TENNESSEE VOTERS FOR ELECTION INTEGRITY

ELECTION MACHINES CAN BE HACKED, SO GET RID OF THEM.
OR AT LEAST TAKE THEM THROUGH A SECURITY RISK EVALUATION BECAUSE
RECERTIFICATION IS SIMPLY CHECKING THE MATH.

Executive Summary

Electronic voting machines, at one time an amazing aid to counting the vote in an election, in many other ways have opened significant concerns about the possibility the voting process can be fraudulently abused during their use. There are numerous documents, videos, presentations and affidavits affirming this fact – which we will cite in this report. Removing some – if not all -- portions of the machine technology from the process, heavily inspecting the technology that remains both before and after each election and/or placing significant guardrails around the technology will be the only way for citizens to have renewed faith in the election experience.

Make no mistake, election machines CAN be hacked and are a danger to Tennessee's and the country's Constitutional Republic.

Following a January 2021 request from the Williamson County Election Commission (WCEC), the Tennessee State Election Commission (SEC) committed to recertify not only Dominion voting machines used in Williamson and Hamilton counties, but the other four brands used statewide as well – ES&S, Hart, MicroVote and UniSyn. Unfortunately, a year and a half later, nothing has been done on this and the issue has faded away. The SEC's promise to recertify the machines has been worthless.

Given all we now know about voting machines and their technologies – and the piles of evidential support we offer in this document -- our preferred recommendation is to get rid of the machines entirely and vote on hand-marked, high-security paper ballots and count those ballots by hand, the evening of the election in precincts… not voting centers. In the interim, the SEC should own the security effort on behalf of Tennessee voters and demonstrate their concern by putting the machines through a Security Risk Evaluation.

Issue

All machines containing technologies are susceptible to being breached. That has been proven again and again by behemoth companies like T-Mobile, Facebook, Marriott, Colonial Oil, Yahoo, the Department of Defense Office of Personnel Management, all of whom spend millions in cybersecurity protection only to be hacked in grand style.

Technology experts and Congressmen and women were adamant that this was a burgeoning problem that could rear its ugly head in the 2020 election. The Dominion manual says the machines can connect to the internet, even while election officials swear none of their machines did. How do they know? The ES&S machines can do the same. And Congressional members affirmed all of this in 2017, 2018, 2019 and 2020 Congressional testimony, news appearances, seminars, hackathons, affidavits, Secretary of State reports and audits.

Even the Dominion president and chief of security/sales verified the connectivity in testimony and sales presentations. Williamson County election machine IT technicians didn't deny the possibility of internet-connectable devices in the machines when asked on September 28, 2021 during machine inspections on behalf of several Williamson County Alderman candidates. When asked directly if any technology expert or election official in either Williamson County or Tennessee has looked deep inside the machines, the county affirms no. No one is allowed to verify the safety of the machines. Except the vendors.

In questions about these technologies and machines sent directly to machine vendors by our team, as well as the state's Director of Elections, Mark Goins (as best we can tell), the vendors refused to answer our questions about machine vulnerabilities, leading us to assume there must be some truth to our assumptions.

Despite this, election and legislative officials seem complacent and continue to feel that all things voting machines in Williamson County and Tennessee are fine and secure. And have remained oblivious at the facts/information we've presented in our various presentations. In fact, they have been anything but curious about our findings.

There is no question in our research that the machines are vulnerable and that needs to be remedied post haste. Our group, Tennessee Voters for Election Integrity, recommends that if we can't get rid of all machines used in the voting process NOW, then at least pursuing a Security Risk Evaluation on all the machines – not recertification -- is the best thing to do in order to win back the trust and confidence of consumers/citizens and their belief in the people and entities responsible for ensuring elections are trustworthy.

Discussion

Following the 2000 election, a movement began in the US to get rid of paper ballots and move toward voting on electronic machines. The Help America Vote Act of 2002 further enabled this crusade by setting aside billions of dollars for states to accelerate that move to electronic machines. Following the agony of hanging chads, dimpled ballots and the related hangover from the Bush-Gore election, electronic voting machines sounded good.

However, there's a problem. Technology can be hacked. And it didn't take long for that reality to bubble up. The 2006 documentary "Hacking Democracy,"[1] featuring cybersecurity expert Harri Hursti, was the first big blip on the screen that all was not well – or would be well -- with digital voting machines.

Later, J. Alex Halderman, professor of computer science and engineering at the University of Michigan, appeared. He is also the director of the Center for Computer Security & Society Election Integrity.[2] **For more than ten years, he's been a clarion call to whomever would listen about the vulnerabilities of electronic voting machines and their effect on our democracy**. He's been logical, consistent and information-based in his message. To prove it, he and his colleagues have hacked all types and makes of

[1] https://www.bitchute.com/video/FHIKK12Avnox/
[2] https://security.engin.umich.edu/

electronic voting machines used in America demonstrating their weaknesses on various news programs and seminars.

In 2012, he launched a University of Michigan course titled "Security Digital Democracy: How you can hack machines."[3] In 2018, he developed a brilliant opposing editorial for the New York Times titled "I hacked an election. So can the Russians."[4] In 2020, long before the 2020 presidential election, Halderman again warned Americans that the machines were a critical problem. In the documentary "Kill Chain: The Cyberwar on America's Elections,"[5] he appeared with Hursti and other experts documenting once again how easy – and frightening -- it is to hack an election.

But probably his most poignant argument came on June 28, 2017 when he testified before the US Senate's Select Committee on Intelligence, which looked into the security of US elections. In fact, within the first few minutes of his testimony,[6] he virtually predicted what many believed happened in the 2020 election.

His proof also entailed speaking at the Defcon 26 conference in Las Vegas in 2018. The conference features a room called the Voting Village, where hackers of all types and backgrounds are allowed to hack all voting machines used in the U.S. Interestingly, the organizers of the Voting Village invited representatives of all voting machine companies to attend the event in order to learn the vulnerabilities of their machines so they could design more secure software and hardware to stop hacks. None of the representatives attended.

Halderman's 30-minute presentation at that conference about how elections can be hacked[7]… even without day-of-election internet connections… is fascinating. He goes into great detail about the role of malware and companies that set up elections for various election commissions. His points have been a part of our presentations since our early research, but, surprisingly, have failed to illicit much curiosity among legislative and election officials who have attended and seen our data.

Halderman's consistent voicing of the grave concerns surrounding election machinery vulnerabilities has not been contradicted… only added to. And that has made him an outstanding expert on what these machines can do.

In 2018, a number of Congressional Representatives and Senators loudly echoed Halderman's points. A video that shows Representative Adam Schiff, Representative Sheila Jackson Lee, Representative Val Demings, Senator Ron Wyden, Representative Jennifer Wexton, Representative Ted Lieu, Senator Amy Klobuchar, Vice President Kamala Harris and Senator Mark Warner all confirming their adamant belief that voting machines can be hacked is stunning.[8] But where are these loud voices now that their

---

[3] https://www.youtube.com/watch?v=eXSF798qnCA

[4] https://www.americanthinker.com/blog/2020/11/michigan_professor_demonstrates_how_easy_it_is_to_hack_voting_machines_in_2018_new_york_times_video.html

[5] https://www.hbo.com/documentaries/kill-chain-the-cyber-war-on-americas-elections

[6] https://www.youtube.com/watch?v=3qr67h54VO0

[7] https://www.youtube.com/watch?v=4K0YZcbbzhc

[8] https://rumble.com/vtah4d-congressional-members-testify-voting-machines-can-change-votes.html

candidate of choice won the presidency in 2020? Why would that have changed their position and turned them silent on their message of election issues due to machines?

Other states have proven our proposition that these machines are a hindrance on the voting public.

In early 2020, the **Texas Secretary of State** issued a report denying certification to Dominion for use anywhere in Texas for the 2020 elections because of the security issues they found in the machines. Holes were in the software and hardware that would give bad actors a chance to ply their skills in changing election results. Their executive summary report is staggering.[9]

In **Michigan**, a forensic audit was held in Antrim County in December 2020 with a report of results issued on December 13, 2020.[10] Several disturbing claims were documented… one that "Dominion appears to be intentionally designed with inherent errors to create systemic fraud and influence an election." Another was that the Ranked Choice Voting (RCV) algorithm, which is used in some low-level elections to split votes into a percentage of a vote, was enabled. (Fortunately, Tennessee doesn't allow RCV.)

In **Georgia,** Dominion voided its Voluntary Voting System Guidelines 1.0 certification when it changed software the night before the election (November 2, 2020) in the state without testing the new software and without the move being certified by the Election Assistance Commission,[11] which is the process vendors must go through when making changes to their equipment. One has to assume that since that change was made in Georgia, is it possible that the same Dominion machines in other parts of the nation were suddenly out of compliance, too?

Also in **Georgia**, in the 2020 primary election, voting systems cybersecurity analyst Harri Hursti witnessed a number of highly questionable actions by Dominion and noted them in his August 24, 2020 affidavit[12] as a poll observer. Problems he cited included:

- Multiple Dominion system irregularities that cause intentioned votes clearly not to be counted;
- System escalates the security risk to the extreme;
- A group of Dominion employees were in a nearby room troubleshooting the Dominion voting system (while voting was occurring) via a remote access to key parts of the system; and
- Dominion employees were working the election in lieu of Georgia election employees.

In 2022, in **Tarrant County, Texas**, Col Shawn Smith (USAF Ret.), a subject matter expert on the security of computer-based election voting machines, testified about the fallibility of both the machines and the current testing and certification processes of all machines used in the United States.[13]

---

[9] https://www.sos.texas.gov/elections/forms/sysexam/dominion-d-suite-5.5-a.pdf
[10] https://www.scribd.com/document/488105156/Antrim-County-Forensics-Report-on-Dominion-Voting-System#fullscreen&from_embed
[11] https://themarketswork.com/2020/12/13/firm-that-conducted-audit-of-georgia-voting-machines-has-long-history-with-dominion/
[12] https://storage.courtlistener.com/recap/gov.uscourts.mied.350905/gov.uscourts.mied.350905.1.17.pdf
[13] https://rumble.com/v15st7w-military-cyber-security-expert-why-no-county-should-use-electronic-voting-s.html

But other states aren't the only ones to document the vulnerabilities of machines as even **Dominion employees have acknowledged their machines have wireless connections to the internet,** making election officials who claimed otherwise in 2020 look foolish.

In **testimony before a House Administration Committee** on Capitol Hill on January 9, 2021, Dominion Voting Systems President and CEO John Poulos admitted his machines can hook to the internet.[14] And not to be outdone, the company's sales/security chief, Eric Coomer, admitted in various videotaped sales presentations that data from Dominion machines can be sent worldwide,[15] joking in one presentation that the machines could send their data "all the way to Mongolia."

Following the 2020 election, where a number of credible, widespread allegations of voter fraud emerged nationwide, the **Williamson County Election Commission (WCEC) and its Chairman Bob Brown and Tennessee State Senator Jack Johnson** held a local public listening session to allow citizens to voice their concerns about the Dominion voting machines on which they just voted. The system used in the county was the Dominion Democracy Suite ImageCast version 5.5 which was first purchased on September 4, 2019 and upgraded to the D-Suite with de Minimis changes on January 12, 2020. Citizens were quite vocal at the meeting about continued use of Dominion.

And perhaps for good reason.

On January 11, 2021, because of all the concerns about the machines and the 2020 election, Williamson County Election Commission (WCEC) Administrator of Election Chad Gray sent a letter to the Tennessee State Election Commission (SEC) requesting on behalf of the WCEC for the SEC to "reexamine all voting machines provided by Dominion Voting Systems for use in our state in order to ensure that such machines meet the minimum criteria for certification pursuant to TCA 2-9-117".

On April 5, 2021, the SEC voted unanimously not only to look into Dominion machines but the other four brands of machines used in the state… ES&S, Hart, MicroVote and Unisyn. Unfortunately, more than a year later, the Commission has done nothing on this promise and simply gone silent. They have abandoned Tennessee voters and all 95 county election commissions on what they said they'd do – inspect the machines to be sure they are safe.

But they weren't safe.

In a relatively small Alderman election in Franklin on October 26, 2021, seven Dominion scanners in three distinct voting centers (a large voting location that encompasses all county precinct elections so citizens could vote at any of 8 or more voting centers instead of their assigned precinct) all malfunctioned during voting, causing scanner tapes to cease tracking votes.[16] The situation caused the Secretary of State to call the election an "incomplete election" that would have to be resolved the

[14] https://www.theepochtimes.com/some-dominion-machines-can-connect-to-the-internet-ceo-acknowledges_3620741.html
[15] https://www.thegatewaypundit.com/2021/01/new-video-shows-dominions-eric-coomer-admitting-voting-machines-wireless-support-networks/
[16] https://www.williamsonhomepage.com/franklin/election-officials-call-for-a-hand-count-of-votes-from-tuesday-s-city-of-franklin/article_29c49a8e-3719-11ec-b3f3-370527d0638a.html

following day by a full recount of all election-day, early and absentee ballots. That produced winners and losers. But it didn't sooth citizens' concerns about the ability of these machines to accurately count votes.

Keep in mind, before coming into Tennessee and before any Williamson County elections, these Williamson County machines had been certified by the Election Assistance Commission (EAC), their Voting System Testing Labs (VSTLs), the State Election Commission (SEC), the Williamson County Election Commission (WCEC) and their IT technicians as free of any problems and ready to safely and securely count votes. Despite all of these assurances, the machines failed their assigned duty.

But, even worse, following the election, two national security organizations – the EAC[17] and the Cybersecurity Infrastructure Security Agency (CISA)[18] – had to issue nationwide bulletins warning other states of these security issues that turned out to be **erroneous code in the machines**. Yes, in machines approved by all of these entities and which citizens and candidates were not allowed to inspect before the election.

Other studies have been performed on this issue by unrelated cybersecurity groups here,[19] here[20] and here[21] and come to the same startling conclusion. Machines that were declared able to perform their function defect-free, weren't. So much for trustworthy testing and certification.

That, plus a poor performance record in the county, got Dominion removed from Williamson County by the Williamson County Election Commission with a shove from the Secretary of State[22].

Today, Williamson Countians vote on ES&S machines. Yes, from the frying pan to the fire. We remain deeply concerned because all of the machine brands used in Tennessee – ES&S, Hart InterCivic, MicroVote, Unisyn and Dominion – have a heritage that factors back to the same foundation. Smartmatic, Dominion, ES&S, Sequoia, Diebold, American Information Systems, Premier. Components are intertwined. And the vendors are anything but transparent.

Perhaps the most frightening evidence concerning the vulnerabilities of these machines are the operational manuals themselves that we've looked into. When we were voting on Dominion, the technology experts on our team studied a number of Dominion manuals and have confirmed problems.

Our backgrounder recommending the county and state add best practices[23] to address the variety of issues we've seen is filled with numerous examples – both technological and process -- that allude to

---

17 https://www.eac.gov/sites/default/files/TestingCertification/EAC_Report_of_Investigation_Dominion_DSuite_5.5_B.pdf

18 https://www.cisa.gov/uscert/ics/advisories/icsa-22-154-01

19 https://kanekoa.substack.com/p/jeff-lenberg-dominions-erroneous

20 https://uncoverdc.com/2022/06/06/cisa-advisory-report-admits-voting-machine-vulnerabilities-denies-exploitation/

21 https://rumble.com/v18sodb-voting-machine-erroneous-code-doug-logans-williamson-county-tn-eac-report-r.html

22 https://tennesseeelectionintegrity.com/wp-content/uploads/2022/09/Hargett-approves-disposal-of-Dominion-in-WC-021622.pdf

electronic vulnerabilities of voting machines… so we won't repeat them here. But one issue stands out to us.

On September 7, 2021, following a deeper study of the most current Dominion manuals, and with no answer from Dominion or Williamson County about these specific concerns, we sent the following question to Director of Elections Mark Goins for an answer.

> Information we found in the latest manual (Dominion User Manual Version 5.5.139 for the Dominion Result Tally and Reporting (RTR) module) implies the system allows for mass vote changing by deleting results previously entered (Section 9.3 & 9.4) from secure removable media and replacing them with data from a local file (Section 7.4) or NAS (indicating some form of network is supported) attached files (Section 7.5) or by manual entry (Section 9.2)… with no dual-party authentication required. We've also seen that reports can be published to "Public" transfer points (Figure 65, Section 13.3), both "Local and Global" apparently including FTP sites (Figure 66) inferring that there is at least an indirect connection to the internet. Additionally, Section 14.4 indicates that remote clients can communicate with the server through Dominion… again inferring a network connection. Can you clarify this?

We never heard back from Goins, the Secretary of State's office nor Dominion about this. However, we have since heard a frightening answer from the Williamson County Election Commission.

In looking into the RTR manual, it was plain that this could be done by a single individual with access to the system and with no dual-party authentication or other oversight required.

In a meeting to inspect the voting machines for several Alderman candidates on September 28, 2021, the individual in the Williamson County Elections office who manages the RTR was questioned about this. They indicated that they were, in fact, able to make such a change, but that they would never do so. While we trust that this is true and we have no reason to mistrust the WCEC employee, we feel that the controls protecting against such an action are dangerously inadequate.

Additionally, it appears that the RTR system can publish results to "Public" transfer points inferring that the RTR system supports at least an indirect connection to the internet and, therefore, is exposed to hacking. Finally, the manuals state that remote clients can communicate with the server … again inferring a network connection. Williamson County has assured us that our RTR system is not used for either of these purposes and is in no way connected to the internet.

Still, this all affirms to us that numerous votes can be switched, and the vote totals changed by nefarious actors hacking into the RTR system which is designed to allow connection to the internet. Fortunately, there appears to be a trustworthy person currently at the helm of the RTR in Williamson County. But that's not enough to help citizens feel safe.

---

[23] https://tennesseeelectionintegrity.com/wp-content/uploads/2022/01/Best-practices-should-replace-issues-012622.pdf

We have identified two controls that may prevent such a manipulation from occurring undetected which we understand are currently not in place. They are included in the recommendations our team has made for a best practices pilot in Williamson County:

- A parallel hand tally of voting center, precinct early voting and absentee voting totals confirmed to match the numbers published by the state for our county; and
- A mandatory audit of the RTR/RTM log files, prior to certifying election results.

When inspecting the new ES&S voting machines which replaced the Dominion machines in early 2022, we asked the Chairman of the Williamson County Election Commission if these new machines had that same capability and he said yes, that it's a common aspects of these machines!

Trust… but verify

Given all this, as engaged citizens, our team has wanted from the start to ensure every Tennessee election is transparent, trustworthy and free of fraud, regardless who wins. We have been seeking – and we expected state and county election officials to seek the same with us – total election integrity and the confidences of voters in our election systems. While we didn't have overt reasons to believe that the problems alleged to have occurred in Georgia, Michigan, Pennsylvania, Arizona and elsewhere occurred in Tennessee, we just weren't sure. That led us to join together to search for answers, first as Williamson County Voters for Election Integrity and, later, Tennessee Voters for Election Integrity.

We saw as our mission:

- To **research, document and alert county election commissions, the Tennessee State Election Commission, legislators and government officials – professionals who could address and fix the problems -- to the weaknesses in our current election systems** that might result in election fraud from bad actors and exacerbate the public's lack of confidence and trust given noteworthy claims/reports/ affidavits of fraud in the 2020 election.
- To **establish a best practice template for elections, as well as the selection of election technology and procedures** in evaluating an existing election solution or in the selection of a new system.
- And to **recommend best practices, as well as innovative, outside-the-box election procedures**, that go beyond current procedures, ensuring a voting process that is accurate, transparent and trustworthy.

Our research since our November 2020 launch has been extensive. We've:

- Reviewed reports about machines, ballots, voter rolls, voting processes, nullification of legislators and voting laws, court cases, Big Tech/media censorship;
- Filed open records requests with the county and state… even having to employ a lawyer to force Williamson County to give us the Cast Vote Record from the November 2020 election;
- Reviewed election records to document every election since October 2021 to see if the election documentation is correct – we've found issues, including missing scanner tapes that have not appeared;
- Evaluated affidavits, data presentations, documentaries, Dominion user manuals, voter rolls;
- Canvased Williamson County to validate/invalidate anomalies we've found in the rolls;
- Studied the audit processes in various states;
- Interviewed poll workers, poll watchers and national election experts;

- Attended open meetings; and
- Presented our findings to legislators, government officials and the public.

Our conclusions have been wide-ranging. Just some of what we've determined:

- We've uncovered increased security risks caused by voting system machines;
- Voting equipment standards are weaker than those of the first smartphone and the standards are not being enforced by entities charged with doing so;
- There were issues in our 2020 election and we suspect there are state-wide similarities;
- There were issues in Franklin's October 26, 2021 Alderman election;
- Documentation of elections, while improving, is still lacking;
- Voter rolls are nowhere near as clean as they need to be;
- Voting centers are an opening for more technology and fraud into the voting process;
- There is an overconfidence in a weak, limited audit process that currently only looks at one of three functions of the voting process and at only 28 of 95 counties of the state;
- We might have outsourced our election in 2021 to a software vendor because their rep was the only one who could run absentee ballots to be counted;
- Election voting machine vendors are completely opaque and basically flip the bird at transparency and citizens who ask them questions;
- We learned we can't audit 70% of Tennessee counties due to the fact that no paper ballots are created in 67 counties from the questionable software of the DRE voting machine;
- Vendors are now controlling more of the election process than the voters and county commissions do; and
- County and state election commissions, as well as the Secretary of State and Tennessee Elections Coordinator, are anything but willing to work with citizens to implement security steps that could return citizen confidence in our voting system.

Because of these conclusions and, certainly, the vulnerabilities of machines, confidence in voting has been severely damaged in Williamson County and across the nation. Nearly 6 in 10 Americans (59%) believe permanent harm has been done to the US as a result of the 2020 election[24] process (June 2021 Democracy Fund Voter Survey). In a March 2022 poll,[25] 83% of voters viewed election integrity as either an important or very important issue. Two months later, in a Rasmussen poll,[26] 55% of likely U.S. voters believe cheating likely affected the outcome of the 2020 presidential election, including 39% who think it's very likely.

In short, because of the actions of other states, Tennesseans, especially now, don't trust our elections, our election commissions or our government election officials.

---

[24] https://www.voterstudygroup.org/publication/crisis-of-confidence
[25] https://nationalfile.com/poll-83-voters-view-election-integrity-important-issue/
[26] https://www.rasmussenreports.com/public_content/politics/general_politics/may_2022/election_integrity_most_voters_still_suspect_cheating

In mid-2021, since no election or commission official was helping us in our attempt to restore confidence in our elections, **we decided to ask all five machine vendors who have equipment in Tennessee some security/technical questions that might help us better understand the equipment.**

We first directed questions to Hart, ES&S and MicroVote following the July 12, 2021 Tennessee State Election Commission meeting where Hart and ES&S demonstrated machines to be certified by the Tennessee State Election Commission. Hart replied they weren't going to answer our questions because we "weren't election officials." We surmised the others would say the same, so, we asked Tennessee Election Coordinator Mark Goins to deliver all questions to the voting machine vendors**.**

Here are the questions we placed into Goins' hands on August 11, 2021, asking him to secure us answers since he was an election official:

ES&S QUESTIONS

1. **External to EMS Ballot Security Controls and ExpressVote/DSxxx Optical Scanner Compatibility** - this question was asked at the July 12, 2021, Tennessee State Election Commission meeting. However, we would like additional details from your response.
    - Would you please elaborate on the types of external ballot security controls that can be applied to your ES&S thermal ballot paper and still maintain full function and compatibility with the integrated optical scanner (e.g., won't interfere with proper reading of the barcodes for unique ballot identifiers and voter selections data). For example, holographic watermarks, mylar, dual-encrypted character strings in ballot margins, third-party QR codes or other identifiers such as serial numbers, etc.
    - Can any thermal paper be used with ES&S implementations, or do customers have to purchase paper ballot supplies exclusively from ES&S?
2. **Vote Cast Record Tracking** - Are you willing to partner with Third Party Ballot Security vendors on these types of measures?
    - Are you planning to use Microsoft Election Guard for vote cast record tracking (e.g., the voter can track their vote through the tabulation and results process)?
    - OR do you have other integrated solutions, or willing to work with other Third Parties?
3. **Logging** - Are Winevt logs for applications enabled, and security and system events set to archive and not overwrite?
    - Is file access auditing enabled on all program, data, and configuration files?
    - Are workstations configured to have ample disk space and other hardware configs to maintain robust logging for a minimum of 22 months?
4. **DS200 Adjudication** - would you elaborate further on point of scan adjudication?
    - How do you maintain voter privacy in the event their ballot is rejected due to configured outstack conditions (e.g., overvote, undervote, blank ballot, read/confidence level errors, etc.)?
    - How flexible are your outstack conditions for adjudication (e.g., some are fixed always, all can be enabled/disabled, combination of options, etc.)?
5. **User Roles and Security** - How many user roles do you have per functional area of the ExpressVote (including XL)/DSxxx system?

- Are there more granular security settings within each user role that can be enabled/disabled for each unique login (e.g., Election Designer can configure some elements of a ballot but not others)?
- Do you force password changes with users that are assigned to a role?
- Are there any shared UID's allowed, or is each UID assigned to a named person?

6. **General Adjudication** - Do you have configurable upper limits on adjudication that would visibly notify election officials? For example, multiple ballots are requiring adjudication (for some or all configured outstack conditions), which may indicate an upstream ballot printing or configuration issue?
7. **Internet Connectivity Verification** - Upon the delivery of your hardware, how do you verify for the customer that ES&S products do not have any hardware components capable of connecting to the Internet, e.g., Ethernet, WiFi and/or Bluetooth NIC hardware, etc.?
    - For any workstations with ES&S software, does internet connectivity prevention go beyond software/OS/BIOS configurations, and include any physical impairments for Ethernet, WiFi and Bluetooth NIC hardware, and how is that verified upon delivery?
8. **Hardware Manufacture** - Where are ES&S hardware components (and physical thermal ballot paper) manufactured, and assembled? This includes any internal electrical/electronic components, e.g., wiring, chips, etc.

HART INTERCIVIC QUESTIONS

1. **vDrive File Security** – This question was asked at the July 12, 2021, Tennessee State Election Commission meeting, which prompted a Hart representative to share a business card to allow for follow-up.
    - What are the file security measures (e.g., to prevent manipulation of the Unique Identifiers, Voter Selection data, etc.) in place for your vDrives from the point of exit from the Verity Scan Optical Scanner to the point of entry into a computer workstation (e.g., laptop, central server, etc.) running the Verity Count client, and from the point of entry into that computer workstation and loaded into the Verity Count client (or another applicable Hart module)?
    - Can the data on the vDrives be read or edited by tools other than your clients/applications?
    - Is there an independent and parallel manual verification that the totals match after the transfers and consolidation?
2. **External to EMS Ballot Security Controls and Verity Scan Optical Scanner Compatibility** – This question was asked at the July 12, 2021, Tennessee State Election Commission meeting. However, it was not clear in your response from our notes, and we are requesting a reminder of your answer.
    - Would you please elaborate on the types of external ballot security controls that can be applied to your Hart InterCivic-only Thermal ballot paper and still maintain full function and compatibility with the integrated optical scanner (e.g., won't interfere with proper reading of QR code and OCR for voter selections data)? For example, holographic watermarks, mylar, dual-encrypted character strings in ballot margins, third-party QR codes or other identifiers such as serial numbers, etc.
    - Are you willing to partner with Third Party Ballot Security vendors to integrate and use these types of measures?

3. **Logging** – Are Winevt logs for applications enabled, and security and system events set to archive and not overwrite?
    - Is file access auditing enabled on all program, data, and configuration files?
    - Are workstations configured to have ample disk space and other hardware configs to maintain robust logging for a minimum of 22 months?
4. **Vote Cast Record Tracking** – Will you work with other Third Parties, aside from Microsoft Election Guard (open-source code), to integrate voter cast record tracking of unique identified ballots?
5. **Verity Count** - Do you allow any manual entry of voter selection data in the event of the failure of a vDrive to load data? If so, how is this managed through the software business logic to maintain data integrity, no duplicate ballot tabulation, and logging for audit purposes?
6. **Two Factor Authentication** – Would you further elaborate on how you achieve two-factor authentication without the use of the Internet or external device (e.g., smartphone) for all Verity modules where it applies?
7. **Kiosk Mode** – While Verity Scan and Verity Duo (and Duo Standalone) may not connect to the internet, how do you protect the workstations running other Verity clients (e.g., Data, Build, Count, etc.) from internet connectivity aside from "kiosk" mode? Who has the ultimate administrative role to program and deploy "kiosk" mode to Hart workstations, as well as maintain those systems for operating system and server security updates?
    - Upon the delivery of your hardware, how do you verify for the customer that Verity Scan and Duo products do not have any hardware components capable of connecting to the Internet, e.g., Ethernet, WiFi and/or Bluetooth NIC hardware, etc.?
    - For workstations with Verity clients, does Kiosk Mode go beyond software/OS/BIOS, and include any physical impairments for Ethernet, WiFi and Bluetooth NIC hardware, and how is that verified upon delivery?
8. **User Roles and Security** – Do your user logins (UIDs) depend on Windows Active Directory?
    - How many user roles do you have per functional area of the Verity system?
    - Do you force password changes with users that are assigned to a role?
    - Are there any shared UID's allowed, or is each UID assigned to a named person?
    - Are there more granular security settings within each user role that can be enabled/disabled for each unique login (e.g., Election Designer can configure some elements of a ballot but not others)?
9. **vDrive metadata identification** – Do you use unique identifying information for each vDrive and carry that over to the Verity Count database in order to create a link between the vDrive from which the voter selection data originated? We want to ensure the unique ballot identifiers that prevent multiple scans of a single ballot carry over to the software database and it is impossible to manipulate without obvious traces.

MICROVOTE QUESTIONS

1. **Product Options** – Does MicroVote offer only DREs, or do you have any paper ballot systems (either Ballot Marking Device or Hand Marked Paper with Optical Scanners)?
2. **User Documentation/Demos** - Do you have any public facing user/installation/configuration/ hardware documentation that we can review? Do you have demo and/or training videos you could share with us?

3. **Internet Connectivity Verification** – Upon the delivery of your hardware, how do you verify for the customer that MicroVote products do not have any hardware components capable of connecting to the Internet, e.g., Ethernet, WiFi and/or Bluetooth NIC hardware, etc.?
    - For any workstations with MicroVote software, does internet connectivity prevention go beyond software/OS/BIOS configurations, and include any physical impairments for Ethernet, WiFi and Bluetooth NIC hardware, and how is that verified upon delivery?
4. **Hardware Manufacture** – Where are MicroVote hardware components (and VVPAT paper) manufactured, and assembled? This includes any internal electrical/electronic components, e.g., wiring, chips, etc.

DOMINION QUESTIONS

1. **Removable Media Failures –** What is the process for vote tabulation if removable media containing votes fails to load into the RTR software? How is this managed through the software business logic to maintain data integrity, no duplicate ballot tabulation, and logging for audit purposes?
2. **Results Tally & Reporting (RTR) Concerns** - The Dominion RTR User Manual Ver. 5.5.139 seems to indicate the RTR system allows for mass changing of votes by deleting results previously entered from secure removable media cards and replacing them with data from a local or NAS attached file or by manual entry. It also indicates that reports can be published to "Public" transfer points, including FTP sites, inferring that there is at least an indirect connection to the internet. These two capabilities in a desktop application used to tally voting results seem incredibly insecure. Are we correct in our interpretation of the manual and therefore the functioning of the RTR application? If we're not correct, how do you overcome these security concerns?
3. **In Person Adjudication –** Would you please explain any processes available to handle in person voting adjudication?
4. **General Adjudication** – Do you have configurable upper limits on adjudication that would visibly notify election officials? For example, multiple ballots are requiring adjudication (for some or all configured outstack conditions), which may indicate an upstream ballot printing or configuration issue?
5. **User Roles and Security** –Do your user logins (UIDs) depend on Windows Active Directory?
    - How many user roles do you have per functional area of the Dominion system?
    - Do you force password changes with users that are assigned to a role?
    - Are there any shared UID's allowed, or is each UID assigned to a named person?
    - Are there more granular security settings within each user role that can be enabled/disabled for each unique login (e.g., Election Designer can configure some elements of a ballot but not others)?
6. **Logging** – Are Winevt logs for applications enabled, and security and system events set to archive and not overwrite?
    - Is file access auditing enabled on all program, data, and configuration files?
    - Are workstations configured to have ample disk space and other hardware configs to maintain robust logging for a minimum of 22 months?
7. **Internet Connectivity** –

- Upon the delivery of your hardware, how do you verify for the customer that any Dominion products do not have any hardware components capable of connecting to the Internet, e.g., Ethernet, WiFi and/or Bluetooth NIC hardware, etc.?
- For workstations with Dominion clients/software, e.g., RTR, does security go beyond software/OS/BIOS, and include any physical impairments for Ethernet, WiFi and Bluetooth NIC hardware, and how is that verified upon delivery?

8. **Vote Cast Record Tracking** – Are you willing to partner with Third Party Ballot Security vendors on these types of measures?
   - Are you planning to use Microsoft Election Guard for vote cast record tracking (e.g., the voter can track their vote through the tabulation and results process),
   - OR do you have other integrated solutions, or willing to work with other Third Parties?
9. **External to EMS Ballot Security Controls –** Would you please elaborate on the types of external ballot security controls that can be used with ImageCastX connected printers and still maintain full function and compatibility with the ImageCast Optical Scanners (e.g., won't interfere with proper reading of QR code and/or OCR for voter selections data)? For example, holographic watermarks, mylar, dual-encrypted character strings in ballot margins, third-party QR codes or other identifiers such as serial numbers, etc.
   - Are you willing to partner with Third Party Ballot Security vendors to integrate and use these types of measures?

UNISYSN QUESTIONS

1. **Removable Media Failures –** What is the process for vote tabulation if removable media containing votes fails to load into the Unisyn software? How is this managed through the software business logic to maintain data integrity, no duplicate ballot tabulation, and logging for audit purposes?
2. **In Person Adjudication –** Would you please explain any processes available to handle in person voting adjudication?
3. **User Roles and Security** – Do your user logins (UIDs) depend on Windows Active Directory?
   - How many user roles do you have per functional area of the Unisyn system?
   - Do you force password changes with users that are assigned to a role?
   - Are there any shared UID's allowed, or is each UID assigned to a named person?
   - Are there more granular security settings within each user role that can be enabled/disabled for each unique login (e.g., Election Designer can configure some elements of a ballot but not others)?
4. **Logging** – Are Winevt logs for applications enabled, and security and system events set to archive and not overwrite?
   - Is file access auditing enabled on all program, data, and configuration files?
   - Are workstations configured to have ample disk space and other hardware configs to maintain robust logging for a minimum of 22 months?
5. **Internet Connectivity** –
   - Upon the delivery of your hardware, how do you verify for the customer that any Unisyn products do not have any hardware components capable of connecting to the Internet, e.g., Ethernet, WiFi and/or Bluetooth NIC hardware, etc.?

- For workstations with Unisyn clients/software, does security go beyond software/OS/BIOS, and include any physical impairments for Ethernet, WiFi and Bluetooth NIC hardware, and how is that verified upon delivery?

6. **Vote Cast Record Tracking** – Are you willing to partner with Third Party Ballot Security vendors on these types of measures?
    - Are you planning to use Microsoft Election Guard for vote cast record tracking (e.g., the voter can track their vote through the tabulation and results process),
    - OR do you have other integrated solutions, or willing to work with other Third Parties?
7. **External to EMS Ballot Security Controls –** Would you please elaborate on the types of external ballot security controls that can be used with Unisyn and still maintain full function and compatibility with Unisyn Optical Scanners (e.g., won't interfere with proper reading of QR code and/or OCR for voter selections data)? For example, holographic watermarks, mylar, dual-encrypted character strings in ballot margins, third-party QR codes or other identifiers such as serial numbers, etc.
    - Are you willing to partner with Third Party Ballot Security vendors to integrate and use these types of measures?
8. **Hardware Manufacture** – Where are Unisyn hardware components (and physical ballot paper) manufactured, and assembled? This includes any internal electrical/electronic components, e.g., wiring, chips, etc.

Over a year later and after multiple follow-ups with Goins, we're received no answers back. That speaks volumes to us about vendors' – and Goins' -- aspirations for transparency and caring about the ultimate customers of these machines -- the citizens --and their trust in these machines.

So, we have to assume there is truth to our assumptions. Otherwise, Goins and the vendors would have attempted to persuade us differently. If their machines truly perform without vulnerabilities, without the internet, logic implies that vendors would surely affirm this point by demonstrating their equipment, wouldn't they? Why are they and state election officials being so secretive? In our judgment, a simple solution would be to demonstrate that their machines have no internet connection technologies inside the machines to a group of cybersecurity experts who sign NDAs to ensure the vendors' proprietary technology remains a secret, if that is their concern.

What can be done?

So, the question becomes, if officials can't see the logic and cost-savings of going back to paper and removing the technologies and machineries, what can be done to plug these vulnerabilities? And what could help citizens begin to feel more confident in these machines and our elections. The answer is simple. Every machine that is left behind on both the registration side of the precinct and the voting side of the precinct – regardless its brand – should undergo a <u>Security Risk Evaluation</u>.

In our judgment, if recertification is EVER attempted now by the State Election Commission, it's a waste of time. It's checking the math. <u>And it's checking the math to 2005 standards because that's the extent of what the EAC demands</u>. It is not looking deep into the machine to check for the presence of nefarious – or the latest -- technology, which is what citizens have been crying for. That's what hundreds of affidavits, videos, data studies, etc. across the county affirmed. And that's what Tennessee citizens – and others across the nation – are seeking in order to help return their trust in our elections.

Think about how out-of-date the EAC standards are.

The first smartphone was launched by Apple in 2007. The iPhone became the standard against which other smartphones in the marketplace had to aspire. So, recall what changes, upgrades, security patches, new models, technologies and certifications have occurred in smartphones over the last 15 years? From 2007 to 2022. But the machines on which we vote are only certified to 2005 standards. Two years earlier than the first smartphone.

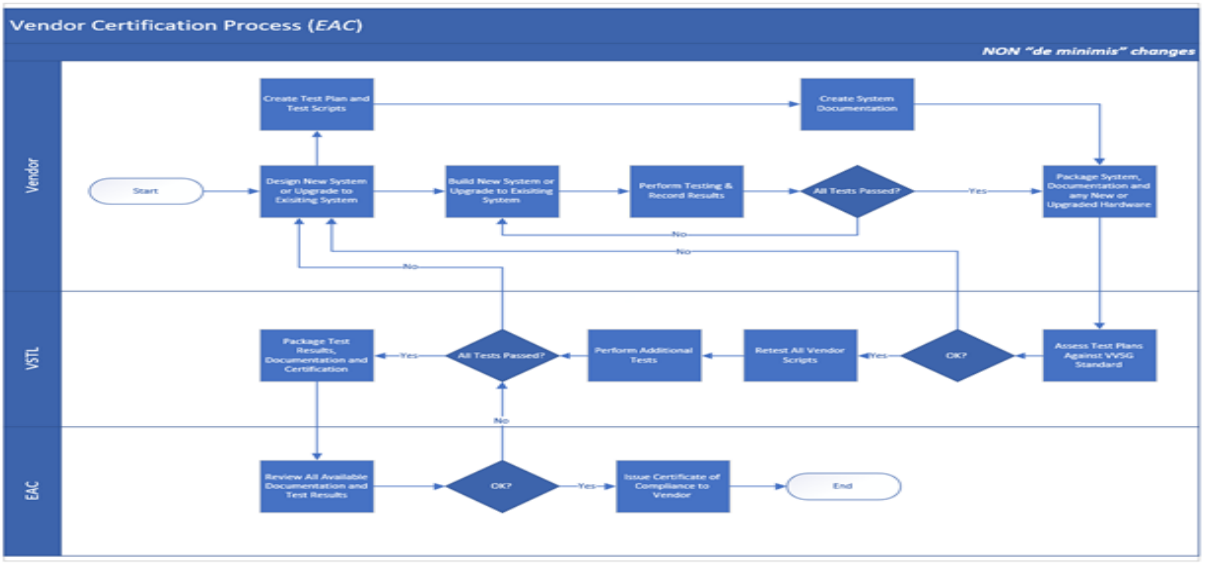
But what did we have to be concerned about? The machines used in the October 2021 election in Franklin, Tennessee were already certified by every possible entity overseeing our elections.

So why hasn't the EAC or other entities demanded that machine vendors meet new, improved, more robust security criteria reflecting new developments in technology? If they are to be the purveyors of security and standards for the industry, why didn't they mandate that vendors adopt the higher standards in 2015 when the EAC introduced VVSG 1.1?

And even harder to explain, why did the EAC earlier in 2021, with no public debate or no review from their Board, institute new, far more lenient guideline changes that helped the vendors' bottom lines, but greatly weakened the security of voting systems by allowing wireless networking devices in machines? [27]

That cost the EAC one of its most ardent supporters in Dr. Phillip Stark who has now left the EAC Board and is suing the EAC because of the move.

This graph shows our understanding of the certification process… the one that all the machines have been through already. And the one that will probably govern the recertification process if pursued.



[27] https://www.scribd.com/document/516851701/2021-07-13-complaint-4814-7096-7793-1#from_embed

To us, this process does not appear to dig into the true validity of the machines. To the best of our knowledge, it does not involve experts digging into technologies within the machines. All websites of the EAC and their VSTLs share no information about their staffing or expertise of those who might do the certification, recertification or decertification. This is another reason why we believe recertification will only repeat this process, not enhance it.

Their recertification process, which involves two accredited Voting System Testing Labs in the US who verify the testing done by the vendor, is, likewise questionable. One of these firms, which are to oversee the security standards of the EAC – ProV&V – has a completely unsecured website. What does that say about their own process, standards and devotion to security?

And in case you didn't know. It's the vendors who pay the VSTLs to certify their machines, not the EAC. Isn't that a highly questionable arrangement for a company you just paid to render judgement on the cleanliness and security of your own machines?

In our judgment, the EAC is a paper tiger that has acquiesced more and more to the desires of the vendors, versus looking out for the needs of consumers and citizens. They cannot be trusted to really dig into the problems as they recertify machines.

Another questionable arrangement? The EAC employee who recently oversaw certifications for the EAC is Jessica Bowers, a former ten-year employee of Dominion before she joined the EAC in May of 2019.[28] She's also the person who pitched the Tennessee State Election Commission to allow Dominion to enter Tennessee in 2018 and shepherded their entry into Williamson County in 2019 before jumping to the EAC. We suspect she – or a colleague (they are a small staff) – will be the one to officially decertify or recertify the Dominion machines. How can anyone believe that the person who sold Dominion voting machines to Tennessee and Williamson County will do anything BUT recertify the machines? Decertifying Dominion machines will say much about the product she first pitched the state a short four years prior. And using common sense and factoring in human nature, you know that she most probably won't let that happen.

We're also concerned about the local side of this process.

At the July 12, 2021 meeting of the Tennessee State Election Commission, two firms – Hart and ES&S – were presenting new versions of existing equipment to be approved by the SEC for use in Tennessee. Interestingly, there was no IT expert with the Secretary of State's department who testified that the equipment had been checked by the state to ensure there was nothing nefarious in it. There was no written report entered into the record. The commission simply accepted the EAC certification without any question.[29]

At the January 10, 2022 SEC meeting, Hart requested the SEC to allow them to update their machines from Windows 7 to Windows 10. Seemingly no big issue, right? Unfortunately, no one on the

[28] https://themarketswork.com/2020/11/20/the-small-world-of-voting-machine-certification/
[29] https://sos-tn-gov-files.tnsosfiles.com/SECAGEND%20-%20July%2012,%202021.pdf?3jGvBK5zy5mgcPY0KRaPdkVy.kZzrHfh

commission or Mark Goins seemed to know that Microsoft had stopped supporting Windows 7 on January 14, 2020. That meant that all Hart machines in the state were at high security risk before, during and after the November 2020 election since security patches were not being installed by Microsoft. No one said a word about this at the meeting, especially not Hart.

What were administrators doing in the 25 or so counties that had Hart machines? Were they patching them? If so, how? Or did they even know they needed to be patched? Most of those county election commissions don't contain IT security expertise. None of these questions were discussed, although we did send Goins a follow-up note about this vulnerability to which he never replied. And where was the State Election Commission staying on top of this security situation? What about the Secretary of State's IT personnel?

Given all the concerns about voting machine technology in the aftermath of the 2020 election you would think the SEC would go the extra length to ensure security. But they didn't. The state appears to have done nothing in the way of machine cybersecurity to assure Tennesseans were getting safe, secure, trustworthy equipment. This is simply the state of performance of the Tennessee state election commission.

Implement a Security Risk Evaluation
Since the SEC has refused to recertify the machines as they promised on April 5, 2021, what they need to do if machines are kept in the voting process is conduct a Security Risk Evaluation, where non-EAC experts check the machines from both the voting side and the registration side of the precinct.

The evaluation should be conducted by a bi-partisan committee of citizens with credentialled data/internal/process control experts and IT/cybersecurity experts. This process was detailed and recommended to the State Election Commission on October 11, 2021 during our presentation to the group. Yes, it was ignored.

It will take legislators and government officials who are bold and are willing the seize this opportunity to make a statement about themselves and the state of Tennessee to make this move to a special evaluation. If they do enact a Security Risk Evaluation, it will say a lot about their devotion to election integrity.

Here is how this evaluation might work.

1) The State Election Commission (SEC) should decide on any essentials that they will require. We suggest:
    a. Paper ballots
    b. No encryption of voter selections
    c. Protection from counterfeit ballots
    d. Protection from ballots being counted twice
    e. Protection against any form of network (internet, Wi-Fi, Bluetooth, modem, etc.) or onboard added tech (Telit chips, Qualcomm chips, iDRAC chips) on the motherboard and any other connection "whitelisted."

   f. Protection against unauthorized hardware and software being utilized in the election process by way of software and hardware verifications before and after every election.

2) The SEC would fund a team consisting of 6 bi-partisan IT, Cybersecurity and internal controls experts who would evaluate VVSG 2.0 and create a subset of criteria – a Minimum Voting Standards Guideline (MVSG) -- that are critical to ensuring a secure and accurate election.
   a. The team should add to those criteria the requirements of the SEC above, if necessary
   b. The team should research and identify any alternative vendors that they propose should be considered for certification.

3) The criteria and proposed vendor candidates should be reviewed, modified as appropriate and approved by the SEC.

4) These criteria should then be sent to each of the vendors being considered for certification or re-certification for them to self-analyze and provide a report back within one month as to whether they: 1-fully meet; 2-partially meet; or 3- do not meet each criterion. They should describe any pertinent details and any compensating features of their systems that may address the concerns of unmet criteria. Vendors should also describe any particular features they offer above and beyond the criteria which they feel are beneficial.

5) The team should then do an audit on each vendor of their responses focusing on a few of the most important criteria and anywhere they have reason to believe the vendor may be weaker than reported.

6) The team would then make a recommendation to the SEC on their findings ranking the vendors quality, stating which vendors they feel are adequate to be certified and providing the most critical pros and cons that were identified in the process including the following when pertinent:
   a. Prioritize risks, determine the likelihood and impact
   b. Document vendors' ability/plans to remediate risks
   c. Identify any vendor plans to remediate that are critical to the vendors certification

7) The SEC would then evaluate the recommendations and data provided by the team and make a decision on which and how many systems would be certified. There should be no requirement of 5 options if there are not 5 viable vendors.

Finally, after this process has been done, it will be important for the committee to issue a report to the state concerning their findings. It should be expected that news media will cover this entire effort, and, especially, the results from the evaluation.

If Tennessee really cares about election integrity at this time of great citizen unrest with the process, it will take this step to begin winning back the confidence and trust of consumers/citizens in the state's election system.

Recommendation

Our recommendation to address the significant vulnerabilities demonstrated in these machines is, ideally, to remove all machines in the voting process and return to hand-marked, high-security paper ballots counted in precincts by hand on the evening of the election. This process is the safest, most secure option for voting, which has been proven over[30] and over[31] and over[32] and over[33] again.

If the SEC requires a number of steps to reach this confidence-inspiring goal, then the State Election Commission should, in the meantime, conduct a Security Risk Evaluation as spelled out above on all machines to more fairly judge the condition of the existing election machinery from both the voting side and the registration side of the precinct.

A report should then be issued statewide detailing the results of the evaluation and appropriate machinery changes should be made at that point as needed.

Conclusion

Electronic voting machines used throughout Tennessee on which citizens vote are exceptionally vulnerable to being hacked.[34] A wide variety of sources have proven that point. And given the events involving these machines in other states and in Tennessee, there is now great distrust in these machines and, by extension, great distrust in the election process and the entities whose responsibility it is to ensure elections are conducted fairly and in a trustworthy manner.

Taking this more detailed, extensive step in ensuring the machines are trustworthy – if they remain by default -- will go far in restoring citizen trust in the machinery and process of electing our leaders throughout Tennessee.

###

[30] https://www.pbs.org/newshour/politics/election-security-experts-urge-georgia-to-swap-out-touchscreen-voting-machines
[31] https://www.pbs.org/newshour/show/what-election-officials-think-about-paper-ballots-and-voting-machines
[32] https://www.theatlantic.com/magazine/archive/2017/12/guardian-of-the-vote/544155/
[33] https://tennesseeelectionintegrity.com/wp-content/uploads/2022/09/Voting-machines-what-could-go-wrong-New-York-110518.pdf
[34] https://www.nbcnews.com/politics/elections/online-vulnerable-experts-find-nearly-three-dozen-u-s-voting-n1112436