Laura Carlson – lauracarlson@protonmail.com

Vote centers necessitate the use of internet-connected, electronic pollbooks. All of the poll book providers have suites of centralized, all-inclusive software that do everything in the election and voter registration process (even campaign finance reporting) except shove paper ballots thru a scanner. They can even process the tabulator electronic files and geolocate voters. So depending on how a county sets up their vote centers-they can potentially exposed the entire election to the internet and provide ways that 'results' can be overwritten. This is happening in NM. There is a video of the pollbooks adding votes after the close of polls in 2022 is quite powerful. These were KnowINK pollpads. Certain modules of these suites of software have been shown to be compromised-especially voter registration. There is no oversight of pollbook software except that provided by CIS-which takes money from Democracy Fund and hires owners of election software to lead teams that decide that non-voting software is safe and secure. CIS was also part of the scheme to censor discussion of the 2020 election. From last November where KnowINK pollpads stole an election while poll workers watched. And don't forget that KnowINK owns BPro-which illegally processes the entire election in NM thanks to Maggie Toulouse-Oliver. This is now CONFIRMED to be COUNTY WIDE in Dallas County, TX. We also have strong evidence that it happened in other states.

This lie have been perpetrated on the American public for too long. When you hear it, remember that following:

1. It's been proven that every vendor includes modems in their machines (many don't need a password)
2. CISA, EAC and the Halderman report have shown that all of the machines are remotely hackable. (actually watched a live hack on tv)
3. Several Secretaries of State have now openly admitted (some in legal documents) that their voting systems are remotely hackable.
4. All modern election systems employ what officials naively believe are 'internal secure networks'
5. Passwords for remote access to election systems are kept by the vendor and the SOS. (those are hackable)
6. Federal (home and security) malware protection hardware and software has been installed in nearly every US county, and it is readily hackable
7. Most US county networks use security protocols that have been readily hackable for several years

8. Any election systems that use portable media to transfer data are easily hackable (the military hasn't used thumb drives for years because that's how we hacked Iran's nuclear infrastructure)
9. Even our finest Air Force electronic systems are assumed to be hacked as their cyber security teams are endlessly detecting new hacks
10. Recounts and forensic images of computer systems have shown multiple cases of voter and ballot manipulation (proven in several court cases)
11. Etc, etc

Laura Carlson – lauracarlson@protonmail.com