures based on the feedback of the examiners."[324]

557. Election Advisory No. 2019-23, cover hash validation procedure as well as the "Tracking of Ballot Numbers Through the ExpressVote Activation Card Printer/ExpressLink Software"[325]

a. Ballot sequential advising jurisdiction to ignore election law.[326]



4. For tracking purposes, you will continue to have the presiding judge fill out the Ballot Register (PDF), and the original and duplicate

[324] https://www.sos.texas.gov/elections/forms/sysexam/chuck-pinney-examiner-report-ESS-6110-aug.pdf#search=evs%206.1.1.0 Last visited 06/23/22

[325] https://www.sos.state.tx.us/elections/laws/advisory2019-23.shtml Last visited 06/23/22

[326] *See* Tex. Elec Code § 51.006, 51.007, 51.008, 52.062

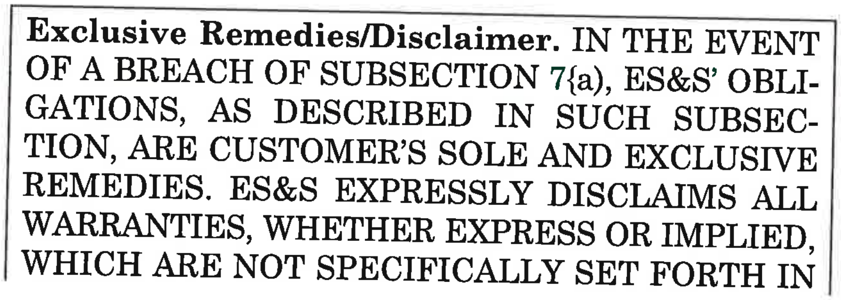
> forms will be returned in the applicable envelopes. The ballots shall be tracked, distributed, and retained just as you would with a traditional pre-printed full ballot in accordance with Sections 51.006, 51.007, 51.008 with the exception of notating the serial number of the ballot ranges.

b. Hash validation advising jurisdictions MUST complete with the vendor provided specific instructions.

> 3. The entity MUST complete a system validation. Your vendor should provide you with specific instruction in how to validate that software that is being installed and used on your voting system is the same software that was certified by the EAC.

558. On June 4, 2019 executed ES&S vendor contract for ES&S voting equipment and systems.

a. General Term Section 7(b) Exclusive Remedies Disclaimer expressly requires the Collin County to use ES&S for hash-validation testing. Below is the provision.[327]

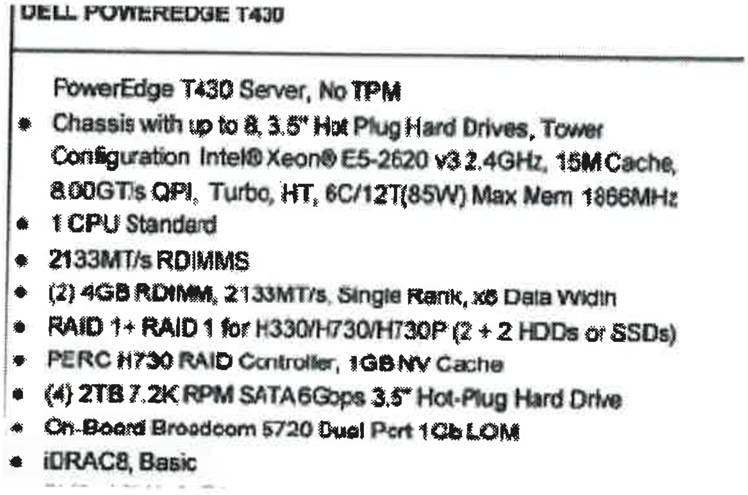


Exclusive Remedies/Disclaimer. IN THE EVENT OF A BREACH OF SUBSECTION 7{a), ES&S' OBLIGATIONS, AS DESCRIBED IN SUCH SUBSECTION, ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES. ES&S EXPRESSLY DISCLAIMS ALL WARRANTIES, WHETHER EXPRESS OR IMPLIED, WHICH ARE NOT SPECIFICALLY SET FORTH IN

[327] https://eagenda.collincountytx.gov/docs/2020/CC/20200601_2483/48428_2018241%20Contract.pdf Last visited 06/023/22

THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. FURTHER, IN THE EVENT CUSTOMER DECLINES ES&S' INSTALLATION AND ACCEPTANCE TESTING SERVICES OR IN ANY WAY AT ANY TIME ALTERS, MODIFIES OR CHANGES ANY EQUIPMENT, SOFTWARE, THIRD PARTY ITEMS AND/OR NETWORK (COLLECTIVELY "SYSTEM") CONAGURATIONS WHICH HAVE BEEN PREVIOUSLY INSTALLED BY ES&S OR WHICH ARE OTHERWISE REQUIRED IN ACCORDANCE WITH THE CERTIFIED VOTING SYSTEM CONFIGURATION, ALL WARRANTIES OTHERWISE PROVIDED HEREUNDER WITH REPECT TO THE SYSTEM PURCHASED, LEASED, RENTED AND/OR LICENSED UNDER THIS AGREEMENT SHALL BE VOID AND OF NO FURTHER FORCE AND EFFECT.

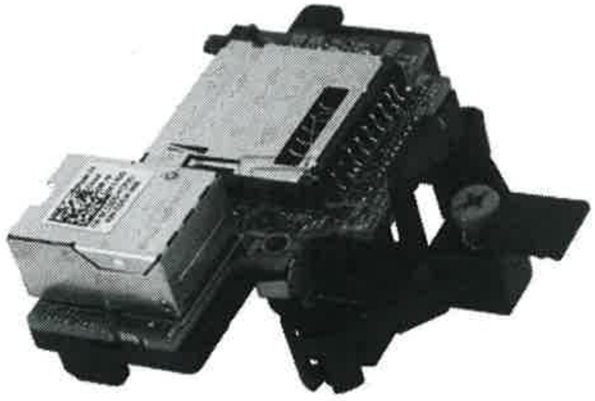
b. Listed under Dell Poweredge T430 is listed a component "iDRAC8" which is installed in the EMS.



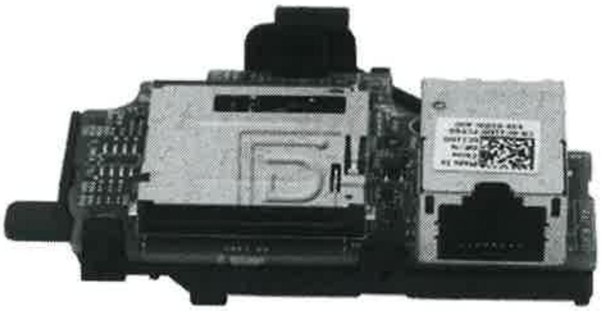
DELL POWEREDGE T430

PowerEdge T430 Server, No TPM

- Chassis with up to 8, 3.5" Hot Plug Hard Drives, Tower Configuration Intel® Xeon® E5-2620 v3 2.4GHz, 15M Cache, 8.00GT/s QPI, Turbo, HT, 6C/12T(85W) Max Mem 1866MHz
- 1 CPU Standard
- 2133MT/s RDIMMS
- (2) 4GB RDIMM, 2133MT/s, Single Rank, x8 Data Width
- RAID 1+ RAID 1 for H330/H730/H730P (2 + 2 HDDs or SSDs)
- PERC H730 RAID Controller, 1GB NV Cache
- (4) 2TB 7.2K RPM SATA 6Gbps 3.5" Hot-Plug Hard Drive
- On-Board Broadcom 5720 Dual Port 1Gb LOM
- iDRAC8, Basic



c. Dell touts the (iDRAC) as an integrated Dell Remote Access Controller.



"iDRAC . . . . is part of a larger datacenter solution that helps keep business critical applications and workloads available at all times . . . allows administrators to deploy, monitor, manage, configure, update, troubleshoot and remediate Dell servers from any location, and without the use of agents."

d. "Leveraging the incomparable agent-free capabilities of the embedded, integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller technology, server deployment, configuration and updates are streamlined across the OpenManage portfolio and through integration with third-party management solutions."[328]

e. "Remote management: iDRAC8 with Lifecycle Controller, iDRAC8 Express (default), iDRAC8 Enterprise (upgrade), 8GB vFlash media (upgrade), 16GB vFlash media (upgrade)"

[328] https://i.dell.com/sites/csdocuments/Shared-Content_data-Sheets_Documents/en/aa/Dell-PowerEdge-T430-Spec-Sheet.pdf Last visited 06/23/22

f. The iDRAC8 modem creates a serious security breach and violates a multitude of election and penal codes.[329]

g. According to Bruce Sherbet, Elections Administrator's own words via email states that the county must receive an approval from the SoS's office prior to purchasing a voting system.[330]

559. ProV&V was the VSTL that certified EVS 6.1.1.0.[331]

560. ProV&V is not an accredited laboratory in accordance with the Voting System Test Laboratory Program Manual ver. 2.0 effective May 31, 2015, page 38, Sec 3.6.1.

DENTON COUNTY

561. The voting machines used in Denton County for the November 2020 elections were not certified, as is required by Texas law (TX Election Code § 122.001, TX Admin. Code § 81.60 (3). TX Admin. Code § 81.60 (8)(B) and TX Admin. Code § 81.61), therefore violating Art 6, § 2(c) and Art 6, § 4 of the Texas Constitution. TX Election Code § 122.001 prevents voting systems from being used in an election unless they met the

562. VOTING SYSTEM STANDARDS contained within, one such requirement ensuring the system

[329] *See* Tex. Elec Code 122.001(a)(4), TEX. PEN. CODE § 16.02, § 33.05, 18 U.S.C. § 1030

[330] *See* Tex. Elec Code 122.005(a)

[331] https://www.eac.gov/voting-equipment/evs-6110 Last visited 06/23/22