TENNESSEE VOTERS FOR ELECTION INTEGRITY

**ENSURE MACHINE AND VOTING PROCESS ISSUES ARE REPLACED WITH BEST PRACTICE SOLUTIONS STATEWIDE**

## Executive Summary

During our research, we identified a number of issues that appeared to have occurred in Williamson County in the 2020 election. After continued research and seeing many of these issues crop up in other states and counties, we now have reason to believe they all probably can be found statewide.

Our inquiry led us first to send 51 questions to the Williamson County Election Commission for answers about our concerns. At one point the State Election Commission began working with the WCEC to answer these questions, but they both stopped the process months and months ago and have never resumed efforts. So, we decided that our assumptions must be correct and identified industry best practices that would address each concern. Which is what we have been sharing with audiences before whom we've spoken.

We have since identified a few answers along the way; other issues still await answers, though.

For instance, the question "Are all paper ballots, documentation of chain of custody, seal verification logs, SD cards, thumb drives and original disk images of the systems being securely maintained for 22 months," though answered somewhat, remains a problem. We now believe that electronic records, logs, CVR's etc., in Williamson County are not maintained for 22 months in the case of a national election and for six months in the case of a local election. This is a key issue if there are later questions about the election that must be addressed through a study or audit of both paper and electronic records. This is especially critical since election records on the machines can be overwritten when the machine vendor updates the machine's software. In Williamson County, that occurred in January 2021 when Dominion applied an update to the Williamson County machinery. So, if Williamson County did not separately maintain electronic records somehow, then all electronic records for the 2020 election are gone.

That's the type issue we're dealing with here. Problems that if not addressed open the door to nefarious actors to do nefarious things with our elections.

In our efforts to make legislators, election commissioners and government officials aware of potential problems in various counties, this support document lists a number of our concerns and offers best practice solutions to them. We have shared much of this information with them before.

## Issues

We grouped the issues into three categories of solutions:

- Technological issues and solutions
- Process issues and solutions
- Legislative issues and solutions.

Below are the questions – and our recommended solutions -- grouped in this order.

**Discussion**

We have not arrived at these Williamson County issues haphazardly. Our group has done a tremendous amount of work in election integrity[1] to uncover these concerns including:

- Reviewed reports about machines, ballots, voting processes, nullification of legislators and voting laws, court cases, Big Tech/media censorship, citizen videos, news reports;[2]
- Evaluated affidavits, data presentations, documentaries, IT and cybersecurity recommendations, even a number of Dominion user manuals.
- Followed the audit processes in various states;
- Talked with election officials in a number of other states;
- Studied Tennessee voting laws, legislation and national certification regulations;
- Sent questions to voting machine vendors and State of Tennessee officials;
- Interviewed poll workers;
- Attended open meetings;
- Performed voting machine inspections for several current candidates for public office;
- Discussed our findings with legislators, government officials
- Talked with members of the public about our work following special meetings and presentations.
- Filed open records requests with both WCEC and the Secretary of State and presented results of our findings and research to legislators and the Tennessee State Elections Commission.

Our work has been methodical and thorough. Following are our recommendations.

**Best Practice Solutions: Technological**

**Establish dedicated encrypted, physical network for voter roll/eligibility system**. Some Voter roll/eligibility systems utilize an Intranet to span multiple physical locations. This provides a convenience that voters can vote at any location served by the Intranet connection, but it is also a security concern depending on how the Intranet is architected. A dedicated physical network would be preferable, but more often systems will use a VPN (Virtual Private Network). VPN technology rides in an encrypted fashion over the Internet and the level of this encryption, if used, should be specified. Further, if any devices connected to the VPN Intranet are also enabled to the public Internet, a significant vulnerability is created and should be avoided. VPNs are good but not infallible.

**Disk encryption must be verified**. The Dominion promotional material states that Dell Full Disk Encryption is utilized in the Democracy Suite, but a third-party forensic audit in Michigan said that the Dominion disks were not encrypted. The implementation of disk encryption must be verified.

**Add a system log and alarm to warn of ethernet traffic, especially from outside the voting machine's network scope.** The Dominion system has the capability for ethernet connections, but we're told no connection to the internet was intentionally in place to any of the connected devices. A system log

[1] https://www.heritage.org/election-integrity/commentary/election-integrity-national-imperative
[2] https://www.dailysignal.com/2021/02/02/9-election-reforms-states-can-implement-to-prevent-mistakes-and-vote-fraud/

should be enabled in the operating system to record any ethernet traffic and to alarm on any traffic that originates or has a destination IP outside of the voting machine network's scope.

**No OS or hardware changes should be allowed that haven't been approved, tested and certified at least 90 days prior to an election**. The Dominion manual provides instructions for the update of scanner drivers; if requested by the OS, this is a significant vulnerability. No software changes should be allowed that have not been specifically tested and certified for use. This is especially inappropriate for something as critical as a scanner driver which is essentially the interface between the scanning of the ballot and the reporting of scanning results to the election software. Security Certificates required for the function of the EMS should be checked to ensure they are valid and will not expire during the election period and are issued by a viable third-party provider. Upon receipt a random hardware audit should be performed (e.g., remove outer shell) to confirm no ethernet or other internet modem cards are found on motherboards, or otherwise clandestinely installed unless they have been physically and irreversibly disabled.

**Direct access to files within the system must be eliminated and logged if an Administrator accesses them**. Encryption should be at the application level whereby a computer user or admin cannot access voting results from the operating system and thereby bypass the security of the voting software. It is reported that Dominion's current practice is to delete bad "batches" of votes that need to be rescanned at the OS level in MS File Explorer leaving no trace of this activity in the application logs. These files are apparently unprotected and available to any user in the C:\dvs\project\ folder of the Window's C: drive. Direct access to the files must be eliminated and if Administrator access occurs it must be logged.

**Prior to – and after -- any day's vote, a software verification hash to verify the proper software version and integrity – as well as any modifications through the day -- should be run and documented**. A software verification hash should be run on each voting system to verify the proper software version and integrity both before voting is commenced and to ensure no modifications occur during the voting process it should be run again after the voting and reporting is completed. The Dominion manual only appears to currently stipulate this during setup.

**All application-specific passwords should be managed by the user and required to be changed on first login to the system and changed on demand if it is believed they have been compromised**. Administrator and Supervisor accounts within the Democracy Suite software have significant configuration privileges and their passwords are managed in the Election Event Designer. Functionality should be provided that these application-specific passwords are managed by the user and required to be changed on their first login to the system and be changed on demand should the owner believe their password may have been compromised. The EMS should have advanced user security where all actions are tracked within the system by a unique and individual login. Broad user role-based security (e.g., only one or two levels of roles per software module) and one login to multiple users should be prohibited.

**All printed reports should come directly from the election software and not funneled through a third-party process or platform**. The procedure is specified in the Democracy Suite User Guide of running a report to the screen, then "Select all of the data in the window and copy/paste it to Notepad" then "In Notepad, print the content and save the report for audit purposes." This was recommended as a zero documentation prior to tabulating votes; a relatively critical step. This procedure neither ensures that

the printed data was not modified while in Notepad prior to being printed nor does it provide a reliable log of the report for auditing. All printed reports should come directly from the Election Software and not be funneled through a third-party process where integrity can be compromised.

**A log-in should be required for both dual-party poll workers and observers in all stages of election processing**. Dual party poll workers and observers were reported absent in some stages of the voting procedure. It is the policy of some counties that dual party participants be present at some stages of election processing such as ballot adjudication. It would be advisable that the system require a login from both party workers in order to accomplish these processes. This is believed not to be currently available in Dominion.

**Every voting system in use must provide all users with separate UIDs with forced password changes at first login and security-minded password management**. A shared and simplistic password was used by Williamson County each day of early voting. This eliminates traceability to a user in the audit log and presents the opportunity for off hours, inappropriate scanning to occur without being able to audit the user associated with that login. The system must provide all users with separate UIDs with forced password changes at first login and provide a well-designed password management.

**Microsoft Winevt logs for applications should be enabled and security and system events set to archive and not overwrite**. Microsoft Winevt logs for applications and removable storage devices should be enabled and security and system events set to archive and not overwrite. These files should be reviewed at least on a statistically significant basis after the election with inappropriate findings resulting in a hand recount.

**Paper ballot OR codes should be unencrypted and able to be read by the voter to assure the ballot is correctly reporting his/her ballot choices**. QR barcodes are printed on the paper ballots in some of the Dominion system ballots to facilitate scanning. The QR codes ostensibly contain the same voter selections as are printed on the ballot in open text. But the QR codes are encrypted, frustrating any attempt to verify their content. Notwithstanding any good reason for this, these QR codes should be required to be unencrypted.

**The Dominion Results Tally and Reporting (RYR) system definitively allows for mass vote changing downstream from the precinct.** On September 7, 2021, following a deeper study of the Dominion manuals, we sent the following question to Director of Elections Mark Goins for an answer. We asked him to include this question in a list of questions we requested he seek answers to from Dominion:

> Information we found in the latest manual implies the Dominion Results Tally and Reporting (RTR) system allows for mass vote changing by deleting results previously entered from secure removable media and replacing them with data from a local file… with no dual-party authentication required. We've also seen that reports can be published to "Public" transfer points inferring that there is at least an indirect connection to the internet. Additionally, it seems that remote clients can communicate with the server through Dominion… again inferring a network connection. Can you clarify this conclusion?

After submitting this mid-2021, we have heard nothing back either from Goins, the Secretary of State's office or Dominion. However, we have heard a frightening answer from the Williamson County Election Commission employees.

In studying the RTR manual, it was plain that the system could allow mass vote changing by voiding results previously entered from secure removable media from the vote tally and replacing them with data from another file or by manual entry. This can be done by a single individual with access to the system and with no dual-party authentication or other oversight required.

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.

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 interviewed. 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, we feel that the controls protecting against such an action are dangerously inadequate.

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 is making 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. (As an aside, Dominion performed a software update on our system in January '21, it has been reported from other locations that this upgrade writes over the digital log files that would have been written for the 2020 general election. Williamson county currently considers only paper records as election artifacts that must be retained for 22 months after an election. As a result of our queries, they are now asking for clarification as to whether digital records must also be retained.)

So, it appears that thousands of votes could 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 is currently a trustworthy person at the helm of the RTR in Williamson County. But this is a technology hole that must be addressed!

**Best Practice Solutions: Process**

**Include IT/data/cyber security/process control professionals in review committee**. The evaluation team should include IT, data, cyber security professionals, as well as industrial/process engineering skills in the evaluation and decision making. The team can also include lay person members including functional experts in the election processes who can act as the liaison between the end user and the

technical engineers. The findings should be transparent and published for other states to utilize should they desire.

**County election officials must ensure sufficient training resources for volunteers to staff and operate the election fully, without the involvement of the machine/software vendor**. The State Election Commission should consider the value of providing or approving training resources for each of the approved systems that can be utilized by the counties rather than having each county duplicate this effort with more limited resources. The training should be consistent and thorough so that no employee or contractor of the voting machine vendor is needed to run or manage a portion of the voting and counting process on or around election day. From witnessing parts of Williamson County's election process, we don't think this is happening as a Dominion employee appeared to be the only employee able to run the absentee voting ballot processing. When the employee was called away to address other technology issues elsewhere, processing in this area ground to a complete halt for three hours. This is unacceptable.

**Require dual party poll workers at key steps**. Dual-party poll workers or observers should be allowed, or, better, required, at critical portions of the process, specifically including:

- Opening of a tabulation procedure;
- Closing of a tabulation procedure;
- Discarding a batch of ballots;
- Reopening a Poll ID for additional ballots;
- The printing of Start, interval and ending status reports; and
- The adjudication of ballots.

**Protections to ensure ease for dual party observers**. In areas of the process where dual party observers are allowed a view of the activity, they must be given an unobstructed view equivalent to those preforming the process. Pictures and video should be allowed throughout the process with the sole exceptions of where a voter's identity and their ballots selections can be connected and where security passwords are entered into voting systems. There should be severe penalties when views of the process for duly appointed observers are prevented.

**Place cameras in polling/precinct/ballot processing areas to publicly stream video of activity to increase transparency**. Cameras should be placed in polling/precinct/ballot county/election processing areas for public viewing of these activities. Just not in a way that can connect a voter's identity and ballot selections. If a citizen can secure his home with a few cameras and an inexpensive security program, voting centers, precincts and ballot counting areas should be able to easily, and affordably, be transparent and allow the public to witness activities in these areas via the internet.

**Formally specify and document the criteria and process for archiving voting artifacts**. The level of securing the archives of voting artifacts and the criteria and process for access to these archives should be formally specified. Prior to a "live" election period, all Election Event Design, Adjudication, and any other administrative software settings should be captured and "locked." A GUI and database (presumably where these settings are stored and then displayed by the GUI) snapshot should be produced, archived, and secured. This should create a "certified" election settings artifact. If any changes need to be made, dual observers should be present to review the specific settings, ensure the

implemented change functions as expected, and then a secondary certified election settings artifact created. These should be maintained for 22 months.

**Require a printed zero report as well as status reports at the beginning and end of each working period, in front of dual observers and retained for the appropriate retention period in a physically secure location**. Dominion "recommends" in their manual that the printed zero report (ensures no votes are present in the system at the beginning of tabulations) be kept in a physically secure location for a period of at least 22 months. This should be required and, in addition, such status reports should be produced and secured at the beginning and end of each working period at a time when dual observers arrive and depart from the operations.

**Independent validation of accurate transfer of votes to next level of consolidation**. A dual-party validation should occur and be documented at each voting jurisdiction whereby local vote tallies are verified through a separate means than the original reporting against a read-only access to the tallies that were attributed to them in the consolidated location. Failure to pass and document this validation should be cause for a reconsolidation.

**Appropriate chain of custody is a must and should be audited prior to certification of vote**. Questions have arisen regarding adequate chain of custody and documentation in Williamson County in transmission and consolidation of votes from polling locations to the county and ultimately the state and national levels. A verification of the chains of custody should be audited prior to certification of the vote. Failure to pass and document this validation should be cause for a reconsolidation.

**800 phone number to report election issues throughout Tennessee**. TEC should consider the setup and running of an 800 service for local citizens to report possible improper election issues

**Standard operating procedures and process charts should be developed for every voting process to ensure concise, consistent communications leading to a high quality, highly trustworthy election result by a disparate team of volunteers and workers**. When any manufacturer wants to ensure consistent, systematic quality in every single product or piece of a product that it manufactures, it implements standard operating procedures and process charts.

Standard operating procedures and process charts are step-by-step instructions detailing how a process should proceed by either one person or multiple persons to ensure the outcome is consistently the same, regardless who performs it or how long it takes to perform it. <u>These "blueprints" are a manual that involves detailed procedures of tasks so that anyone who enters a process can execute it fully and effectively simply by following the steps on the sheet so that the finished outcome/product from the complete manufacturing team is of high, consistent quality</u>.

In the case of voting, the "manufacturing process" includes all of the steps that all of the volunteers working the election need to take to ensure their particular portion of the process is completed with high integrity. Whether they work the set-up, maintenance and security of the voting equipment, the registration process, the voting process or the counting/reporting process, each person must follow a precise step-by-step course to ensure the highest quality, consistent outcome.

This is especially critical in an election as a majority of individuals working elections are dissimilar volunteers and the results of a trustworthy, accurate, transparent election are critical… with everyone being counted on to do precisely the right thing.

Despite our requests to see them, to our knowledge, detailed process charts and standard operating procedures do not exist for any of the procedures that are necessary in elections in Williamson County. We are aware there is some type of training process, but we've not been privy to that information. This means people working the election might cavalierly freelance their way through their jobs in the various precincts or stages of processing the votes if not shown precisely what they need to do and how they need to do it. Meaning outcomes might be unduly erratic or untrustworthy.

We also strongly suggest that an overall Process Flow Diagram tracing the actual "vote" that lays out its chain of custody is paramount to ensure a robust system. Secondly, standard operating procedures and process charts should be developed by a process engineer to ensure that communications of all duties to all workers in all elections in Williamson County is clear, consistent, effective, leading to a high quality, highly trustworthy election result by a disparate team of workers.

**Require Voluntary Voting System Guidelines 2.0 certification**. In recertifying or replacing Dominion or other voting systems, the commission should demand that the system be certified against the VVSG (Voluntary Voting System Guidelines) provided by the United States Election Assistance Commission (EAC). The VVSG Version 2.0 was just adopted on February 10, 2021. It appears to be a robust set of criteria for both election systems and procedures, with the latest version offering significant upgrades in the areas of system integrity, cyber security, data protections, auditability, and testing.

(Unfortunately, the EAC has just approved allowing vendors to make changes in these standards such as allowing machines to contain wireless network devices. The move has cost the EAC one of its lead Board members who has resigned because of this irrational move and is now suing the EAC.)

Dominion and all five voting systems on we vote in Tennessee are currently certified only to a Version 1.0 from 2005 and has not been certified to either of new newer versions of VVSG (version 1.1 adopted in 2015, or version 2.0 adopted in 2021). The first iPhone was launched in 2007 and is more secure, has greater technology guardrails and is certified higher than any of the equipment on which we vote in Tennessee. That is frightening.

**Develop a Minimum Voting System Requirements (MVSR) mapped to VVSG 2.0 for Tennessee software selection and certification process.** As of May 27, 2021, no voting systems used in Tennessee have been Election Assistance Commission (EAC)-certified to be compliant with VVSG 1.1 or VVSG 2.0, according to Jonathon Panek, EAC Testing and Certification Director. This is frightening since our smart phones are far more secure, updated and certified to much more current, stringent, security standards than our voting equipment! The newer guidelines provide more robust security safeguards and should strongly be considered as critical standards to be met in a risk audit or recertification process. Since no software vendor is likely to immediately be compliant with VVSG 2.0 during this current process, it is recommended the Tennessee Election Commission develop their own minimum requirements for Tennessee voting systems by identifying and prioritizing VVSG 2.0 standards. This document would then

be used to evaluate and certify the top five software vendor brands. A further step would be to outline not only the systems, but the processes by type of voting that are certified for use in Tennessee.

**Other state evaluations**. Evaluations by other states and the election software solutions they are considering should be reviewed and any concerns found should be investigated and considered in the Tennessee decisions.

**Best Practice Solutions: Legislative**

**Each voting system should use and retain paper ballots; Digital Recording Electronic systems (DREs) without paper ballots should be eliminated**. Tennessee counties can choose from a selection of five voting systems, all with a variant of versions that are either DREs or BMDs (ballot marking devices). Currently, Tennessee counties use MicroVote (46), Hart (25), ES&S (20), Unisyn (2) and Dominion (2) systems. For instance, we understand that there are currently two versions of Dominion SW in use, one provides a paper ballot audit trail, the other does not, a significant variation. Because of increasing election-related issues that could require an audit, all voting machine systems should provide a paper-based archive of each vote to easily and efficiently provide for quickly establishing an audit trail, if necessary. (DRE voting devices without VVPAT should not be considered viable for reliable or auditable election audits because the stored vote tallies are under the control of precinct voting machine software that can be maliciously altered. Additionally, since the Tennessee code verification of a voter-verified paper ballot" means a permanent, individual paper ballot that is marked either manually by the voter or with the assistance of a device and verified by the voter as correctly reflecting the voter's intent, the VVPAT would not meet this definition because the ballot is not "individual.")

**Replace the current post-election mandatory audit of just optical scanners/tabulators, as specified in the Voter Confidence Act (TCA 2-20-103), with a two-pronged audit process.** The current election Voter Confidence Act dangerously enables overconfidence in the auditing results after a Tennessee election because this audit does not include a hand count of paper ballots election selections. It only audits one third of the end-to-end process: The Vote-Cast-to-Vote-Count portion of the process involving only the optical scanner/tabulator, located in the middle of the complete voting process. It leaves out two key parts: the Voter-Intent-to-Vote Cast portion (hand counted paper ballot) and the Vote-Count-to-Vote Tally portion (election results reporting). Tennesseans may believe this audit is sufficient, but our research has proved it's not.

First, we strongly advocate for a paper ballot or backup ballot to be mandatory across Tennessee. Currently, there are three options for this in each county:

1. A hand-marked paper ballot must be available to be scanned by an optical scanner/tabulator;
2. A Voter Verified Paper Audit Trail (VVPAT) printer with ballot roll tape needs to be added to existing DREs (where available) so a paper trail can be audited on these machines that create no paper ballots; or
3. A voting machine-printed human readable ballot containing a bar or QR code to be scanned into an optical scanner tabulator and then retained as paper ballot in a storage box.

The great thing for this recommendation is that rather than spend funds on more technology in electronics, this is actually placing more financial and technology in the ballot, which is cheaper and more secure!

We also strongly advocate that Williamson County return to precinct voting in order to enjoy smaller precincts for voting, ballot maintenance and ease of counting.

Then, we recommend that as soon as the precinct has closed, that a new, fresh team of counters check into the precinct and count all ballots, which, depending upon the size of the precinct, may take 3-4 hours. The count is streamed live and videotaped for citizens to witness. Counters will know that they are being watched which should also improve honesty. The count becomes the mandatory audit. And is reported to the Elections Office at that point.

But, then, let's take it a step further.

The day after the election, the Williamson County Election Commission should post all ballot images online, which, since there is no personal identification on the ballots, should not be a problem. Additionally, WCEC should post key election documentation/poll officer forms, as well as the locked, pre-election voter list so citizens could do their own audit of the election from top to bottom. Call it the People's Audit.

As we have advocated for a randomized number be placed on every ballot, this process could also mean that with the high-security, hand-marked paper ballot that we are recommending, voters could check the processing of their ballot, by number, and rest assured it was counted as they cast it.

Coupled with the Operational Audit, which we're also recommending, that uses an independent auditor to audit every Tennessee county election commission and their processes every five years, citizens should have much greater comfort that the election is fair and secure.

**Amend the law banning paper ballots for audits.** Tennessee Code 2-19-111 makes opening the ballot box, examining any voter's marked ballot, removing the ballot from the ballot box, preventing the ballot being placed in the ballot box or destroying or changing a voter's ballot a Class A misdemeanor. This section needs to be amended to allow an exception for conducting the Mandatory post-election statistical random sample paper ballot hand-counted Risk Limiting Audit.

**All software configurations should be dictated by the state to ensure consistency in vote**. The Dominion Democracy Suite allows for numerous configurations during setup. All of these should be dictated by the state as a requirement for each of the approved systems as should a similar set of configurations for other software suites. Specific items for Dominion should include but are not limited to:

- Allowing an operator to close a poll requiring an Admin to reopen;
- Selection of scanner exceptions that will stop the scanner versus adjudication;
- Options for all-batch summary reports to be printing for archive detailing batch #, scanner ID, time of scan and number of ballots; and
- Assigning a Poll ID to each ballot.

**No vendor employees working election processes; no outsourcing the election to the software vendor**. At no time should an employee or contractor of an election voting equipment company or related company be performing any step in the voting and ballot counting process.

Yes, some voting systems require a higher dependency on the software vendor than others. Software errors, crude manual processes, administration passwords on the vendor, frequent fixes and substandard training can create a dependency environment. Having little or no technical expertise, the county essentially outsources the election to the software vendor. Software vendor contracts provides for an onsite programmer free of charge for a limited number of elections and pay-as-you-go thereafter. The danger here is that the software vendor runs the operation with the ability to change software on the fly. This creates not only a vulnerability of software misbehaving, but the fact that such last-minute changes virtually de-certifies the election equipment.

For instance, a Dominion employee was reported as the only one that appeared able to scan absentee ballots into the system at one Williamson County absentee ballot tallying location last November. That is unacceptable in and of itself. However, this employee had to leave this area to fix another technology issue and the counting ground to a halt for three hours. All routine processes in the election software should be performed by trained local workers/ volunteers independent of the software developer/ voting equipment vendor and with dual party involvement where appropriate. And training should be significantly beefed up to assure this is the case.

The Tennessee Election Commission should be aware of this when certifying voting systems and demand sufficient training to ensure no election equipment employee, in essence, runs the county's election.

**Standardize requirements for vote certification throughout all counties and the state**. Impose a standardized set of requirements for county and state voting that must be met prior to votes being certified. The TEC should create a standard list of Reports that all counties should produce for public review during the Election Result Certification process and final certified Reports. The TEC should also create standard internal reporting for all Ballot Images, and Ballot Image Histories in the case of adjudication.

**Take critical steps regarding absentee ballot**s.

- Limit absentee ballots to valid excuses and require validated witnesses. Only allow for unusual circumstance such as hospitalization, nursing home residents and out of district for the entire period of early voting and election day.
- All absentee ballots must be received by election day at close of polls.
- All absentee ballots must be printed on uniform, watermarked paper. (Achieved by General Assembly – Thank you!)
- Aggressively enforce law against vote trafficking/ballot harvesting.
- Design/pretest ballots to ensure smooth counting with no false adjudications.
    - There was an unusually large list of presidential candidates on the Williamson County ballot in November 2020 causing the absentee ballot form to be abnormally long (approximately 16 inches with 3 folds). Scanning a batch of 100 ballots through the Dominion optical scanner successfully the first time was almost impossible unless

someone stood at the output tray and flattened the bunched-up ballots to more easily feed them through. Upon jamming often, the file had to be deleted with File Explorer and the ballots re-flattened to re-scan once more. Additionally, because of the scanning and re-scanning there was uncertainty as to whether ballot hand markings at the fold lines or elsewhere were recorded accurately. The company that prints the absentee ballots should be forced to design the ballot in such a way that folds and other inerrant marks don't force the ballot into adjudication or prevent ballots from passing smoothly through counting. It is also recommended that every ballot form be machine-tested weeks before the ballots are needed to prevent these problems.

**Laws and punishments for tampering with our election system should be greatly strengthened**. Voting is the most sacred gift American citizens hold. It is the center point of our liberty… our voice as Americans… the right to select our leaders and have our voice be properly cast and registered every time we do so. Americans must trust that their voice is rightfully heard and anyone who meddles with that process should be significantly punished. Anyone found guilty of tampering with an election should be held accountable, subject to heavy financial penalty, in addition to mandatory prison time of three-to-seven years, depending upon the situation and severity. But criminals no longer fear being held accountable for what they might do to our election system. Laws are weak and enforcement is likewise. That MUST change and legislators MUST add teeth to all laws and punishments guarding our election process. Legislators MUST strengthen election laws and associated punishments and unleash law enforcement entities to find and punish criminals who are, in essence, creating treason. We owe that to our Founding Fathers… and to every citizen of America today.

But we don't want to stop with just our own recommendations. We add here best practice recommendations that have been developed by Heritage Foundation experts based on long experience in the area of election integrity. In "The Facts About Election Integrity and the Need for States to Fix Their Election Systems,"[3] these experts address:

- Voter registration
  - Verify the accuracy of voter registration lists
  - Verify citizenship of voters
- In-person and absentee voting
  - Require voter ID
  - Limit absentee ballots
  - Prevent vote trafficking
  - Allow election observers complete access to the election process
  - Provide voting assistance
- Counting votes
  - Prohibit early vote counting
- Election litigation
  - Provide state legislatures with legal standing
- Other
  - No same day registration
  - No automatic voter registration

[3] https://www.heritage.org/election-integrity-facts

- No private funding of election officials and government agencies

These recommendations provide sound solutions that will lead to trustworthy elections.

**Recommendation**

We strongly recommend that Tennessee establish a bi-partisan, independent citizen committee to evaluate these weaknesses statewide and make further recommendations to address them. The committee should include credentialed data/internal/process control experts, as well as IT/cybersecurity experts to work on addressing them. But no vendors. These issues are well documented and the solutions – some from national election integrity sources – are sensible.

**Conclusion**

Addressing these issues will go far in restoring consumer/citizen trust and credibility in our election system.

###