TENNESSEE VOTERS
FOR ELECTION INTEGRITY

VOTER CENTERS ARE AN OPENING FOR DECEIT;
WE MUST RETURN TO PRECINCT VOTING SO THE VOTE PROCESS CAN BE BETTER SECURED

Executive Summary

So, few of the experts are looking at the vulnerabilities that voting centers add to election integrity concerns versus the former precinct voting they are designed to replace. In addition to the ease they offer hackers to tap into registration data to change election numbers and results, voter centers also provide election machinery vendors a nice steady flow of income. However, they add greater risks to counties during elections and should be completely gotten rid of.

Issue

Voting centers are a relatively new concept whose risks far outweigh their rewards.

They require all voting centers – which are larger voting locations than a neighborhood precinct – to be connected via the internet to prevent multiple check ins at multiple voting centers by one person. But how many companies having had their data stolen lately are replacing their security with a VPN?

They also justify the need for ballot marking devices (BMDs) which have been proven to be suspect (see our other support documents about “No paper ballots in 70% of Tennessee counties” and our need for “Hand marked Paper Ballots” for further documentation) – in handling multiple ballot types.

Voting centers make maintaining control of precinct data and identifying discrepancies and data oddities a lot harder and a lot less successful, making it easier for hackers to do their dirty work under cover.

Tapping into the registration system via the internet, these malicious actors can monitor and exploit the precinct/voting center numbers, as well as ballot inventory, to insert votes supporting their favorite candidate.

With citizens crying out for greater ballot security and election integrity, you have to wonder why election officials are ignoring the pleas of customers and continuing to push concepts like voting centers that add nothing to the security of voting.

Discussion

Launched in 2008 by the Obama administration, voting centers may have seemed to be a good idea. But they have since proven to be anything but. Especially for voters concerned with election integrity.

The idea was simple and established under the guise of offering harried voters another “convenience” voting option. What if a voter is running late and the polls are about to close and the voter doesn’t have time to make it to his designated neighborhood voting precinct? Why couldn’t he just go to the nearest precinct – or voting center – and vote there since all voting centers would have the ability to technologically bring up any ballot in the county on which that voter could vote?

Sounds good, huh? Customer-friendly, right? Safe, secure. Well, not really.

It's a convenience that is filled with a number of opportunities for nefarious actors to exploit the system and hijack, delete or add votes into the count from voters who have not, cannot, or don't want to vote. It's a great way for election officials to pander to citizens who don't want to take the time needed to responsibly execute their right to vote. Who want to rush through the exercise and move on. It's an opportunity for illegal hands and minds to bring phantom voters into the voting arena, a new but very real election integrity issue/phenomena that is commandeering the registration side of the election process across the nation.

How is that so? Well, all ten, twenty, thirty or however many voting centers the county wants to establish have to be connected at all times to each other via the internet to prevent a voter from voting at one voting center and then traveling down the road to another voting center to vote there an hour later.

But wait, supporters of this concept will say…. "We have a VPN protecting the internet connection between all of these voting centers…. So, there should be nothing to worry about!" Yes, it's true that the internet connection is supposedly protected via a VPN.

But what do T-Mobile, Facebook, Marriott, Colonial Pipeline, JBS, Yahoo, the Department of Defense Office of Personnel Management have in common? Well, they're spending billions of dollars every year on security protection for their data and customer services – far more than Williamson County is spending on a VPN – and yet all have reported being hacked within the last two years and massive amounts of their data stolen. A key county in a state election is just as valuable and, unfortunately, far more unprotected.

And strengthening internet security after a hack just will not cut it for voters whose votes have just been nullified by a malicious hacker.

Honestly, the simple retort that our voting centers are protected by a VPN isn't worth anything these days. Especially when the easiest remedy is to simply stop using voting centers, return to voting by precincts and remove the internet connections between them. Viola. A solution looking for a problem is resolved.

So, let's stay with that idea about the ability for the internet connections between voting centers to be hacked for a moment. Because once a malicious actor has hacked into the registration side of the precinct, they have the keys to the kingdom… access to adding/subtracting a new kind of voter. Something called phantom voters. Citizens whose names and identities are on voter rolls who usually don't vote but those names are able to be hijacked by hackers who tap their profile and voting status to insert the "votes" of these phantom voters into the rolls and registration process.[1] After hacking into the registration side of the precinct or voting center, these hackers suddenly have direct access to who has voted, who didn't vote and who won't likely even show up at the poll to vote. The phantom voters become real.

[1] https://www.americanthinker.com/articles/2021/11/meet_the_technology_thats_uncovering_2020s_voter_fraud.html

No internet connection between them? No phantom voters.

And once they know all the historic particulars of how votes usually go in a specific voting center, these malicious actors can reach into their vote slush fund and supply the necessary votes to put their favorite candidate just over the finish line… yet not so far over that it causes automatic audits. Or spurs questions from election workers.

There's an easy explanation of how this can work and the evidence comes from the report of a whistleblower in a recent December 13, 2021 public hearing in Pima County, Arizona.[2] In an Oct. 10, 2020 letter to the criminal division of the Arizona Department of Justice, where the whistleblower asked Democrats at a private meeting where the embedding of 35,000 illegal votes into the vote count was planned, he was told "that spread distribution (of the 35,000 votes) would be embedded across the total registered vote range and will not exceed the registered voter count. It was also stated that total voter turnout versus total registered voters determine how many votes we can embed. The embedding will also adjust based on voter turnout."

When the whistleblower asked if this process had ever been tested and how do you know it works, the response was "yes, this has been tested and has shown significant success in Arizona judicial retention elections since 2014."

So, if it can work in Arizona, why not Tennessee? With state election officials fighting so hard to keep and increase the technology around the voting process, who's to say it hasn't already worked here in Williamson County and Tennessee? Why are election officials so focused on keeping technology in a process that can be hijacked so easily?

Another problem with voting centers is their size. They force all voter information in an election to be available in large voting centers. Which makes it exceptionally difficult to see and stop nefarious activity. Smaller precincts can halt illegal voting behavior far, far earlier – and easier – than in big voting centers.

Its' like the old "Where's Waldo" artwork. In a huge poster, ask "Where's Waldo" and its very hard to find him and it take a lot of time to do so. Greatly reduce the size of that poster – say, the size of an average precinct – then finding Waldo is a lot easier. Think how much simpler it is to lose control of precinct and voting data in a large voting center. Greatly decrease the size of the venue then identifying discrepancies and data oddities is a lot easier.

That's exactly what happens when you compare a large voting center next to a small neighborhood precinct. If you're interested in ensuring election integrity, then you want a smaller precinct versus a voting center.

In a presentation that Secretary of State Tre Hargett and his Elections Coordinator Mark Goins made to the House Local Government Committee of the General Assembly on January 25, 2022, Goins made the point of how much safer and secure precinct voting is opposed to voter center voting. Answering the

[2] https://uncoverdc.com/2021/12/14/dirty-voter-rolls-and-mail-in-ballots-key-issues-in-pima-county-hearing/

question of Bolivar Representative Johnny Shaw of how can you trust that your vote is counted correctly in a precinct, Goins said:

> "Most of the time, those poll officials want to work in their community (as opposed to a vote center far away), many times because they're retired. And you go in… you're seeing your old teacher, whatever. That's really instilling integrity, as well. These are folks that care about you personally because they know you. But they also care about the system."[3]

Quite the opposite of a voter center.

Another issue. With the larger size of a voting center, vs. the precise size of a neighborhood precinct, that means more ballots – in fact, an almost innumerable number of ballots – have to be printed and available for use at the voter center. Which means a vast number of probably unused ballots that are just sitting around the precinct in case certain types of voters come into the voting center. That means an increased amount of inventory control will be necessary to ensure these extra ballots don't fall into questionable hands for misuse.

In the Franklin election of October 2021 six Dominion machines glitched and stopped recording votes. It was a small 7,000-vote election and it caused undue angst. And everyone continues to wait months later for the Williamson County Election Commission to determine what happened. So, you're going to tell us that the same folks that can't manage a 7,000-vote election are going to be able to maintain a secure, intense overwatch over extra ballots that are sitting around in a precinct?

You would think the logic of the aforementioned issues would lead election officials away from the problems and challenges of voting centers. But there's another behavior we've noticed associated with the voting centers a nd the attraction election officials have for them. The centers demand the presence of more technology from election machine companies, including ballot marking devices (BMDs), those costly, vendor-heavy pieces of equipment that must be connected to printers to work and use vendor-demanded software, paper and processes. Election officials want more technology? Well, then, the more need for election equipment rentals and purchases and ever-ongoing vendor service payments from their buddies the election equipment vendors.

Some election officials claim that the technology being added into the process far outweighs any advantages from the "old-fashioned" paper ballots and counting. Actually, we're still waiting to see their studies that support their contention. In the meantime, here are a few studies that offer an entirely different perspective about BMDs and voting centers:

- BMDs increase polling place lines, make voting less efficient, less secure than paper ballots
    - *Guess Which Ballot Costs Less and is More Secure Paper or Electronic? (August 2019)*[4]
- BMDs can fail; BMDs take 3x longer than paper ballots
    - *Reliability of Pricey New Voting Machines Questioned (February 2020)*[5]

[3] https://tnga.granicus.com/MediaPlayer.php?view_id=658&clip_id=25799

[4] https://www.pennlive.com/opinion/2019/08/guess-which-ballot-costs-less-and-is-more-secure-paper-or-electronic-opinion.html

[5] https://apnews.com/article/voting-hacking-voting-machines-ae388fb69d14e5d3619128a591cdc0c4

- BMDs rely on voters detecting ballot errors; yet only 5-7% of voters find, report errors
  - *Can Voters Detect Malicious Manipulation of Ballot Marking Devices (May 2020)*[6]
- BMDs can be hacked, mis-programmed, misconfigured, or contain malware which alters the ballot or tallies
  - *Ballot Marking Devices Cannot Assure the Will of the Voters (April 2019)*[7]

Actually, BMDs depend upon the use of bar codes and QR codes in most current machines, which supposedly interpret the voter's choices on paper to be read by the scanners looking at the QR code and bar code. In other words, it is the QR code – not the actual text choices printed on the ballot – that is read by the scanner. And since the codes can't be read by a voter using a simple QR code reader on his phone to be sure the code correctly interpreted his vote choices, these BMDs actually prevent voters from having something that is a long-claimed ballot attribute -- a voter verified paper audit trail.

BMDs prevent that.

In the August 4, 2022 Williamson County state primary/county general election, coupled with a long ballot, waits for voters to vote topped two hours in some precincts. That was because of the BMDs, whose supply can never fully accommodate for citizen flow in a voter center. Buying more and more BMDs is an exceptionally expensive proposition. Williamson County already has a quarter of a million dollars invested in 200 BMDs… and they're talking about purchasing more. (Wouldn't it be simpler and cheaper simply to do away with the BMDs technology and move to a hand-marked, high-security paper ballot marked by voters in those temporary privacy ballot stands? No question. The logical answer is YES!)

Finally, there's simply one last fallacy on which election officials have been selling the voting center concept. The idea of convenience. But, not surprisingly, we've seen no studies that affirm voters want convenience over security. Where is that study? Who authored it? Has it been produced by a voting machine company that manufactures voting equipment? Actually, it's a false narrative.

In fact, throughout time that we have been digging into election integrity, we've continually asked the question of voters… do you want convenience or the security that your vote was counted as you cast it? We can assure you that few Tennesseans have opted for "convenience."

Voting centers are an easy opening for deception to enter in the voting process and Williamson County – and any county that currently is testing or considering that concept – needs to return immediately to precinct voting if they care anything about protecting election integrity.

First, and emphatically the county needs to jettison voting centers and return to precinct-based voting.

This would be the case for early voting, absentee voting and election day voting. This step will greatly protect the integrity of the vote because an internet connection between voting centers will no longer

[6] https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf
[7] https://www.researchgate.net/publication/333245177_Ballot-marking_devices_BMDs_cannot_assure_the_will_of_the_voters

be necessary, immediately limiting the ability for the registration side of the precinct being hacked. Additionally, it will limit the number of ballots needed for the precinct to have on hand to only those contests that are being addresses in the specific precinct. So, as it becomes harder for unused ballots to be misused, inventory control will be easier. Reconciliation of all ballots – those used and voted, those voided and those unused – will be easy and a special form needs to be developed for reporting these numbers at the end of the voting day.

Second, the county should study ways for the Voter Central registration software to be better protected, including having this software go offline – go completely dumb -- for early voting, absentee voting and election day. Keeping the system dumb most of the time, along with whitelisting only those computers that will be able to connect to the system at sporadic times of the day, should limit access. Importantly, the county should keep a record of every moment the Voter Central software is "live" and every ip address that connects with it or attempts to connect with it throughout the election.

Finally, the system should eliminate the need for any network connection for voter check-in. That will prevent one avenue of real-time monitoring of voting that can be used for criminal fraud activities or malicious information gathering.

Recommendation

As proven in this white paper, voter centers are an opening for treachery executed by malicious actors who want to hijack the system for their own nefarious purposes. Any county in Tennessee currently using voting centers should immediately return to precinct-voting.

The county should study ways for the Voter Central registration software to be better protected, including having it go dumb during most of its use to prevent hacking and whitelisting those machines approved to access the software system.

Finally, the system should eliminate the need for any network connection for voter check-in.

Conclusion

Implementing these changes immediately will help the county immediately begin to return its election process and system to a system focused on election integrity.

###