RON HANKS FOR HOUSE DISTRICT 60

Merry Christmas to Christians around the world, and likewise I hope Jews around the world enjoyed a happy Hanukkah.

On 15 Dec. 2020, I attended the Legislative Audit Committee meeting on election integrity, which focused on Colorado's use of Dominion Voting Systems. It was a two-hour meeting that ultimately went more than eight. There was testimony of limited value, some of no value, and some that was quite remarkable. If you listen to no other portion of that testimony, I would recommend you listen to this segment: **https://www. bitchute.com/video/R55QCWT7a1Vm/**

When government proclaims their policy or program is the "Gold Standard", citizens are wise to be leery of what sounds more like a marketing slogan than factual evaluation. That was my takeaway after listening to those with a vested interest in an election that does not invite scrutiny or audit, and the testimony of experts who know how to secure equipment from intrusion and hacking.

In my assessment, many people who are quick and proud to declare Colorado elections the "Gold Standard" are simply not in a position to know all the vulnerabilities of the system: there is too much software code to analyze, too much proprietary information not provided by the voting and tabulation equipment vendors, [and] too many opportunities to insert computer instructions that alter the output.

In the course of my military career, I worked for Cyber Command. My exposure was some years ago and limited. But it was enough exposure to know how LITTLE I know about cyber, and to recognize I must rely on experts who are highly specialized and engaged in the trade. Colorado's Office of the Secretary of State should recognize their own lack of expertise, and reach out to cyber experts.

Defense systems and cyber experts will tell you that all systems are vulnerable unless there is lifecycle control and custody of the equipment. In other words, everything that goes into a system must be controlled – starting with the manufacturing of the chips and computer boards, and all software that is installed, including updates. Of course, all equipment has to be secured by trusted persons. There are no similar controls on any element of the Dominion Voting Systems. The hardware and software are not from a secure procurement chain, and the public access to the equipment during its use makes the entire system vulnerable, as may the varied storage methods and facilities throughout the state.

Security experts will tell you also that system integrity needs to be tested regularly. Military and public infrastructure systems are often tested by "Red Team" attacks, consisting of "white hat" hackers and cyber experts. There is no other way to know if new hacking techniques might allow intrusion. Colorado's Dominion Voting Systems has never undergone such testing. Instead, our "Gold Standard" is based on assurances of Dominion itself, and the security testing of Pro V&V, which provided a meager two-paragraph report. And it is not clear any employee of Pro V&V has ANY cybersecurity experience or expertise, whatsoever. Three company employees appear repeatedly on voter system certifications. One of them, Pro V&V's director, Jack Cobb, claims "no specialized knowledge or background in cybersecurity engineering."

Texas refused to certify Dominion software in 2013, 2019, and 2020, citing the examiner reports "raise concerns about whether the [Dominion] Democracy Suite 5.5A system is suitable for its intended purpose… and is safe from fraudulent or unauthorized manipulation." Colorado used Democracy Suite 5.11 – very similar to that rejected by Texas.

There have been repeated comments and assurances that the voting system is not connected to the internet. I invite anyone to go [to the] Colorado Secretary of State's website, find and click on election results, and watch your page get redirected to a webpage run by ClarityElections. ClarityElections is owned by Scytl, a private company in Barcelona, Spain, which has no servers in the United States. It would appear from testimony and evidence provided there is indeed connection to the internet during the voting and tabulation process, and those servers are indeed overseas.

Bottom Line: It would appear our "Gold Standard" election is starting to show some rust through the cheap golden veneer. Our voting systems ought to be seriously inspected, tested by experts, Red Teamed by white hat hackers. One could argue we have a "certificate of authenticity" worth little more than the "certificate" included with ceramic plates sold on TV at 3 a.m. Coloradans should demand audits and Red Team intrusion tests on any voting system. It shouldn't be a partisan issue: Honest Democrats and Republicans surely agree that election integrity ensures the peaceful transition of power. Yet, in the end, the Republican requests for audits and research into the election system failed on two separate votes, with the Democrats on that committee calling them a "witch hunt" and "fishing expedition". I reject that myopic and close-minded view, and so should Colorado. Honest elections matter.