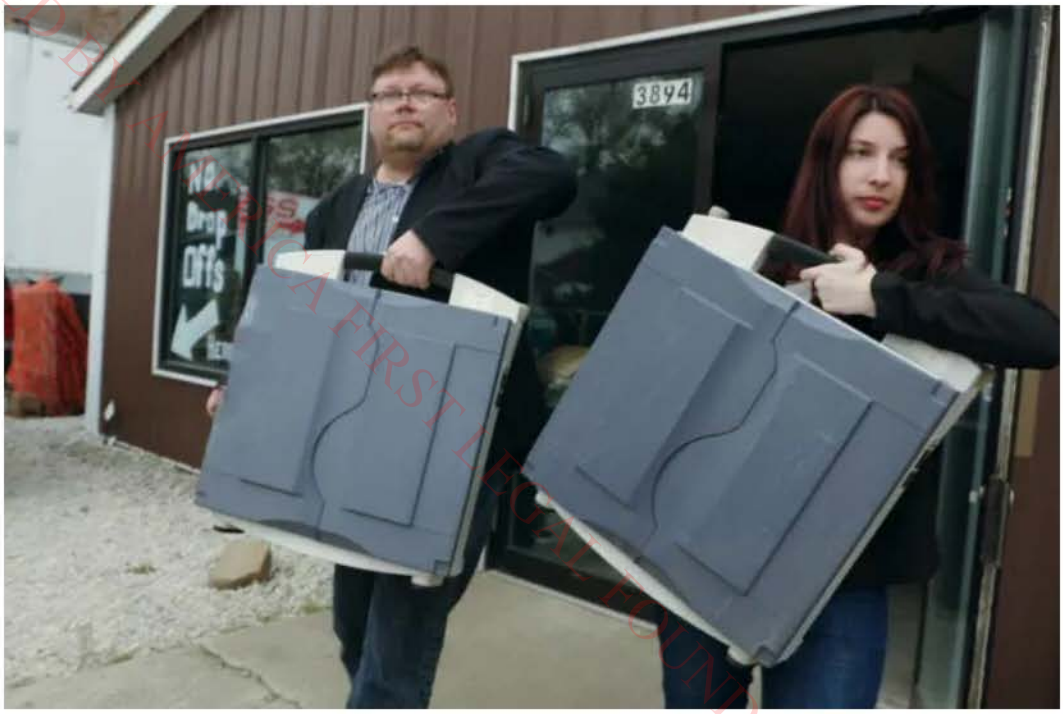
Exhibit 2

Chicago Sun Times

‘Kill Chain’: HBO documentary sounds an alarm about voting machine hacks

‘Kill Chain’: HBO documentary sounds an alarm about voting machine hacks



Election security experts Harry Hurstin and Maggie McAlpine carry voting machines they purchased in “Kill Chain.”
HBO

In the sobering and eye-opening HBO documentary “Kill Chain: The Cyber War on America’s Elections,” we see clips of various government officials and security specialists claiming America’s voting machines are too clunky and old-fashioned to be hacked.

The comments are remarkably similar:

“From what we determined, no voting machines are connected to the Internet …

“Voting machines are not connected to the Internet …”

‘Kill Chain: The Cyber War on America’s Elections’: 3 out of 4

HBO presents a documentary directed by Simon Ardizzone, Russell Michaels and Sarah Teale. Debuts at 8 p.m. Thursday on HBO and streaming on HBO Now, HBO Go and HBO on Demand.

"They are non-network pieces of hardware that are not connected to the Internet ..."

"Those things are not connected to the Internet ..."

Cut to one Harri Hursti, the rotund, avuncular, legendary Finnish expert on hacking and voting security, who has just purchased three commonly used American voting machines for $75 apiece from an Ohio recycling vendor he found on eBay, I kid you not.

Hursti plugs in the machine, turns it on — and the first thing that pops up on the screen is an option to connect to a local area network. So much for the protected-by-being-out-dated argument. As Hursti and other cyber security specialists explain, even when we're voting with paper ballots, there's always a thumb drive, or a USB memory stick — some kind of removable media device, which means there's always the opportunity for some-one to mess with the process.

From directors Simon Ardizzone, Russell Michaels and Sarah Teale, the same team behind HBO's 2006 Emmy-nominated doc "Hacking Democracy" (which also "starred" Hursti), "Kill Chain" is at times a bit dry and tough to track, what will all the techno-terms and cyber-chat, so to speak. But in its most effective moments, it's like something out of a dramatic/comedic feature film on the order of "The Big Short." Our jaws drop as we learn stunning truths about America's messy, outmoded and far too vulnerable voting system.

As author and journalist Sue Halpern explains, "Our elections are run locally. There's no national election system. It's up to the counties and the election officials in those coun-ties — they get to decide how we vote, what machines we use. ... Paper ballots, [votes from] electronic machines, touchscreen computers ... all of the votes go to a central loca-tion."

Three main vendors run the vast majority of election machinery in this country: Domin-ion Voting, Elections System & Software, and Hart. They don't reveal anything about how their systems work, because it's all proprietary. (All three companies declined to be interviewed for the doc.) It would be an understatement to say "Kill Chain" makes the case these machines are hardly tamper-proof.

Time and again, the experts say when government officials proclaim “there’s no evidence votes were changed” in a particular election, they’re missing the point. The goal of the bad actor is to cause chaos — often between cycles, not during the actual election.

“Malware can infect machines between election cycles,” says one expert. “It would be very easy to write a piece of software into [an American voting machine] that would silently change votes as they come in and there would be no evidence [of it happening]. This is a relatively simple machine. It wouldn’t be hard to remove traces it had been tampered with.”

Case in point: In an election in a heavily Democratic precinct in Georgia, there were seven machines. Six machines showed easy wins for Democrats in every statewide race. One showed Republicans winning every race by a large majority. A study found that mathematically, there was less than a one in a million chance of that happening.

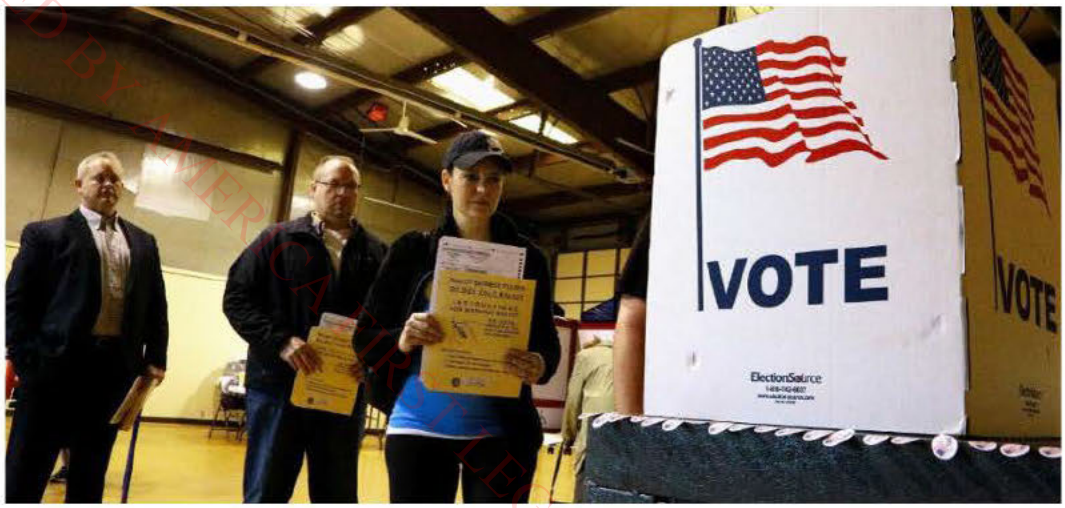
Sometimes the numbers add up in a way that doesn’t add up.

Exhibit 3

Forbes

HBO Documentary Shows The Value Of Cybersecurity In Election Security

HBO Documentary Shows The Value Of Cybersecurity In Election Security



FILE - In this March 15, 2016, file photo, people line up to vote in the primary at a precinct in ... [+] Bradfordton, Il.

ASSOCIATED PRESS

One thing is sure: after the coronavirus is no longer dominating the news, election security will come back to center stage. It is a complicated subject that few people really understand – even election officials. It is important to know right off the bat that election security is **not** just about Russian interference and disinformation campaigns; it is also about the role that private sector companies play in the voting system and the security vulnerabilities associated with voting machines and election processes.

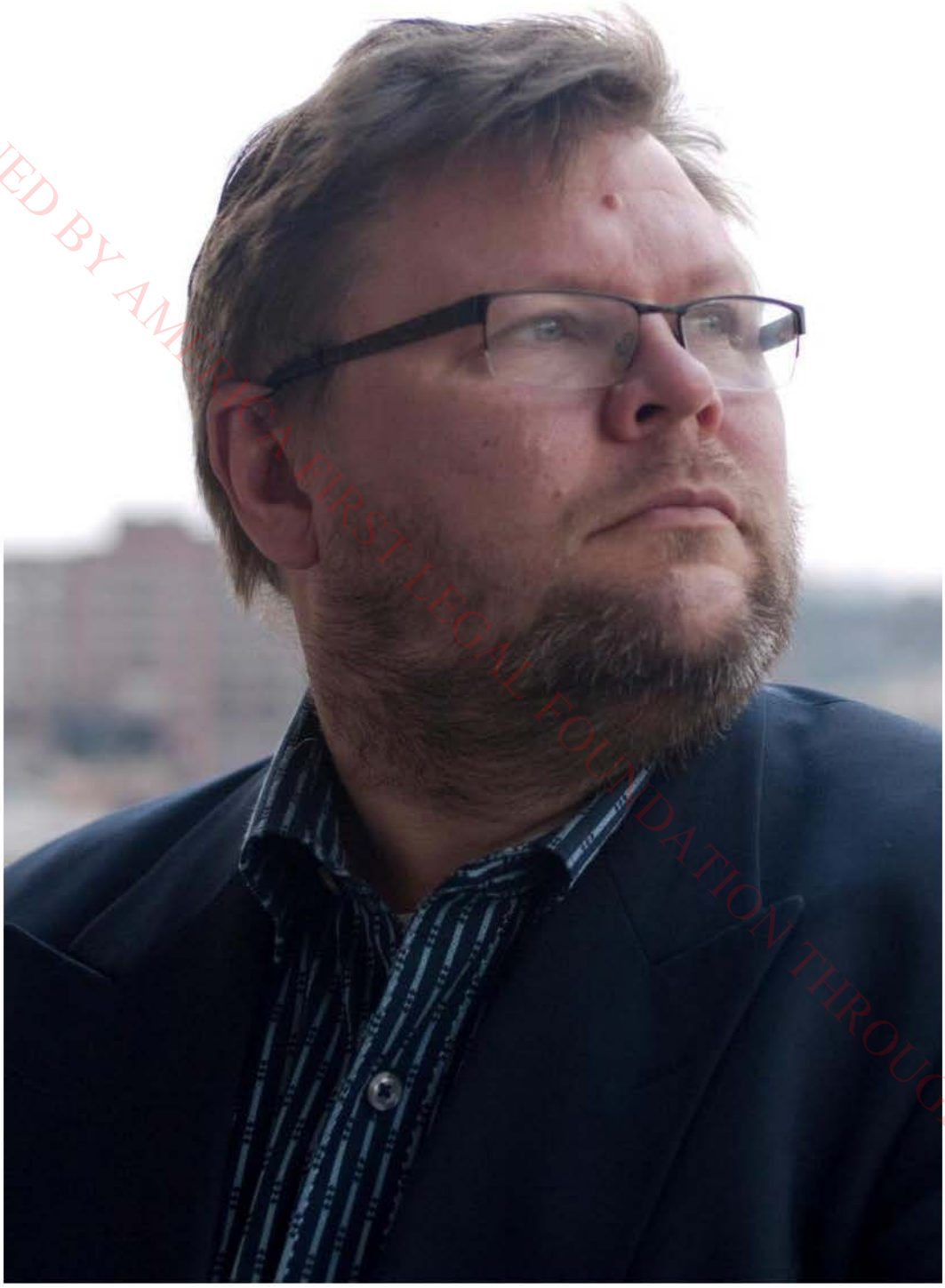
Unbeknownst to most people, the core activities within elections are handled by private sector companies, not state or local officials. Private companies (a) sell the voting machines and program them for most elections, (b) register voters, (c) tally votes, and (d) report votes, and there are known security vulnerabilities in every process. The security of our elections is really about the vulnerabilities within the voting machines and electronic processes used in all of these functions, weak cybersecurity practices

within election agencies, and the cluelessness of election officials about the technology they use.

HBO Documentary — Kill Chain: The Cyber War on America's Elections

HBO spent four years talking to some of the world's foremost experts on election issues, following them around from country to country, and putting together a compelling documentary film telling the real story about election security more completely and clearly than any other news report – Kill Chain: The Cyber War on America's Elections. It premiered March 26 and is now available free on YouTube. The film is one every American should watch to learn the truth from the cybersecurity community, leading reporters and academicians, and the cyber criminals themselves about how insecure our elections really are.

Voting Machines and Electronic Processes



Harri Hursti

Photo courtesy of Harri Hursti

Harri Hursti has been working on election security issues for the past decade and is widely considered one of the foremost experts on the subject. In 2005, Hursti performed the famous Hursti Hack and successfully altered votes in a one-step hack that changed both the central tabulator results and the voting machine results tape. It was the digital equivalent of stuffing the ballot box. The election official who invited Hursti to check the Diebold AccuVote optical scan voting machines said he would not have been able to detect the change and would have certified the election. HBO's 2006 Emmy-nominated documentary (for investigative journalism), Hacking Democracy, covered this hack.

The hack demonstrated that Diebold's claims that votes could not be changed on the memory card and that the cards did not contain any executable code were false. Diebold called the hack a "sham." California's Secretary of State asked UC Berkeley to investigate the Hursti Hack. They did and issued a report validating Hursti's work and stating that it was indeed possible to change the election results. Hursti subsequently found serious security flaws in the Diebold AccuVote TSx touch-screen voting machine.

In 2009, Diebold Election Systems was sold to its competitor, Omaha-based ES&S, and in 2010 ES&S flipped it to Dominion Voting Systems, a company with international headquarters in Toronto, Canada and U.S. headquarters in Denver.

None of the vulnerabilities found by Hursti were ever fixed, and these same machines are planned for use in 20 states in the 2020 election. A later model of these same voting machines – with the same vulnerabilities – was used in the hotly contested and disputed 2016 election for the governor of Georgia between Brian Kemp and Stacy Abrams. During that race, some of the machines malfunctioned, particularly in precincts that were known to be important to the outcome of the race. Lines were long, some waited five hours, and some voters did not get to vote.

As Hursti succinctly notes in the film:

Voting is about our capability to change the way the government works by changing the people who make the decisions, and to have a

peaceful transfer of power when the people have made that choice. If you don't have that, then the alternatives are revolutions.

Harri Hursti, The Kill Chain: The Cyber War on America's Elections

There are many avenues for tampering with an election, including changing votes, causing machines to malfunction, altering voter registration records, and disrupting equipment used to check in voters. The film covers all of these possibilities.

Russians Hacked and Planned

The Russians did more in the 2016 elections than run disinformation campaigns. In the film, Ion Sancho, the Supervisor of Elections in Leon County, FL from 1988-2016, relates how all supervisors of elections in the state of Florida were ordered to participate in a secret call on September 30, 2016, during which the FBI informed them that a foreign power had penetrated a vendor who serviced Florida elections. Mr. Sancho said they very quickly realized the FBI was referring to the GRU, Russia's military intelligence service, and VR Systems, a company that handles all of the programming for the majority of the counties in Florida and handles all absentee ballots and early voting.

VR Systems sells electronic poll books in eight states, which are used to check in voters and determine if they are legitimately registered. The film carefully documents situations in the 2016 elections where electronic voter ID systems in several states went down in certain precincts. These machine "technical glitches" caused hours-long lines for people who had come to the polls to vote. Some voters were unable to wait and others could not vote before the polls closed.

Sue Halpern, an author and contributor to *The New Yorker* who has researched and written about election security problems, states:

If your goal is to undermine democracy, you actually don't need to change votes to hack an election; when you prevent people from casting a ballot, you've hacked an election.

Sue Halpern, Kill Chain: The Cyber War on America's Elections

Mr. Sancho notes that all of the election officials in the country were "clueless" about what had happened until an NSA contractor, Reality Winner, leaked a Top Secret report that detailed how the Russians had launched a voter registration spear-phishing campaign targeting U.S. election officials involved in the management of voter registration systems. *The Intercept* anonymously received the NSA report, independently authenticated it, and reported on the Russian campaign in more detail. Sen. James Lankford (R-OK) states in the film that, "It was about a year later before the states that were actually attacked by the Russians were able to hear and know it was the Russians doing it. We should never have that."

As it turns out, the organization that is tasked with providing voting best practices and assistance to all election officials across the country, the U.S. Election Assistance Commission (EAC) was perhaps the weakest link in the nation's voting system. The EAC is a bipartisan commission established by Congress in 2002. It maintains the national mail voter registration form, accredits testing laboratories and certifies voting systems, and serves as a national clearinghouse of information on election administration. In testimony before Congress, Thomas Hicks, Chairman of the EAC, emphasized that, "Our elections are secure. They are secure because the American election administration system inherently protects them."

Thomas Hicks, chairman of the U.S. Election Assistance Commission (EAC)

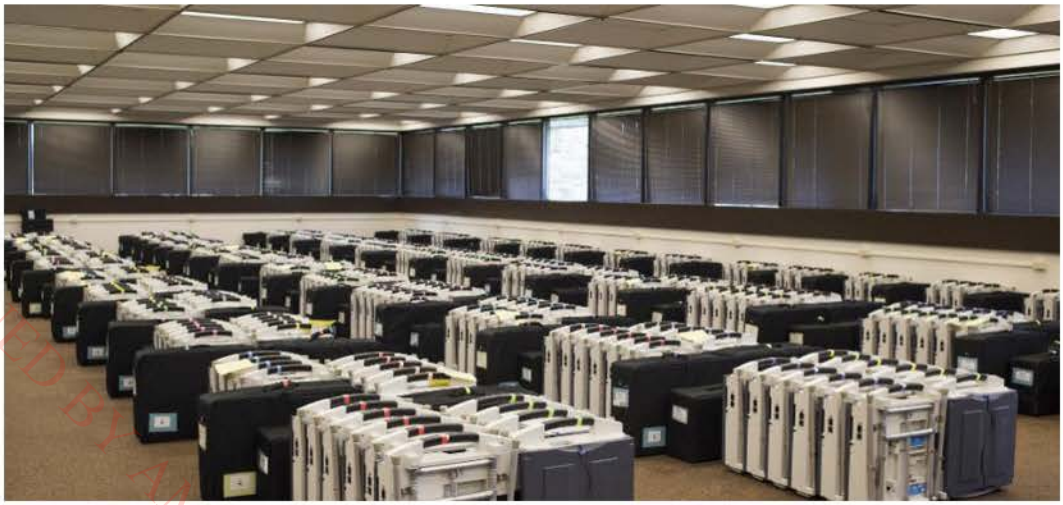
Mr. Hicks's reassurances fell apart in December 2016 when cybersecurity company Recorded Future reported that a Russian-speaking hacker named Rasputin was selling access to the EAC's computers. Recorded Future actually obtained EAC documents from Rasputin, including lists of voting machinery, test reports of their software, and where they were deployed. Hursti called the document a "one stop shop all of the information you need to plan your attack campaign; it is a very horrible scenario." Rasputin had full admin access to the database and could upload any file he wanted.

An EAC employee whose credentials had been compromised said if Rasputin had access to the database, he could access the server where the proprietary information is kept. Sen. Lankford explains in the film that the EAC keeps information about vulnerabilities in voting systems, so a hacker who gets into the EAC could find out where the weak links are in the voting system. He notes that "for a persistent actor, especially for a foreign government, who has the finances and the capability to be persistent in it, this is the way to do it."

Voting Machine Companies: Recalcitrant and Arrogant

James Comey, former Director of the FBI, told Congress, "Our voting system in the United States is so very, very hard for someone to hack into because it is so clunky and dispersed...."

That view is probably shared by most Americans. They know that elections are managed at the local and county levels and assume that it would be too difficult to coordinate a hack that could influence an election.



Electronic voting machines sit packed and ready for precinct distribution at the Fairfield County ... [+] Board of Elections Office in Lancaster, Ohio, U.S., on Saturday, Oct. 29, 2016.

This is wrong-headed thinking. There are three primary vendors for voting machines: Election Systems & Software (ES&S), Dominion Voting Systems, and Hart InterCivic, and very little is known about the security of these companies' own IT systems. Some voting machines are optical scanners, some have touch screen voting, some use QR codes or bar codes, and others send votes in clear text back to vendors to be tallied. They can all be hacked or compromised. If almost all of the voting precincts in our clunky system use equipment from these vendors, an attacker only needs to hack the equipment to reach all of the voters.

Former White House Cybersecurity Coordinator, Michael Daniel, notes in the film that voting machine companies generally are not known for cybersecurity expertise. Jake Stauffer, a former cyber analyst for the Air Force who has tested ES&S and Dominion voting systems for the state of California observed that:

What I have found, especially in the voting system arena, is that security is not really taken very seriously.

Jake Stauffer, former cyber analyst for the Air Force who tested ES&S and Dominion voting machines.

When Stauffer tested ES&S's DS200 machine, they found multiple vulnerabilities that would enable an attacker to gain full access to the system, change configurations, and install a modified operating system without election officials knowing. Stauffer states that the vulnerabilities would enable a hacker to gain the highest level of privilege and gain remote access into the system and do whatever they wanted to do, "whether its change an election or shut the system down." He found similar vulnerabilities in Dominion's Democracy Suite voting equipment that would enable remote code execution, denial of service attacks, and off-line ballot tampering. "How can a vendor sell a voting system with this many vulnerabilities?" he asks.

Unlike major technology companies, such as Apple and Microsoft, these vendors do not allow researchers to test their equipment or review their code to find vulnerabilities and bugs. The symbiotic relationship between tech software and hardware vendors and researchers helps them improve their products and keep them secure. Voting equipment companies, however, have been highly resistant to any review by the research community, claiming their systems are safe and secure.

Three years ago, Hursti and Matt Blaze, the McDevitt Chair of Computer Science and Law at Georgetown University, set up an annual Voting Village at the popular DEF CON conference and invited the cybersecurity community to come test the voting machines and voting equipment that they had been able to assemble. Hursti has been able to purchase at least six machines on eBay, including the AccuVote TSx, which remains one of the most popular – and vulnerable – voting machines. He obtained others at surplus stores or directly from election officials. Most of the machines contained fairly recent voting data.

During the three years of the Voting Village's existence, none of the vendors has supported the effort or has been willing donate or offer equipment for the researchers to work with at Voting Village. The idea behind the Village is to (1) help develop a community of cybersecurity experts in election security so there are more resources nationally to assist election officials, and (2) to help make the voting equipment more secure by revealing vulnerabilities. It is noteworthy that numerous state and local election officials

do partake in the Voting Village and appreciate the work of the cybersecurity researchers.

Voting Machines, Election Officials, and the Internet

There is this popular belief that voting machines do not connect to the Internet. EAC chairman Thomas Hicks testified before Congress that, "From what we have determined, no voting machines are connected to the Internet.... and so there will not be any sort of Internet hack or Internet incidents." Amy Cohen, Executive Director of the National Association of State Election Directors, testified that, "Voting machines themselves are not connected to the Internet." Brian Kemp, current Governor and former Secretary of State for Georgia, testified, "They are non-networked pieces of hardware that do not connect to the Internet." Andy Ozment, Assistant Homeland Security Secretary for Cybersecurity and Communications, testified, "The devices are not connected to the Internet." James Comey, former FBI Director, testified, "Those things are not connected to the Internet."

"Those things are not connected to the Internet."

James Comey, former FBI Director

This was the moment during a private showing of the film for cybersecurity experts when the entire room burst out laughing. Husti says, "Every single system we have, there is a place where it touches the Internet...it might be indirect, it might be infrequent, but it is always there." When Hursti powers up a machine he purchased off eBay, the first thing it wanted to do was connect to the Internet. Additionally, election officials are less alert between elections, so hackers can infect a machine and the malware can remain dormant in machines between cycles. Jeff Moss, founder of the BlackHat and DEFCON conferences, points out that it would not be difficult to hack these simple machines and erase any traces.

"These machines want to be talking to other devices; they are built for it, and that is what magnifies the threat."

Alex Halderman, Professor of Computer Science and Engineering at the University of Michigan.

Alex Halderman, Professor of Computer Science and Engineering at the University of Michigan, examined the Diebold AccuVote TSx touch screen voting machine with Hursti. They discovered that the machine has a slot for a wireless modem, plus it has a telephone jack and network card, and also has room for a SD slot for an additional memory card that could be used for a wireless connection. "These machines want to be talking to other devices; they are built for it, and that is what magnifies the threat," Halderman notes. He demonstrates how to scale an attack with software he developed that could spread code from machine to machine to ultimately "upset an election across an entire county, an entire state, an entire country." The software he said controlled the machine, the printer, ballot programming, and paper summary tapes. The whole ball of wax.

Sandy Clark, a cybersecurity researcher at the University of Pennsylvania, noted, "I feel like we are in terrible danger of losing what it means to be a democracy; if elections can be altered subtly, they can be altered in a way that is undetectable, how does one trust the results of their election....those of us who know how vulnerable the voting systems are in these elections are terribly afraid right now."

In 2018, Hursti was contacted by Nathaniel Herz, a reporter for the Anchorage Daily News (2013-2018), about some election concerns he had been investigating since the 2016 election. The paper was investigating whether recent activity in Alaskan election systems was linked to the Russian activities they had been reading about. In a call with Josie Bahnke, Alaska Elections Director (2015-2018), Ms. Bahnke said the FBI had advised them that Russians had, in fact, "rattled the door" of their election systems and looked at their website but there had been no breach.

The paper sent a FOIA request to the election office. After a year, they received a packet of documents that included a summary of the FBI call. The documents revealed that a

hacker whose Twitter handle was @CyberZeist had compromised the Alaska Division of Elections on election day in 2016 by compromising the web application. He used privilege escalation to access the server's file system, and posted a screen shot from the system's election results as proof that he was able to access administrative areas of the server. The message also indicated the ballot administrator's password had been compromised.

CyberZeist had a reputation for cyber hacking and had an Indian IP address. Hursti felt like a proper investigation had not been performed and "the whole thing was brushed over." Through Twitter, the movie crew was able to find CyberZeist and filmed several communications they had with him. Initially, Hursti did not trust him, but later concluded that he was indeed behind the Alaskan hack.

CyberZeist said he entered a "certain kind of instructions" in the username and password logon fields that produced an error which provided the details of what was installed in the election database. He was able to access every user account and password, even administrator credentials. In the film, CyberZeist says, "I had root access, which not only allowed me to make small changes, but granted me full access of the system." He was able to access the GEMS (Global Election Management System) system that held the live voting data of the 2016 U.S. presidential election. "I could have made any changes in the system...changes like deleting the candidate...I could alter any data, any vote," he explained. Ultimately, CyberZeist said he chose not to do anything within the system at that moment out of fear that he might get caught. He disclosed that he was aware of a Russian hacking group that was also actively scanning U.S. election systems and trying to change the vote.

Paper Ballots, Voting Machines & the Senate

Virtually all of the scientific and cybersecurity experts – including the National Academies of Science – who have studied vulnerabilities in the election process are advocating the use of paper ballots. In part, this is due to the vulnerabilities that are known to exist in the voting machines currently in use and, in part, it is due to the necessity of having a paper audit trail to validate elections. QR and bar codes can be hacked, optical scanners and touch screens do not have a paper trail, even the touch screen machines with side printers do not provide an adequate audit trail. In order to have a meaningful, auditable ballot, it needs to be a hand-marked paper ballot. Mail in ballots may be the perfect solution for 2020; any security issues are surely less than those in our current system.

The American Bar Association, which represents over 400,000 attorneys, recently adopted a Resolution that urges the U.S. Congress to enact legislation that would define federal standards for election systems software, infrastructure, and hardware used in the handling, storing, processing, or transmitting data for voter registration, vote tallying, voter polling, or the manufacturing, servicing, or writing of election parameters of voting machines and equipment.

The Resolution also calls for a security certification process for election systems and an analysis of the private sector's role in the election process, with recommendations of any functions that should be performed by government. The Resolution urges that federal funding be restricted to only those jurisdictions that:

- Comply with the NIST standards
- Use equipment that undergo annual comprehensive cybersecurity assessments
- Use only private sector vendors who also undergo cybersecurity assessments and make their reports available to election officials.

The ABA also urges Congress to require the deployment of machine-readable paper ballots.

The problem is...Senate Majority Leader Mitch McConnell refuses to bring election security bills to the floor to be voted on. Why? Well, perhaps because the current system has worked just fine for a politician in the White House.

Cybersecurity Best Practices & Standards Can Help

Election security problems will not get corrected overnight, but standing up a cybersecurity program for election systems that is in alignment with cybersecurity best practices and standards will be a big first step. Election officials should already be doing this, but most clearly are not. They are not only using equipment with vulnerabilities; their own networks and systems are vulnerable as well.

Election officials also should require election vendors to meet cybersecurity standards and best practices and conduct annual risk assessments of their program's maturity. This is what all businesses are supposed to do – manage third party risk; election officials should do the same. In addition, they should follow the lead of California and other jurisdictions and hire experts to test the security of their voting machines and equipment

and then demand that vendors close any vulnerabilities found. The findings of these tests should be shared among election officials around the country.

Legislation and other reforms are needed, but election officials can achieve these things through their own direction and in legal agreements with their election vendors. They should begin now and do as much as possible before November.

Exhibit 4

Kill Chain – HBO Documentary April 6, 2020

Kill Chain https://www.youtube.com/watch?v=3c8LMZ8UGd8

Exhibit 5

MEMO to the President

MEMO
To: President Donald J. Trump
From: A Grateful Trump Supporter
Re: PREVENTING MASS VOTER/ELECTION FRAUD THIS NOVEMBER USING FEDERAL LAW AS A SIMPLE SOLUTION

Dear Mr. President –

I cannot thank you enough for having the courage to straightforwardly oppose the Democrats and squishy Republicans (state and federal) latest attempt at massive voter/election fraud – using the coronavirus pandemic as an excuse to destroy our electoral system with mandatory mail-in balloting and ballot harvesting:

Donald J. Trump @realDonaldTrump · Apr 14
GET RID OF BALLOT HARVESTING, IT IS RAMPANT WITH FRAUD. THE USA MUST HAVE VOTER I.D., THE ONLY WAY TO GET AN HONEST COUNT!

As you are clearly aware, the single most critical issue for the General Election, November 2020, is Voter/Election Fraud, with such methods as "ballot harvesting" with massive fraudulent mail-in ballots of millions of illegal aliens *as well as probable cyber manipulation of actual vote totals via online access through porous election counting software which has been exposed in many articles and this link to The Economic War Room (videos and resources) both of these are key reasons that enabled the Dems to flip the House in 2018. This was the warm-up act for 2020.*

As you say, America must have Voter ID now. The question is how. I would like to respectfully suggest a simple way.

*Massive voter fraud can be prevented in 2020 by implementing a US federal law, signed by President Clinton in 1996 and never challenged: *The Illegal Immigration Reform and Immigrant Responsibility Act of 1996* (IIRIRA: https://www.congress.gov/104/crpt/hrpt828/CRPT-104hrpt828.pdf), which has this provision:

> *"§ 611. Voting by aliens: (a) It shall be unlawful for any alien to vote in any election held solely or in part for the purpose of electing a candidate for the office of President, Vice President, Presidential elector, Member of the Senate, Member of the House of Representatives, Delegate from the District of Columbia, or Resident Commissioner"*

This provision of the IIRIRA has never been fully *implemented*. There is a clear legal way to *implement* the IIRIRA regarding the prevention of non-US citizens voting in a federal election:

*The Real ID Act, a federal law that sets forth requirements for state driver's licenses and ID cards to be accepted by the federal government for "official purposes", as defined by the Secretary of Homeland Security. Among them are a photo of the card holder and documented proof of US citizenship or legal status in the US.

The Real ID Act – Public Law 109-13 Title II Section 201 (3) – gives carte blanche to the DHS secretary to specify an "official purpose" for which this ID is required.

As the DHS website states:

> *"Starting October 1, 2020, every state and territory resident will need to present a REAL ID compliant license/ID, or another acceptable form of identification, for accessing Federal facilities, entering nuclear power plants, and boarding commercial aircraft. This is what we call 'card-based' enforcement. The card, itself, must be REAL ID compliant unless the resident is using an alternative acceptable document such as a passport."*

The key is what constitutes an "official purpose" for which a Real ID proof of citizenship is required. The Real ID Act – Public Law 109-13 Title II Section 201 (3) – gives this definition:

> *"Official purpose. The term 'official purpose' includes but is not limited to accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine."*

That is, at your direction, Mr. President, the Secretary of Homeland Security *has unlimited legal authority to require "federal identification" for whatever is deemed an "official purpose."*

Such as voting in a federal election – from which non-US citizens are prohibited per the IIRIRA.

With voting in a federal election as an official purpose under Real ID law, all those drivers' licenses for illegals that Blue states are issuing as end runs around Real ID would be invalid for voting in November 2020. All the ballot-harvesting and mail-in fraud ends.

*Preserving the honesty and integrity of our elections is a clear matter of national security, recognized by your predecessor and his DHS Secretary in designating the US election system as part of our nation's critical infrastructure: https://www.eac.gov/election-officials/elections-critical-infrastructure.

In sum, Mr. President, as a matter of national security, please **reimplement the October 1, 2020 Real ID Enforcement Deadline**, and **specify that voting in a federal election is an official purpose of the Real ID Act**, in compliance with the IIRIRA.

When challenged in federal court – this can be quickly resolved by a SCOTUS decision for federal law is undeniably on your side. It is against federal law for non-citizens to vote in a federal election. [Note: Since non-citizens here legally may get a Real ID card, it would be necessary to issue them a non-voting version of the card.]

*DHS Acting Secretary Wolf recently (February 20, 2020) cited both the IIRIRA and Real ID Act as his authority to expedite building sections of the Southern Border Wall:
https://www.federalregister.gov/documents/2020/02/20/2020-03452/determination-pursuant-to-section-102-of-the-illegal-immigration-reform-and-immigrant-responsibility.

*Speaker Pelosi attempted to federally mandate ballot harvesting nationwide in her failed stimulus bill:
https://www.breitbart.com/2020-election/2020/03/23/pelosi-stimulus-bill-imposes-nationwide-ballot-harvesting-without-any-limit/. Now she is making the same attempt for the second stimulus bill:
https://www.breitbart.com/politics/2020/03/31/house-democrats-pushing-for-mail-in-voting-as-part-of-next-stimulus/

These attempts clearly expose her and the Democrats' #1 goal of allowing the tens of millions of illegal aliens now in the US to vote in 2020. Blue states are now giving illegal aliens driver's licenses and registering them to vote at DMV offices. Using the Coronavirus Panic as an excuse for vastly expanding mail-in voting is part of this clear effort. *This is further compounded by new ballot marking devices, the porous election counting software which was developed and managed by a non-US company see this link on The Economic War Room (videos and resources).*

The outcome of November is simple: If massive Democrat voter fraud is prevented, President Trump will win reelection. If it is not, he will not. With the latter, voter fraud will be permanently institutionalized by the Democrats as Pelosi has demonstrated, we will never have an honest election ever again, and American democracy dies.

Mr. President, I firmly believe that the future of freedom in America is at stake this November. That your winning reelection will preserve it, that your losing reelection will doom it. That you will win if the election is honest, that you will lose if it is fraudulent. That it is clearly within your legal authority to prevent the massive illegal alien and mail-in voter fraud being planned by the Democrats. That if you do not exercise this legal authority your re-election and America's future are in grave danger.

Thank you for your consideration in this matter, Sir. It is with extraordinary gratitude for all that you have done and continue to do for our country that I write this.

A Grateful Trump Supporter – April 15, 2020 *(Italic comments on Cyber Election Fraud added to tell the whole story)*

Exhibit 6

Election Fraud Battle Plan

NEW LANDING PAGE ***(additional will be added as we continue the effort)***

https://www.economicwarroom.com/myvote

Election Fraud – Our Democracy is Under Threat and It Impacts Your Money, Your Livelihood and Your Way of Life

1. This landing page opens with our 2019 Update Video on Kentucky Governor's Race
   Additional videos:
   2016 What Happened?
   2018 Update "Blue Wave?
   2020 Update New Devices – Ballot Marking Devices – The New False Flag – 11 Ways for Fraud.

2. You can download the FREE Economic Battle Plan™

3. You can download the FREE Resource Guide with Links to Videos and Articles

The EWR Collection Deck – From Kevin Freeman

(List of resources and external links for more information)

Quick Access Links

[ ] - Must Read/Watch

HOT TOPICS

1. **Forbes - Kill Chain - Election Fraud Documentary Review**
2. **Western Journal – April 28 – Experts Speak Out**
3. **Memo to President - April 15 –regarding real ID - A solution for voter fraud**
4. **EWR video - 12 min - Kentucky update**

Where to Access Economic War Room

On BlazeTV
https://get.blazetv.com/economic-war-room/

Our Website
https://www.economicwarroom.com/

Our Facebook page
https://www.facebook.com/economicwarroom/

Our Twitter page
https://twitter.com/economicwarroom

Our YouTube page
https://www.youtube.com/channel/UCfsphUgquqFcp7D_NDe6J_A/videos

Our XOTV Channel
https://xotv.me/channels/233-economic-war-room

Link to all Battle Plans
https://www.economicwarroom.com/battleplans

Does Voter Fraud Really Exist?

[ ] Election Fraud Cases from Across the United States https://www.heritage.org/voterfraud

The Only Misleading Claim About Voter Fraud: 'It Doesn't Exist'
https://amac.us/misleading-claim-voter-fraud-doesnt-exist/

The Battle of Athens https://www.americanheritage.com/content/battle-athens

The Battle of Athens – When WWII Veterans stood up to the corrupt Local Government in Tennessee
https://www.warhistoryonline.com/instant-articles/battle-athens-group.html

[ ] Where Were You During the Battle of Athens?
http://www.nbcnews.com/id/14138208/ns/us_news-life/t/where-were-you-during-battle-athens/#.XFIU8C2ZMII

Serious vote fraud uncovered in key battleground state
https://www.wnd.com/2019/12/vote-fraud-uncovered-key-battleground-state/

[ ] Report Flags Issues With 24,000 Voter Registrations in Single Florida County
https://www.theepochtimes.com/report-flags-issues-with-24000-voter-registrations-in-single-florida-county_3143272.html

Michigan Election Official Charged With Six Felony Counts of Voter Fraud
https://theepochtimes.com/michigan-election-official-charged-with-six-felony-counts-voter-fraud_3098194.html

Heritage Foundation Explains Voter Fraud
https://www.heritage.org/election-integrity/heritage-explains/voter-fraud

Al Franken May Have Won His Senate Seat Through Voter Fraud
https://www.usnews.com/opinion/blogs/peter-roff/2010/07/20/al-franken-may-have-won-his-senate-seat-through-voter-fraud

[ ] Felons for Franken
https://www.wsj.com/articles/SB10001424052748704518904575365063352229680

Nevada voting machines automatically checking Harry Reid's name; voting machine technicians are SEIU members
https://www.washingtonexaminer.com/nevada-voting-machines-automatically-checking-harry-reids-name-voting-machine-technicians-are-seiu-members

Voting Fraud In The 'Banana Republic Of Kalifornia' Is A Huge Warning To America: If Democrats Get Their Wishes, This Method Of Stealing Elections Is Coming To A State Near You!
http://allnewspipeline.com/The_Banana_Republic_Of_Kalifornia.php

Election fraud scheme on L.A.'s skid row got homeless to sign fake names for cigarettes and cash, D.A. says
https://www.sandiegouniontribune.com/news/california/la-me-ln-skid-row-voter-fraud-20181120-story.html

[ ] How Johnson Won Election He'd Lost
https://www.nytimes.com/1990/02/11/us/how-johnson-won-election-he-d-lost.html

How 'Landslide Johnson' stole a win in Texas
https://www.montgomeryadvertiser.com/story/news/local/progress-opinion/2016/02/02/how-landslide-johnson-stole-win-texas/79691404/

The Mystery of Ballot Box 13
https://www.washingtonpost.com/archive/entertainment/books/1990/03/04/the-mystery-of-ballot-box-13/70206359-8543-48e3-9ce2-f3c4fdf6da3d

Sharron's Angle: Harry stole election
https://www.politico.com/story/2011/06/sharrons-angle-harry-stole-election-056698

Nevada Senate: Final Polls
https://www.realclearpolitics.com/epolls/2010/senate/nv/nevada_senate_angle_vs_reid-1517.html

[ ] Shock Claim: Florida County Has 'Thousands' of Voters Over Age 100
http://archive.is/HYJzi#selection-697.0-697.66

Records: Too many votes in 37% of Detroit's precincts
https://www.detroitnews.com/story/news/politics/2016/12/12/records-many-votes-detroits-precincts/95363314/

Ghost Voters
https://www.nationalreview.com/2017/08/election-fraud-registered-voters-outnumber-eligible-voters-462-counties/

Chicago reported thousands more votes than voters in 2016, GOP official says
https://www.foxnews.com/politics/chicago-reported-thousands-more-votes-than-voters-in-2016-gop-official-says

America may have 3.5 million more voters than eligible adult citizens
https://www.dallasnews.com/opinion/commentary/2017/08/11/america-may-35-million-voters-eligible-adult-citizens

[ ] U.S. Has 3.5 Million More Registered Voters Than Live Adults – A Red Flag For Electoral Fraud
https://www.investors.com/politics/editorials/u-s-has-3-5-million-more-registered-voters-than-live-adults-a-red-flag-for-electoral-fraud/

ORANGE COUNTY VOTE COUNT SUGGESTS FRAUD
https://www.wnd.com/2018/11/orange-county-vote-count-suggests-fraud/

[ ] Illegal immigrants use Motor Voter to get on rolls, can't be removed
https://www.washingtontimes.com/news/2018/sep/3/illegal-immigrants-use-motor-voter-get-rolls-cant-/

2 Investigators: Chicago Voters Cast Ballots From Beyond The Grave
https://chicago.cbslocal.com/2016/10/27/2-investigators-chicago-voters-cast-ballots-from-beyond-the-grave/

Can Elections Be Hacked?

[ ] Cyber Experts Warn of Major Election Vulnerabilities Going into 2020
https://www.westernjournal.com/cyber-experts-warn-major-election-vulnerabilities-going-2020/

[ ] Kill Chain: The Cyber War on America's Elections | Full Documentary
https://www.youtube.com/watch?v=3c8LMZ8UGd8

[ ] Hacks, Security Gaps And Oligarchs: The Business Of Voting Comes Under Scrutiny
https://www.npr.org/2018/09/21/649535367/hacks-security-gaps-and-oligarchs-the-business-of-voting-comes-under-scrutiny

How We Can Safeguard Our Election Process
https://amac.us/how-we-can-safeguard-our-election-process/

America Can We Talk with Debbie Georgatos Interviews Russ Ramsland
https://www.youtube.com/watch?v=JiuaZlPqlW4&t=1s

Los Angeles County to Introduce VSAP E-Voting System: NOT Hand-Marked, NOT Paper, NOT Hand-Counted in Public
https://www.nakedcapitalism.com/2019/11/los-angeles-county-to-intoduce-vsap-e-voting-system-not-hand-marked-not-paper-not-hand-counted-in-public.html

Election Fraud on a National Scale?
https://www.americanthinker.com/articles/2019/11/election_fraud_on_a_national_scale.html

[ ] Democrats Accuse Conservatives
https://medium.com/(b) (6) /updated-attachment-states-have-bought-voting-machines-from-vendors-controlled-and-funded-by-nation-6597e4dd3e70

Others Accuse Soros
https://www.lifezette.com/2016/10/concern-grows-over-soros-linked-voting-machines/

Hackers break into voting machines within 2 hours at Defcon
https://www.cbsnews.com/news/hackers-break-into-voting-machines-defcon-las-vegas/

YOUR VOTE COUNTS. BUT HOW DOES YOUR BALLOT GET COUNTED?
https://www.wired.com/2016/11/vote-counts-ballot-get-counted/

Private Equity Controls the Gatekeepers of American Democracy
https://www.bloomberg.com/news/articles/2018-11-03/private-equity-controls-the-gatekeepers-of-american-democracy

[ ] Kids at hacking conference show how easily US elections could be sabotaged
https://www.theguardian.com/technology/2018/aug/22/us-elections-hacking-voting-machines-def-con

There's more than one way to hack an election
https://www.axios.com/be-smart-there-is-more-than-one-way-to-hack-an-election-1529424861-1e0c75d9-32b8-4a85-98b3-47d5a853fdeb.html

Nielsen: Election officials don't have necessary security clearances
https://www.axios.com/how-secure-are-us-elections-nielsen-state-local-officials-security-clearances-jeh-johnson-eb68ecff-add4-4047-80cd-6df9cb56b6ed.html

Can the elections get hacked?
https://us.norton.com/internetsecurity-privacy-can-the-elections-get-hacked.html

Voting machine vendors under pressure
https://www.politico.com/newsletters/morning-cybersecurity/2018/07/12/voting-machine-vendors-under-pressure-277054

[ ] If the 2018 Election Is Hacked, This Is How It Will Happen
https://www.popularmechanics.com/technology/security/a24666436/2018-midterm-election-hacking/

Voting Machine Used in Half of U.S. Is Vulnerable to Attack, Report Finds
https://www.wsj.com/articles/widely-used-election-systems-are-vulnerable-to-attack-report-finds-1538020802

Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States
https://motherboard.vice.com/en_us/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states

Leading voting machine company admits it lied
https://boingboing.net/2018/07/18/election-systems-and-software.html

[ ] ELECTION HACKING: VOTING-MACHINE SUPPLIER ADMITS IT USED HACKABLE SOFTWARE DESPITE PAST DENIALS
https://www.newsweek.com/election-hacking-voting-machines-software-1028948

Washington, Silicon Valley Struggle to Unify on Protecting Elections
https://www.wsj.com/articles/washington-silicon-valley-struggle-to-unify-on-protecting-elections-11568392455

Election machine keys are on the Internet, hackers say
https://www.foxnews.com/tech/i-have-the-keys-to-your-voting-machine-probably

Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials
https://www.vice.com/en_us/article/3kxzk9/exclusive-critical-us-election-systems-have-been-left-exposed-online-despite-official-denials

[ ] 10,000 polling sites could be hacked because they use Windows 7: report
https://nypost.com/2019/07/14/10000-polling-sites-could-be-hacked-because-they-use-windows-7-report/

AP Exclusive: New election systems use vulnerable software
https://apnews.com/e5e070c31f3c497fa9e6875f426ccde1

Switzerland's e-voting system source code leaked ahead of its bug bounty program; slammed for being 'poorly constructed'
https://securityboulevard.com/2019/02/switzerlands-e-voting-system-source-code-leaked-ahead-of-its-bug-bounty-program-slammed-for-being-poorly-constructed/

[ ] Researchers Find Critical Backdoor in Swiss Online Voting System
https://www.vice.com/en_us/article/zmakk3/researchers-find-critical-backdoor-in-swiss-online-voting-system

'They think they are above the law': the firms that own America's voting system
https://www.theguardian.com/us-news/2019/apr/22/us-voting-machine-private-companies-voter-registration

Insider 'Backdoor' Found in 'Hack Test' of Vaunted Swiss Internet Vote System: 'BradCast' 3/22/2019
https://www.dailykos.com/stories/2019/3/22/1844382/-Insider-Backdoor-Found-in-Hack-Test-of-Vaunted-Swiss-Internet-Vote-System-BradCast-3-22-2019

Who Might Try to Hack Our Election?

[ ] Trump re-election campaign targeted by Iran-linked hackers: sources
https://www.reuters.com/article/us-cybersecurity-iran-exclusive/trump-re-election-campaign-targeted-by-iran-linked-hackers-sources-idUSKBN1WJ1ZM

Beijing's Online Manipulation and Interference During the Election
https://theepochtimes.com/beijings-online-manipulation-and-interference-during-election_3101962.html

[ ] Exclusive: U.S. officials fear ransomware attack against 2020 election
https://www.reuters.com/article/us-usa-cyber-election-exclusive/exclusive-u-s-officials-fear-ransomware-attack-against-2020-election-idUSKCN1VG222

New US Bill Calls Attention to China's Meddling in Upcoming Taiwan Elections
https://theepochtimes.com/new-us-bill-calls-attention-to-chinas-meddling-in-upcoming-taiwan-elections_2986816.html

Hackers will be the weapon of choice for governments in 2020
https://www.technologyreview.com/s/614974/hackers-will-be-the-weapon-of-choice-for-governments-in-2020/

[ ] Election hackers likely targeted 50 states in 2016. The states will be watching this time around.
https://www.technologyreview.com/s/614019/election-hackers-targeted-50-states-in-2016-the-states-will-be-watching-this-time-around/

Democrats Accuse Conservatives regarding Voting Machines
https://medium.com/(b) (6) /updated-attachment-states-have-bought-voting-machines-from-vendors-controlled-and-funded-by-nation-6597e4dd3e70

Soros Linked Voting Machines?
https://www.lifezette.com/2016/10/concern-grows-over-soros-linked-voting-machines/

Possible Solutions

[ ] Commentary: Auditable Paper Trails for Electronic Voting Machines Secure Our Votes
https://texasscorecard.com/commentary/commentary-auditable-paper-trails-for-electronic-voting-machines-secure-our-votes/

[ ] America Needs Paper-Based Ballots for the 2020 Election—Cyber Saturday
https://fortune.com/2019/08/10/america-needs-paper-based-ballots-for-the-2020-election-cyber-saturday/

[ ] A professor at MIT demonstrated just how easy it is to tamper with voting machines – but there's a fairly simple way to prevent it from happening
https://www.businessinsider.com/hacking-voting-machines-and-how-to-stop-it-2018-9

[ ] Report outlines keys to election security
http://news.mit.edu/2018/report-keys-election-security-0925

Note: The Economic Battle Plan™ contains hyperlinks to other Internet sites not under the editorial control of EWR-Media Holdings, LLC. These hyperlinks are not express or implied endorsements or approvals by EWR-Media Holdings, LLC, of any products, services or information available from these 3rd party sites. Links to these 3rd party sites are open source links that may require subscription or registration.

Shareable Quote:

"It's not the people who vote that count, it's the people who count the votes."

–attributed to Joseph Stalin

CONFIDENTIAL SUMMARY REPORT OF

DALLAS COUNTY, TEXAS

ELECTION IRREGULARITIES,

MANIPULATIONS AND MASSIVE SECURITY BREACHES

INVOLVING MAJOR INTERNATIONAL ELECTRONIC VOTING FIRMS

DOCUMENTED ISSUES WITH DALLAS COUNTY ELECTIONS ELECTIONS FRAUD AND DISCOVERY OF "ACHILLES HEEL" IN "SECURE" ELECTRONIC ELECTIONS SYSTEMS USED EXTENSIVELY IN U.S. ELECTIONS

The following narrative and bulletized summaries are a distillation of a collection of documented facts consisting of official voting records, public records, sworn statements of poll watchers, expert computer-based investigations and analysis, voter and voting data files, white papers, and information located on corporate and journalist internet publications which revealed outrageous vote processing abuses and mind-numbing stored data security breaches affecting tens of millions of voters in more than a dozen major U.S. states.

The evidence presented in these summaries reveals and documents a disturbing set of systemic problems with the complex electronic voting systems utilized in Dallas County, Texas, the large international companies that produce and market voting software, hardware, voting data processing and storage, and the governmental officials who are charged with selecting, securing, overseeing and operating those systems. Those problems are emblematic of the deep-seated, unresolved flaws and conflicts inherent in the DNA of electronic voting systems and their use in the political decision-making process. Those problems and the quest to imbed electronic voting systems through a global set of government-private industry partnerships threaten the integrity of the voting process and security of the democratic foundations of the United States and other countries.

The core subject of this report is electronic voting software and systems and their misuse. It is a complex topic on which there is extensive debate and little in-depth knowledge outside the realm of industry insiders, computer scientists and hackers. This general lack of knowledge about electronic voting systems is due in large part to the "trade secret" protections staunchly embraced by electronic voting companies and public deference to the quirks of computing science. Proponents of electronic voting argue it is secure, faster to deliver accurate voting results, and is the key to extending voting participation. Their opponents counter that a computerized voting system has to balance a range of important features, including security, authenticity and prevention of manipulating results, but that the "black box" nature of the technology obscures the risks and flaws from politically selected decision-makers.[1]

These flaws – well known and extensively documented by industry experts – are not simply academic. Unfortunately, they came to the attention of concerned citizens in the aftermath of the "Blue Wave" which rolled across the political

[1] *See, e.g.,* https://www.comparitech.com/blog/information-security/electronic-voting-risks/

landscape of Dallas County, Texas in the 2018 General Election. That "wave" swept away a complete slate of elected Republicans ranging from an 11-term Congressman to veteran state representatives and local trial and appellate judges. Beyond the loss itself, many experienced political observers were amazed by the breadth of the sizeable margin of victory for many Democratic neophyte candidates in "safe" Republican precincts – margins that defied time-proven pre-election polling results and conventional methods of post-election vote contesting.

In the aftermath, many voters – both Republican and Democrat, experienced poll watchers, politicos, and voting fraud investigators, suspected that something was amiss. Polls of usually reliable pollsters had placed a 11-term Republican U.S. Congressman from the 32nd Congressional District in a comfortable lead against an inexperienced, relatively unknown candidate. Other incumbent Republican candidates in normally "safe" districts with favorable pre-election polls and positive voter feedback questioned their losses.

Early voting – conducted using electronic voting machines – has historically been a consistent stronghold of Republicans for decades. In the 2018 General Election, Republicans lost the Early Vote by large margins for the first time in many decades.

Attention of the Dallas GOP focused on irregularities with the handling of ballots at the Central Counting Station of the Dallas County Election Department ("DCED"). During Early Voting tabulation, experienced poll watchers encountered significant delays, diversions and obstructions to their observing election vote tabulation activities by election officials and personnel from voting systems vendor Electronic Software & Systems, Inc. ("ES&S") personnel. These official observers noted the absence of election officials as voting data cards were removed from sealed pouches and read into the central computer "accumulator." They challenged election officials' failure to administer the required oath to ES&S personnel and succeeded in their challenge despite grudging resistance from at least one ES&S employee. They witnessed an ES&S voting technician's repeated entry of vote counting information into a "personal" laptop computer, connection of that laptop to a live wireless "hotspot" and transmission of information over the hotspot during vote counting activities. They also observed his daily removal of the laptop from the Central Counting area and his return of that laptop on following days. The witnesses watched as the ES&S technician casually overrode countless system error messages with obtaining election official approval. Each of these instances alerted poll watchers to the realization that election officials and ES&S personnel had no intention of following protocols and procedures required by the Texas Election Code and were bent on hiding their activities from the scrutiny of poll watchers.

Following the election, it took more than a week to get a summary report of the unofficial results from DCED officials and two weeks to get a mandatory printout of the ES&S electronic voting system log detailing the voting system computer processes for the entire vote counting process, which took place from October 25, 2018 through November 6, 2018.

The vote processing log and reported election results revealed that the Early Vote results for "Straight Party" tickets contained a massive "under vote" of nearly 152,000 vote – something experts opined was extraordinary and called into question the tabulation accuracy. Expert examination of the computer logs revealed that thousands of error codes for "Time stamp mismatch" and Votes exceed ballots" were overridden by the ES&S technician. The logs confirmed that Early Voting data stored on hundreds of compact flash memory cards was read into the ES&S "Accumulator" computer, then "cleared" and re-entered four (4) times on Election Day. The log also revealed that on Election Day, votes were "REPLACED" for 25 of the 215 Dallas County precincts voting on the 32nd Congressional District race, and multiple error messages of "Precinct already update" and "Votes exceed ballots" appeared for the same precincts.

Detailed written complaints regarding the election vote processing problems were delivered to the Texas Attorney General and Federal Bureau of Investigation. Each agency assembled a team of voting fraud experts, listened to a presentation of the facts, registered concern, and promised to conduct an investigation.

In February 2019, both agencies received a private sector confidential forensic report authored by a team of former federal investigators with electronic surveillance and security backgrounds. That report revealed that the private investigators had discovered a treasure trove of *unsecured* "open source" voter and voting data by tracing links from a DCED website to an internet site owned by clarityelections.com and serviced by Amazon Web Services ("AWS") in Virginia. Encountering no security obstacles or challenges to their search, the investigative team found files with administrative names and passwords for critical information, perused a massive set of digitized voter registration lists containing personally identifiable information for 1.3+ Million Dallas County voters and the precinct where they voted, all previous voting uploads, all election software source code, all electronic ballots for Dallas County (including future ballots), all counting and tallying functions, and total access to the voting companies' entire AWS database. That database included personally identifiable information for tens of millions of voters from other states. Most importantly, the investigators were shocked to find coded instructions for automatic forwarding of data from the AWS clarityelections.com site to other domestic and foreign Domain Name Registrations (DNS addresses) for sites in England, Spain, and Russia.

Remarkably, the FBI and Texas Attorney General failed to interview identified witnesses, ignored the report, and quietly shelved their inquiries.

This report is the first of a series of reports regarding voting irregularities and DCED election officials' misconduct preceding and during elections. The authors are preparing additional reports concerning election issues with a May 2019 $1.1 Billion Dallas County Community College District bond election and the 2020 Super Tuesday primary. Notably, litigation contesting the bond election has revealed covert destruction of the ES&S equipment, software, and data storage devices used in the 2018 Primary and General Election in mid-July 2019. Texas law requires maintenance of all election records for federal elections for a period of 22 months.

1. **Dallas County Elections Systems and Data Entrusted to World's Largest Electronic Voting Processing Software and Systems Companies.**

A. Dallas County and its Dallas County Elections Department ("DCED") have contracted with Elections Software & Systems, Inc. ("ES&S") for more than 20 years.

i. ES&S is an Omaha, Nebraska-based company that manufactures and sells voting machine equipment and services. Its offerings include vote tabulators, direct-recording electronic (DRE) machines, voter registration and election management systems, ballot-marking devices, electronic poll books, Ballot on Demand printing services, and absentee voting-by-mail services. ES&S is the successor to a long series of predecessors. In June 2019, ES&S was purchased by Government Systems, Software, & Services, Inc., a privately owned subsidiary of McCarthy Group, LLC.[2]

ii. In May 2011, ES&S and a company named Scytl signed an agreement to jointly market solutions for military and overseas voters in the United States. The two companies partnered with the Virginia Board of Elections. In a 2012 *Businesswire* article, the two companies touted their credentials: "Scytl is a worldwide leader in the development of secure technology solutions for the modernization of elections. The company's solutions incorporate unique cryptographic protocols that enable Scytl to carry out a variety of election processes in a completely secure and auditable manner." "Election Systems & Software, LLC. (ES&S) is the world's largest and most experienced provider of total election management solutions. For nearly 40 years, ES&S — as a company solely focused on elections and the leader in its industry — has grown to support a customer base of more than 4,372 jurisdictions throughout the world, and more than 290,000 election systems installed worldwide."[3] [Emphasis added]

iii. By 2014, ES&S was the largest manufacturer of voting machines in the United States, claiming customers in 4,500 localities in 42 states and two U.S. territories. As of 2014, the company had more than 450 employees, more than 200 of whom are located in Omaha. That year, ES&S claimed that "in the past decade alone," it had

[2] *See* Wikipedia report on ES&S at https://en.wikipedia.org/wiki/Election_Systems_%26_Software.

[3] https://www.businesswire.com/news/home/20120328005562/en/Voting-Technology-Leaders-Scytl-Election-Systems-Software

installed more than 260,000 voting systems, more than 15,000 electronic poll books, provided services to more than 75,000 elections. The company has installed statewide electronic voting systems in Alabama, Arkansas, Georgia, Idaho, Iowa, Maine, Maryland, Minnesota, Mississippi, Montana, Nebraska, New Mexico, North Carolina, North Dakota, Rhode Island, South Carolina, South Dakota, and West Virginia. ES&S claims a U.S. market share of more than 60 percent in customer voting system installations.[4]

B. ES&S and Spanish Company Scytl Have Partnered And Dominate the World Market for Electronic Voting Software, Equipment, Data Storage and Election Night Reporting.

i. Scytl a multi-national corporation headquartered in Barcelona, Spain. Scytl's website touts the firm as the world's largest voting processor and election night reporter. It lists a clientele of 28 countries in Europe, the USA, Latin America, Asia Pacific and India, Africa, Middle East, and EU.[5]

ii. Scytl is run by European executives and reportedly is connected financially with Soros-owned entities. In 2014 Microsoft co-founder billionaire Paul Allen's Vulcan Capital invested $40 Million in Scytl.[6]

iii. Over the last two decades, Scytl has acquired or established collaborative relationships with the world's leading biometric security, cryptographic security, predictive analytics, vote processing, vote delivery, vote reporting, and mobile technology firms.[7]

iv. In January 2012, Scytl acquired all assets of SOE Software, a Florida company. At that time, SOE Software was the largest voting machine and software vendor in USA. As part of its acquisition, Scytl acquired the trade name "Clarity Elections."

---

[4] *See* https://en.wikipedia.org/wiki/Election_Systems_%26_Software

[5] https://www.scytl.com/en/election-night-reporting/

[6] *See* https://www.osetfoundation.org/blog/2014/4/10/money-shot-what-does-a-40m-bet-on-scytl-mean

[7] https://www.thenewamerican.com/usnews/item/16724-soros-connected-vote-counting-firm-expands-in-u-s. *See also*, https://www.scytl.com/en/company-overview/ ; https://www.scytl.com/en/scytl-acquires-soe-the-leading-election-software-company-in-the-united-states/ ; and https://freepress.org/article/scytl-has-all-tools-it-needs-election-fraud.

Subsequent to its acquisition of SOE Software, Scytl rebranded its U.S. operations under the name "Clarity" and established a data processing web domain under the name "clarityelections.com."

v. Presently, clarityelections.com is a large data repository and clearing house for voter and elections data originating from USA states that include counties in Arkansas, Georgia, California, Colorado, Illinois, Iowa, Georgia, Louisiana, Kentucky, New Jersey, Texas, and South Carolina.[8] The clarityelections.com domain maintains its clients' voter and election data in an *unsecured condition* on an Amazon Web Service ("AWS") web server in Virginia.

vi. In 2018, Scytl U.S. supported elections in 12+ states, 900+ jurisdictions involving 70+ Million registered voters.[9]

vii. Scytl touts its involvement in the following election service area: election training, electronic pollbooks, online voting, results consolidation, and election night reporting.[10]

2. Dallas County Elections Are Processed by ES&S and Dallas County Voter and Voting Data Is Maintained *Unsecured* on the Scytl clarityelections.com web server.

A. The DCED website https://www.dallascountyvotes.org/ contains Dallas County voting and elections information links that pull data specific to Dallas County voters and elections that is processed in Scytl servers in Barcelona, Spain and routed through the Scytl clarityelections.com web server in Virginia.

B. Critical voter and vote results data pertaining to the Dallas County 2018 Democratic Primary and General Elections, a 2019 Bond Election, and the 2020 Dallas County General Elections is maintained in unsecured data files on the clarityelections.com domain and processed through Scytl's Barcelona server.

C. Dallas County Voter ID rolls containing 1.3+ Million Dallas County voters' address, phone number, Texas driver license number and social

[8] This listing is based upon actual viewing of files on the clarityelections.com website. Files of other states have not been downloaded in connection with this matter. See ¶1.A,iii above.

[9] Source: https://scytl.us/about-us/

[10] Source: https://cloudblogs.microsoft.com/industry-blog/government/2017/04/26/scytl-microsoft-digitally-transforming-elections/

security number are maintained in unsecured open source files stored on the clarityelections.com domain. This information is retrieved by each Dallas County polling location over ES&S electronic "pollbooks" during an election and used for voter identification verification. It is unclear whether this information is processed by Scytl in Barcelona. *See* FN 9, *below*.

D. Poll worker information for each election is maintained in an unsecured file on the clarityelections.com domain. This information is available to Scytl in Barcelona.

E. Astoundingly, vote count data for Early Voting and Election Day voting for 2018, 2019, and 2020 elections is stored in unsecured open source files on the clarityelections.com domain. This information is available to Scytl in Barcelona.

F. Each of the data files detailed above is readily accessible without challenge to any domestic or foreign hacker.

3. Investigation Established Absence of Security for Critical Voting Data Stored on Unsecured clarityelections.com AWS Servers and Direction of Election Files to Multiple Domestic and Foreign Servers Over the Internet During 2018 and 2019 Elections.

A. Using legal hacking methods, former FBI and intel agency investigators discovered a clarityelctions.com server in Virginia has "open source" files for Dallas elections and contains identity of all Dallas County administrators, all passwords, all vote tabulating software source code and all voter and election data, including voter voting histories. [11]

B. The professional investigators confirmed that massive numbers of Dallas County and other U.S. counties' 2018 elections voter and voting records for the 2018 General Election was automatically forwarded from the clarityelections.com website to multiple domestic and foreign DNS addresses, including ES&S, Scytl in Barcelona, Smartmatic[12] in London, and a Russian server at South Ural State University in Chelyabinsk, a known GRU installation (https://uox.on.urc.ac.ru) [13]

---

[11] The clarityelections.com server also contained a massive number of voter and election files for counties in Alabama, California, Illinois, Louisiana, New Jersey, New York, and Texas. *See* Table 7.

[12] For wiki information concerning Smartmatic, see https://en.wikipedia.org/wiki/Smartmatic.

[13] *See* https://www.glassdoor.com/Overview/Working-at-Smartmatic-EI_IE119108.11,21.htm

C. Professional investigators also have found an Excel spreadsheet file containing algorithms for projecting voting results on an NGP Van website. NGP Van, formerly known as the Voter Acquisition Network, is the voter database and data analytics organization for the DNC. NGP Van works closely with Act Bleu and Shared Blue.[14]. The NGP Van Excel file was created by, and made available to, Democratic political operatives.

D. Professional investigators located and confirmed that data files stored on the clarityelections.com domain contain voting tabulation results that were contemporaneously modified during the Dallas County 2018 Democratic Primary and 2018 General Election. Those modified voting data files evidence changes in voting data that was used in final vote tabulations for the 2018 General Election. The voting data changes are highly consistent with results obtained through use of the NGP Van spreadsheet.

E. Investigators determined that all voting results on clarityelections.com are subject to real time manipulation to reflect a desired outcome. Investigators have concluded forensically that all of the tools necessary to manipulate voter data on the clarityelections.com server are readily available.

4. Documented Election Computer Logs Detail Extensive Anomalies and Skewed Results Raising Serious Questions of Vote Manipulation in Dallas County 2018 General Election.

A. After Absentee, Early Voting and Election Day votes were initially entered into the DCED Central Counting Station ES&S "Accumulator" tabulation computer server, the votes were then cleared by an ES&S technician with delegated authority and repeatedly replaced from data sources other than the original voting machine magnetic flash memory cards.

B. Thousands of "Time stamp mispatch" errors and "Votes exceed ballots" errors affecting 170,703 Early Votes results for a GOP incumbent congressional race (District 32) were recorded on computer logs and overridden by the ES&S technician without consultation with or

[14] Act Blue and Shared Blue have funneled over $1.5 Billion to Democratic candidacies by raising money from 8,000 registered donors and receiving hundreds of millions of dollars of cryptocurrency, Amazon "gift cards" and unverified credit cards which are processes through foreign merchant service companies.

oversight by election officials. This phenomenon was observed by poll watchers.[15]

C. Absentee votes were entered, tabulated, printed on paper reports, then "zeroed out" by a reset, then absentee data was reloaded.

D. Early Voting flash memory cards containing Early Voting votes were downloaded, results tabulated and printed. Then the data was "cleared" and "create[d]" again.

E. Election Day votes were received into the DCED Central Counting Station's "Accumulator" server and subsequently replaced for specific precincts.

F. Investigators determined that ES&S-tabulated 2018 E Dallas County 2018 General Election reported 227,033 *"Under votes"* for "Straight Party" Votes for Democrats and Republicans. Of these, 151,945 were Early Votes cast on digital display voting machines with no paper ballots.[16]

G. Hundreds of flash memory cards containing General Election Early Voting data repeatedly cleared and over-written, with messages indicating overvoting in certain precincts. *See* FN 8.

H. Election Day 2018 results in ES&S computer logs from scanned paper ballots document 96 instances of "*pack received*" and "*replaced by pack*."

I. Election Day 2019 results in ES&S computer log reported "*Votes Exceed Ballots, Precinct already updated*" messages affected 69 Congressional District 32 precincts and 101 State Senatorial precincts.

J. ES&S tabulation computer logs evidence modifications to remove lines of reported computer vote tabulation activities.[17]

---

[15] *See* Attachment 1, Affidavits of Sammy Bickham, Jr., Kristin J. Bickham, Kurt Hyde and Trust Elections, LLC. and Attachment 2, Affidavit of Laura A. Pressley,Ph.D. *See also* Tables 1 through 7, Source: Review of Early Voting Tabulations, Dallas County Central Counting Station, Investigative Report of Allied Special Operations Group, LLC.

[16] See Attachment 3, Summary Report Grp Detail, Unofficial Results, November 6, 2018 and Table 6, Review of Early Voting Tabulations, Dallas County Central Counting Station, Investigative Report of Allied Special Operations Group, LLC.

[17] Table 4, Source: Review of Early Voting Tabulations, Dallas County Central Counting Station,

K. Investigators report that comparison of 2018 General Election ES&S tabulation audit log error messages for Dallas and San Antonio illustrate that the error activity is not "normal." [18]

5. **2018 General Election: DCED Election Officials Failed to Comply With Mandatory Legal Requirements, Obstructed Poll Watchers, and Engaged in Suspicious Conduct.**

A. Mandatory Legal Requirements Not Met.

i. Testing required by Subsection D, §§127.91 et. seq., Texas Election Code, were not followed by DCDE officials.[19] [20]

ii. Poll watchers stationed in the Central Counting Station room during voting tabulations for the 2018 General Election reported an extensive number of activities not permitted by the Texas Elections Code.[21]

Investigative Report of Allied Special Operations Group, LLC.

[18] Table 5, Source: Review of Early Voting Tabulations, Dallas County Central Counting Station, Investigative Report of Allied Special Operations Group, LLC.

[19] Sec. 127.092 Testing Authorities. The programmer, tabulation supervisor, counting station manager, and presiding judge of the central counting station shall prepare and conduct the test jointly.

[20] Sec. 127.093 Times for Conducting Test. (a) The test shall be conducted three times for each election. (b) The first test shall be conducted at least 48 hours before the automatic tabulating equipment is used to count ballots voted in the election. (c) The second test shall be conducted immediately before the counting of ballots with the equipment begins. (d) The third test shall be conducted immediately after the counting of ballots with the equipment is completed.

[21] *See* Attachments 1 and 2.

STATE OF TEXAS §
§
COUNTIES OF Dallas, Denton and Williamson

AFFIDAVITS OF SAMMY BICKHAM, JR., KRISTEN J. BICKHAM, KURT HYDE, and TRUE TEXAS ELECTIONS, LLC

BEFORE ME, the undersigned authorities, personally appeared, and who being on their oath sworn, stated:

"My name is Sammy Bickham, Jr. and I am above the age of eighteen years, and I am fully competent to make this affidavit. My date of birth is (b) (6) I reside at (b) (6) , and I am a registered voter in Dallas County. My Unique Voter ID is (b) (6) I have not been convicted of a felony or a crime of moral turpitude. The following facts are within my personal knowledge and are true and correct."

"My name is Kristen J. Bickham and I am above the age of eighteen years, and I am fully competent to make this affidavit. My date of birth is (b) (6) I reside at (b) (6) and I am a registered voter in Dallas County. My Unique Voter ID is (b) (6) . I have not been convicted of a felony or a crime of moral turpitude. The following facts are within my personal knowledge and are true and correct."

"My name is Kurt Hyde and I am above the age of eighteen years, and I am fully competent to make this affidavit. My date of birth is (b) (6) . I reside at (b) (6) , and am a resident of Denton County. My Unique Voter ID is (b) (6) . I have not been convicted of a felony or a crime of moral turpitude. The following facts are within my personal knowledge and are true and correct."

"My name is Dr. Laura Pressley, owner of True Texas Elections, LLC, and I am above the age of eighteen years, and I am fully competent to make this affidavit. My date of birth is (b) (6) . I reside in (b) (6) , and I am a registered voter in Travis County. My Unique Voter ID is (b) (6) . I have not been convicted of a felony or a crime of moral turpitude. The following facts are within my personal knowledge and are true and correct."

Official Election Records for Dallas County Central March 6, 2018 Primary Show In 154 Precincts, Approximately 1,761 More Ballots Were Counted Than Voters

We have jointly prepared this affidavit and are submitting it pursuant to Chapter 273 of the Texas Election Code. As background, Mr. Sammy Bickham, Jr. and Mrs. Kristen J. Bickham were official

Central Counting Station Watchers for the 2018 Joint Primary in Dallas County[1,2,3] and obtained, from the Dallas County Elections Office:

1) Official Dallas County Central Counting Station Central Accumulator Audit Logs,[4,5]
2) 2018 Democratic Primary Canvassed Results[6]

Mr. Kurt Hyde obtained, through a Dallas County Elections Office open records request, obtained:

1) 2018 Dallas County Primary Voter Rolls,[7] and
2) Results Tapes of Polling Locations.[8]

Dr. Laura Pressley, Ph.D., founder of True Texas Elections, LLC, was contacted by Mr. and Mrs. Bickham and Mr. Hyde to have True Texas Elections assist with analyzing the above election records for what they believe to be potential vote counting discrepancies for the March 6, 2018 Democratic Primary.

Upon analysis and review, we believe that it appears when a comparison is made between the March 6, 2018 Dallas County Audit Logs and the Official 2018 Dallas County Vote Rolls, there are 1,761 more ballots counted than there were individuals that voted in 154 precincts combined for Early Voting, Ballot by Mail and Election Day.

The Texas Election Code Section 127.156 specifies if a discrepancy between voters and ballots cast at a precinct is more than 3, the official tabulation should occur at the central counting station.[9] We are reporting only those precincts that show more than 3 extra ballots. The value of 1,761 extra ballots is a conservative number.

---

[1] Mr. Sammy Bickham's March 6, 2018 Dallas County Primary Central Counting Station Watcher Appointment Form https://dk-media.s3.amazonaws.com/media/1m8vg/downloads/341739/Sammy_-_3-6-18_-_Official_Watcher_Appmt_Form.pdf and Affidavit of observations https://dk-media.s3.amazonaws.com/media/1m8vg/downloads/341741/_Final_Sammy_Bickham_Jr_3-6-2018Affidavit_-_Notarized.pdf

[2] Mrs. Kristen Bickham's March 6, 2018 Dallas County Primary Central Counting Station Watcher Appointment Form - https://dk-media.s3.amazonaws.com/media/1m8vg/downloads/341723/KB_Watcher_Form_3_6_2018.pdf

[3] Mrs. Kristen Bickham's 2018 Dallas County Central Counting Station Affidavit https://dk-media.s3.amazonaws.com/media/1m8vg/downloads/341740/_Final_Kristen_J._Bickham_-_Affidavit_-_Primary_Election_-_3-06-18.pdf

[4] March 6, 2018 Joint Primary Dallas County Central Counting Station Central Accumulator central counting station audit logs. Logs were received from Dallas County Elections Office pursuant to Texas Administrative Code 81.62.

[5] Dallas County Central Accumulator central counting station audit log - https://dk-media.s3.amazonaws.com/media/1m8vg/downloads/341749/Dallas_Audit_Log_March_2018_Primary_Combined_for_report.pdf

[6] March 6, 2018 Dallas County Official Canvass Results for Dallas County Democratic Party from Dallas County website http://results.enr.clarityelections.com/TX/Dallas/73695/193973/Web01/en/summary.html

[7] March 6, 2018 Dallas County Voter Rolls obtained from an open records request. https://dk-media.s3.amazonaws.com/media/1m8vg/downloads/341726/Dallas_County_Primary_Voters_2018_March_6th_from_Dallas_County.xls

[8] March 6, 2018 Dallas County Results Tapes received from open records request. https://dk-media.s3.amazonaws.com/media/1m8vg/downloads/341728/Dallas_March_6__2018_Election_Day_Results_Tape2.pdf

[9] **Sec. 127.156**. TABULATION AT CENTRAL COUNTING STATION IF DISCREPANCY EXISTS IN BALLOT TOTALS. If a discrepancy of more than three exists between the number of ballots recorded on the ballot and seal certificate and the number of ballots cast on the tape containing the ballot tabulation that is produced by the automatic tabulating equipment, the official tabulation of those ballots shall be conducted at a central counting station.

I. Election Day Discrepancies – Comparison of central accumulator audit logs and official Democratic Party voter rolls show 97 precincts have a discrepancy of 4 or more extra ballots reported on the audit logs than there were voters that were recorded on the official voter rolls. There is a total of 1,372 more ballots than voters for these 97 precincts. A representative sample of these precincts are noted below:

Precinct - Audit Log Ref	ED Ballots (Audit Logs)	ED Voters (Rolls)	ED Delta (Ballots > Names)
3806D-	229	63	166
4519D-	264	157	107
3311D-	132	41	91
2307D-	100	29	71
1713D-	91	23	68
3701D-	231	169	62
3807D-	229	171	58
4113D-	122	66	56
3702D-	99	60	39
3316D-	114	89	25
3600D-	115	91	24
1105D-	25	2	23
1107D-	37	14	23
1714D-	91	71	20
4032D-	200	183	17
4118D-	14	0	14
1302D-	81	68	13
3086D-	179	166	13
3608D-	296	283	13

II. Early Voting Discrepancies – Comparison of central accumulator audit logs and official Democratic Party voter rolls show 52 precincts have a discrepancy of 4 or more extra ballots reported on the audit logs than there were voters that were recorded on the official voter rolls. There is a total of 342 more ballots than voters or these 52 precincts. A representative sample of these precincts are noted below:

Precinct - Audit Log Ref	EV Ballots (Audit Logs)	EV Names (Rolls)	EV Delta (Ballots>Names)
2307D-	93	30	63
1013D-	146	134	12
3008D-	345	335	10
4628D-	61	52	9
1130D-	59	51	8
3920D-	33	25	8
2072D-	242	234	8
3053D-	121	113	8
4071D-	20	12	8
2031D-	150	143	7
3107D-	240	233	7
3314D-	202	195	7

III. Mail-In Discrepancies – Comparison of central accumulator audit logs and official Democratic Party voter rolls show 5 precincts have a discrepancy of 4 or more extra ballots reported on the audit logs

than there were voters that were recorded on the official voter rolls. There is a total of 47 more ballots than voters for these 5 precincts. A representative sample of these precincts are noted below:

Precinct - Audit Log Ref	BBM Canvass (Audit Logs)	BBM Names (Rolls)	BBM Delta (Ballots>Names)
1719D-	47	22	25
2307D-	11	1	10
4632D-	14	10	4
2041D-	53	49	4
1084D-	15	11	4

Chapter 33 of the Texas Penal Code[10] and Texas Election Code Sections 64.012[11], 276.003[12], 276.011[13], 276.013[14], specify that preventing lawfully cast votes from being counted is a crime. Also, the Texas Election Code, Section 273.001(a)[15] governs if an election in which potential criminal activity occurred, covers territory in more than one county - such as the Democratic Primary US Senate race - voters may present an affidavit to the attorney general, and the attorney general shall investigate the allegations. We are presenting this affidavit to the Texas Attorney General for an investigation.

Requests and Recommendations

The above concerns warrant an investigation by the Texas Attorney General's Office to determine if the vote tabulations for the Democratic Primary elections on March 6, 2018 were secure and that no legally cast votes were not prevented from being counted.

There are several election software forensic consultant experts that the Texas Attorney General may consider employing to perform a full technical analysis of the issues raised above: Hari Hursti, Dr. Dan Wallach of Department of Computer Security at Rice University, Dr. J. Alex Halderman Director, University of Michigan Center for Computer Security,

"Further affiants sayeth not."

---

[10] Texas Penal Code Chapter 33 - https://statutes.capitol.texas.gov/DocViewer.aspx?DocKey=PE%2fPE.33&Phrases=chapter%7c33&HighlightType=1&ExactPhrhttps://statutes.capitol.texas.gov/DocViewer.aspx?DocKey=PE%2fPE.33&Phrases=chapter%7c33&HighlightType=1&ExactPhrase=False&QueryText=chapter+33

[11] https://statutes.capitol.texas.gov/DocViewer.aspx?DocKey=EL%2fEL.64&Phrases=64.012&HighlightType=1&ExactPhrase=False&QueryText=64.012

[12] https://statutes.capitol.texas.gov/DocViewer.aspx?DocKey=EL%2fEL.276&Phrases=276.003&HighlightType=1&ExactPhrase=False&QueryText=276.003

[13] https://statutes.capitol.texas.gov/DocViewer.aspx?DocKey=EL%2fEL.276&Phrases=276.011&HighlightType=1&ExactPhrase=False&QueryText=276.011

[14] https://statutes.capitol.texas.gov/DocViewer.aspx?DocKey=EL%2fEL.276&Phrases=276.013&HighlightType=1&ExactPhrase=False&QueryText=276.013

[15] Sec. 273.001. INVESTIGATION OF CRIMINAL CONDUCT. (a) If two or more registered voters of the territory covered by an election present affidavits alleging criminal conduct in connection with the election to the county or district attorney having jurisdiction in that territory, the county or district attorney shall investigate the allegations. If the election covers territory in more than one county, the voters may present the affidavits to the attorney general, and the attorney general shall investigate the allegations.