TENNESSEE VOTERS
FOR ELECTION INTEGRITY

Op-Ed for Tennessee Conservative News
October 15, 2025

OUTDATED SOFTWARE UNSUPPORTED BY MICROSOFT RAISES CONCERNS ABOUT TENNESSEE'S ELECTION MACHINES AND SECURITY

Citizens place a lot of trust in their state's and county's election commission and process. But when something basic that should be implemented by election officials to protect the security of an election isn't done, that trust is suddenly in doubt — and with good reason.

On Monday, October 13, 2025, new election integrity information emerged during an election commission meeting in Williamson County that should make voters of all parties in counties across the state alarmed about the security of their votes.

Before explaining this new information, a little background may be helpful.

During the 2021 Franklin Municipal election, seven of nineteen optical scanners/tabulators suddenly stopped counting votes on their tabulator tapes. The election was declared an incomplete election by the Tennessee Secretary of State, and a complete hand recount was performed the next day to decide who won.

Later, national election officials were unable to identify the root cause of the issue while the vendor – Dominion Voting Machines – said the cause was "erroneous code present." The issue became known as the "Tennessee Error," which later showed up in most of the voting machines in Georgia.

The root cause of how the "erroneous code" got into machines that had passed pre-election logic and accuracy testing has never been explained. One of the concerns we have with using machines in elections.

While Tennessee does a decent job with elections, unfortunately, the election processes in our state are riddled with machines that have failed in elections around the nation and import great risk. Keep in mind that no one is allowed to inspect the inner workings of these machines before, during or after an election – not even election or state officials. So, we have no idea what, if any, potentially nefarious components are in them that can affect the election and cause a different result than the majority of voters intended.

Thanks to cyber researchers nationwide (here and here), a few politicians (here and here) and even some journalists, it's been proven that there are grave issues with the equipment. Yes, even Williamson County's own ES&S voting equipment.

Many, if not most, of the voting machines across the state have been running on Microsoft 10. Williamson County's ES&S system – epollbook, ballot marking devices, optical scanners/ tabulators and registration laptop computers – all run on Microsoft 10. And when that software is supported by Microsoft, technical support, upgrades and security patches have been available to add protection to the computers against malware and other security concerns in the marketplace that can affect how the machine performs.

But this past Tuesday, October 14, 2025, was the end-of-life date for Microsoft 10, which means all Microsoft support, upgrades and security patches ceased for that version of the software.

Now, here's the new information I promised.

At a Monday, October 13, 2025 meeting of the Williamson County Election Commission (WCEC), which I attended, it was learned that all Williamson County election equipment is still running on Microsoft 10. The voting machines have not been upgraded to Windows 11, which was available as of October 5, 2021, and won't be upgraded until after the December 2, 2025 District 7 Congressional general election.

So, in essence, since before the machines were set up on September 8, 2025 for the District 7 and BOMA elections, they have been running Windows 10 and they will not be immune to the variety of security issues that have invaded the marketplace since that date.

Eighty-five days of unsupported software on our voting machines.

When confronted at the meeting with this information, WCEC Chairman Jonathan Duda confirmed that the machines were still running Windows 10, but he said the system is just fine without the upgrade and its security patches. Duda went on to say that VPNs were in place and were sufficient protection. He only allowed me to ask one follow-up question before cutting me off. I couldn't ask about this security gap, how it was being handled during the current election in progress nor how it could potentially affect upcoming elections.

In research my organization, Tennessee Voters for Election Integrity, performed three years ago on the performance of VPNs, we uncovered concerns that VPNs are not as trustworthy as the commission thinks. Additionally, in another research project, we tracked a number of companies over a two-year period that are spending abundantly more on data security measures – with and without VPNs -- that greatly surpass what the Williamson County Election Commission is spending on data security. Yet those companies are still being breached.

And here's the statewide concern.

This election security danger doesn't affect just Williamson County; it also affects every county in the state which is using election equipment still running on Windows 10. This is not an issue confined to Republican, Democrat or voters in any other party; it affects us all.

Three years ago, at the January 10, 2022 meeting of the Tennessee State Election Commission (SEC), a representative of Hart InterCivic Voting Machines sought state approval for a change in Hart's equipment. They wanted to move all of their machines in the state – at that time found in twelve counties -- from using Windows 7 to using Windows 10 (see page 24). No SEC commissioner seemed bothered by the request.

But what the SEC apparently didn't know was that the end-of-life date for Windows 7 occurred on January 14, 2020, two years prior. So, during the 2020 and 2021 elections, every Hart voting machine in the state was conceivably running on Windows 7 and susceptible to manipulated votes because the machines most likely weren't being security patched for those two years. Hart obviously wasn't patching them; were the local commissions? Tennessee Election Coordinator Mark Goins was informed of this situation, but he never acknowledged the issue and ignored my questions.

Just as in the case of Williamson County now, we doubt most county election commissions were aware of the software security problem then. If the SEC was aware of the end-of-life issue, they certainly didn't tell those counties with Hart election equipment, otherwise the January 10, 2025, upgrade would have already been done. The SEC left those commissions then – and Williamson County now – hanging by not being aware of and informing them of the needed software upgrade.

So, too, did Hart InterCivic, which apparently didn't tell their customers – the State of Tennessee or its counties using their equipment – about the need for the upgrade back in 2020. Another reason it's hard to trust any of these election equipment vendors.

But the local election commission should have known and acted proactively, too.

So, the challenge now is for every voter to ask their county election commission if their county's voting equipment is still running on Windows 10. (Request proof!) And, if so, what are they doing to mitigate the security issue? Or if in the middle of an election, how will they protect their voting machines during the election from nefarious intrusions that could impact the outcome?

The key question all Tennessee voters need to ask election officials is this: "How can I be sure my vote is secure and was credited to the appropriate candidate?"

We have a serious issue here that goes far beyond a simple VPN for a solution.

Frank Limpus
Tennessee Voters for Election Integrity

###