I am writing to file a formal complaint against the following electronic voting, election management and reporting systems used in our state:

> Elections Systems & Software
> 11208 John Galt Blvd, Omaha, NE 68137
> (800) 247-8683
>
> AVANTE International Technology, Inc.
> 70 Washington Road, Princeton Junction, NJ 08550
> (609) 799-8896
>
> Dominion Voting Systems
> 717 17th St., Ste 310, Denver, CO 80202
> (416)762-1775; Ext 271
>
> Hart InterCivic
> 15500 Wells Port Drive, Austin, TX 78728
> (512) 252-6400

Counties throughout the state have procured expensive election systems from several vendors so that all of us can cast our votes and have them accurately counted as intended. Technical witnesses, for roughly two decades now, have been testifying that these systems have many vulnerabilities. This was evident in New Jersey when ES&S vote tabulation errors caused double counting in the November 2022 general election.

Alex Halderman wrote a report (see attached file) showing how vulnerable equipment and software used by Dominion is and recently in the Georgia case, Curling versus Raffensberger, he demonstrated one example of this. During the bench trial, he borrowed the main counsel's pen and used it to easily reboot equipment, put it into safe mode and open files to change them. He showed how to fix the results and rig the count during an election. For more details please refer to an archived account here -
https://archive.is/2024.01.21154924/https://www.thegatewaypundit.com/2024/01/gig-is-up-exclusive-local-reporter-describes election/

I also direct you to examine the legal affidavit of Terpsehore P. Maras (see attached file). Ms. Maras describes how Voting System Test Labs and certifications are very important because equipment vulnerabilities allow for deployment of algorithms and scripts to intercept, alter and adjust voting tallies. Our currently conducted state certification processes are sorely inadequate to safeguard from these attacks for many reasons, one being that they do not examine the use of COTS – Commercial Off The Shelf - parts. Ms. Maras describes the following:

> *COTS components by voting system machine manufacturers can be used as a "Black Box" and changes to their specs and hardware make up change continuously. Some changes can be simple upgrades to make them more efficient in operation, cost efficient for production, end of life (EOL) and even complete reworks to meet new standards. The key issue in this is that MOST of the COTS used by Election Machine Vendors like Dominion, ES&S, Hart*

Intercivic, Smartmatic and others is that such manufacturing for COTS have been outsourced to China which if implemented in our Election Machines make us vulnerable to BLACK BOX antics and backdoors due to hardware changes that can go undetected.

The proprietary voting system software is done so and created with cost efficiency in mind and therefore relies on 3rd party software that is AVAILABLE and HOUSED on the HARDWARE. This is a vulnerability. Exporting system reporting using software like Crystal Reports, or PDF software allows for vulnerabilities with their constant updates.

24. As per the COTS hardware components that are fixed, and origin may be cloaked under proprietary information a major vulnerability exists since once again third-party support software is dynamic and requires FREQUENT updates. The hardware components of the computer components, and election machines that are COTS may have slight updates that can be overlooked as they may be like those designed that support the other third -party software. COTS origin is important and the US Intelligence Community report in 2018 verifies that. Chinese manufacturers like Huawei that are the world's LARGEST supplier of telecom and other equipment that endangers national security.

26. China, is not the only nation involved in COTS provided to election machines or the networking but so is Germany via a LAOS founded Chinese linked cloud service company that works with SCYTL named Akamai Technologies that have offices in China and are linked to the server that Dominion Software. Scytl, who is contracted with AP that receives the results tallied BY Scytl on behalf of Dominion – During the elections the AP reporting site had a disclaimer. AP – powered by SCYTL. According to DOMINION : 1.4.1Software and Firmware The software and firmware employed by Dominion D-Suite 5.5-Aconsists of 2 types, custom and commercial off the shelf (COTS). COTS applications were verified to be pristine or were subjected to source code review for analysis of any modifications and verification of meeting the pertinent standards.

36. The concern is the HARDWARE and the NON – ACCREDITED VSTLs as by their own admittance use COTS.

37. The purpose of VSTL's being accredited and their importance in ensuring that there is no foreign interference/ bad actors accessing the tally data via backdoors in equipment software. The core software used by ALL SCYTL related Election Machine/Software manufacturers ensures "anonymity" .

38. Algorithms within the area of this "shuffling" to maintain anonymity allows for setting values to achieve a desired goal under the guise of "encryption" in the trap door.

> *39. The actual use of trapdoor commitments in Bayer Groth proofs demonstrate the implications for the verifiability factor. This means that no one can SEE what is going on during the process of the “shuffling” therefore even if you deploy algorithms or manual scripts to fractionalize or distribute pooled votes to achieve the outcome you wish – you cannot prove they are doing it! See STUDY : “The use of trapdoor commitments in Bayer Groth proofs and the implications for the verifiability of the Scytl-SwissPost Internet voting system” Scytl and Dominion have an agreement – only the two would know the parameters. This means that access is able to occur through backdoors in hardware if the parameters of the commitments are known in order to alter the range of the algorithm deployed to satisfy the outcome sought in the case of algorithm failure.*
>
> *55. Trapdoor is a cryptotech term that describes a state of a program that knows the commitment parameters and therefore is able change the value of the commitments however it likes. In other words, Scytl or anyone that knows the commitment parameters can take all the votes and give them to any one they want. If they have a total of 1000 votes an algorithm can distribute them among all races as it deems necessary to achieve the goals it wants. (Case Study: Estonia)*

Please review all 37 pages of the crucial data contained in Ms. Mara's Affidavit. For all the reasons above and more you will see that we have a complete failure to provide elections we can be confident in. Problems even exist with our processes that electronically select ballots to electronically re-count votes during risk limiting audits. Since the integrity of the voting process is at stake, the use of these vulnerable systems must cease. Accurate and honest vote counting is more important than speed and efficiency. If you truly believe that protecting our right to vote in a free and fair election is paramount to our Democratic Republic and that ensuring the integrity of this process is crucial then the only forward is with the use of hand marked, hand counted paper ballots. Taxpayers deserve consumer protection and an end to the use of overly expensive, technically complex vulnerable election systems that have no transparency afforded to us. A full investigation into this matter is past due and highly warranted.