



### THIRTEEN SIMILARITIES BETWEEN DOMINION AND ES&S VOTING MACHINE SYSTEMS\*

*The ES&S system is remarkably like the Dominion system we kicked out of Williamson County in 2022*

If the Williamson County Election Commission (WCEC) is bent on giving us more and more machines on which to vote, have they ever considered that it was the failure of voting machines in the October 2021 election that put us in this position?

Here are thirteen parallels between Dominion and ES&S voting machine systems that prove when the WCEC successfully purchased more machines, Williamson County stepped from the frying pan back into the fire of machine vulnerabilities.

*“Those that cannot remember the past are condemned to repeat it.”  
-- Writer and Philosopher George Santayana*

1. The **architecture is generally the same**: Ballot marking devices, scanner/tabulators and the election management (EMS) central system with all software and hardware. Both Dominion and ES&S are proprietary, closed, secret systems and neither citizens nor cyber experts are allowed unfettered access to jointly inspect the machines.
2. Both systems were originally **certified ONLY to the Voluntary Voting System Guidelines (VVSG) 1.0, established in 2005** by the Election Assistance Commission (EAC). Neither system is certified to VVSG 1.1, established in 2015, or VVSG 2.0, established in 2021. According to our Secretary of State and our county election commission, neither company will upgrade their security certifications to VVSG 2.0 until 2026, at the earliest. Five years AFTER the most recent standards were established and 21 years AFTER the original standards were established.
3. Both Dominion and ES&S produce **paper ballots that are NOT truly voter-verifiable** because they use a QR code (Dominion) or a bar code (ES&S) in which they encase a voter's ballot selections. The scanners read the bar code/QR code, NOT the written text on the ballot. The QR/bar codes cannot be read by a voter in the ballot box to verify that the QR code/bar code properly reflects – and will cast – the selections that the voter just made on his ballot. [Alex Halderman just proved this true.](#) This is one reason why voting-security experts recommend [hand-marked paper ballots that are used in 68% of the elections throughout the United States](#) and in many other countries (UK, Germany, Japan, Taiwan, etc.).
4. Per the Dominion EMS user manual, **there is a back door in the election management system** (EMS) at the Results, Tally & Reporting (RTR) section where votes in the system can be extracted and different votes inserted into the system. An employee of the WCEC and a cybersecurity expert, Clay Parikh, have both confirmed this gross vulnerability to be true. The manual also implies the system provides internet access, a question we've asked, yet has never been answered for us by the WCEC, the State Election Commission (SEC), Tre Hargett, Mark Goins or Dominion. In 2021, WCEC Chairman Jonathan Duda confirmed to the Tennessee Voters for Election Integrity that the ES&S EMS has the same back door access point as the Dominion system. This is not a mistake... it is a FEATURE of all of these machines, according to Duda.
5. A number of **components (such as chips) in the Dominion and ES&S voting machines are made in China**, which is definitively a vulnerability. This is confirmed via news reports, and, in ES&S' case, [by a national NBC News TV interview here with the company's CEO.](#) Neither company allows free cybersecurity access

to the machines so experts can check for iDRAC, Telit or Qualcomm chips, which have been found in voting machines and enable wireless transmission.

6. Both systems **utilize USB ports, which provide sources of vulnerability** for tampering and introduction of malware.
7. The management **software of both systems uses .NET, IIS and SQL, which are sources of vulnerability** to hacking and vote tampering.
8. **The software and user interfaces of both systems are produced, in part, by contractors, with little accountability.** At times, these contractors are foreign nationals. This is a security weakness because parties can influence such contractors (or provide such contractors) to build back doors or other malware into code. Also, low-priced contractors have been sources of sloppy code that creates security problems.
9. According to the professionals who test the systems for vulnerabilities and provide reports of that testing, **the operating systems for these vendors are not kept up to date with security patches.** This creates systems with known vulnerabilities and exploits.
10. **Numerous, identical vulnerabilities have been reported in both systems,** such as easy-to-crack (sometimes unencrypted) passwords, unpatched operating system exploits, exploits from sloppy coding, complications in configuration that can lead to misconfiguration and then failures on voting day, etc.
11. Government and cyber experts say the potential for cyberattacks on election infrastructure continues to be a growing threat to national security. According to voting-system testing experts, **neither system is routinely or thoroughly penetration-tested.** This testing, which is different than Logic & Accuracy testing, which is supposed to be performed by election officials on all machines prior to an election, is designed to probe and disclose bugs in voting machines or source code and provide actionable insights into discovered vulnerabilities and potential attack paths. It is not required by the EAC but its absence means that there can be a large number of vulnerabilities that are not flagged and be fixed before use in elections.
12. **Both Dominion and ES&S have common mechanical and structural roots** that go back to Diebold Machines. [As this article proves, Diebold, Premier, Dominion and ES&S machines share structural, ownership and historical commonalities.](#) Today, three companies control 90% of the voting machines in the US – ES&S, Dominion and Hart InterCivic. That already is a concerningly concentrated control. It is more concerning when there are mechanical links between the companies, as well.
13. **Both Dominion and ES&S are private companies,** meaning the funding, control, decision-making, shareholders, etc. that oversee the companies and the moves they make are unknown to the public. **There is NO transparency here... but we're forced to trust our votes to these companies and their opaque machines.** Dominion = State Street Capital (New York City). ES&S = McCarthy Group LLC (Omaha)

*\* This comparative data has been compiled and verified by the work of two Texas-based election integrity investigators, one of whom has hacked into these machines, as well as several Franklin and Nashville-based IT cybersecurity experts.*

###