At the last board meeting I had to endure the ad nauseum drum beat of being called a fascist, a racist, and an election denier by other members of the public and even by a couple members of the board at the end of the discussion.

I earned these pejorative labels because of my informed opinion that elections based on computerized black-box voting machines cannot be trusted to produce an accurate count of the vote.

Without a hand-count audit approaching 100%, there is no way to verify the results are accurate. I also believe that voters should provide photo ID to verify citizenship.

Those that are slinging these labels seem very committed to maintaining the status quo and claim that my opinions are baseless and lack evidence. On the contrary, there is an abundance of evidence to support my position, as I have detailed numerous times before the board.

Those that want to maintain the status quo often say that its dangerous to "do your own research" and to deviate from the legacy media narrative.

In the spirit of "doing your own research", I looked up the definitions of the pejorative terms.

**Fascism:** A government coerced alignment of commercial enterprise to a political ideology led by a dictator having complete power, forcibly suppressing opposition and criticism, regimenting all industry, commerce, etc.

Some recent familiar examples of fascism are:

1. Government pressure applied to private financial institutions to "de-bank" customers that criticize the government.
2. Government regulations designed to influence the distribution of private commerce based on political ideology.
3. Government coercion of business by executive orders applied through regulatory agencies.

**Racism:** A belief that race is a fundamental determinate of human traits and capacities and that racial differences produce an inherent superiority of one race over another. An example of racism is: Government or corporate hiring policies designed to give preference to applicants based on race as a primary factor.

**Election Denier:** Someone that questions the integrity or official results of an election. Throughout history, there are many examples of election denial following almost every election. These have only increased after the introduction

of computerized black box voting because the process of counting votes has been hidden from the voter.

I don't know how it is fascist or racist to request that the Board of Supervisors exercise their authority to ensure that the voting process in Ventura County has the highest integrity possible. So, I'll just dismiss these as coming from uninformed, ignorant, or otherwise motivated sources.

Even though "election denier" is a nonsensical, grade-schoolish label, I will proudly accept it as I've previously defined. I am here for the sole purpose of questioning election integrity.

As such, I question the conclusion of County Council North in her Report on the Authority of the Board of Supervisors in the Administration of Elections presented at the June 18th meeting.

I'm not a lawyer with a staff of 24 assistants, but the conclusion implying that the Board of Supervisors has subservient authority to the Registrar of Voters over the administration of elections seems to have a weak foundation, as it is based on an inconsequential case law opinion from a drunk driving case.

The Board of Supervisors represents the Executive and Legislative branches of county government and has the ability to create the Registrar of Voters office as an elected or appointed office, as part of combined offices, or as an individual entity.

Considering the current trajectory of increasing the complexity of voting processes to support unsecure computer systems, that will never be safe from sophisticated nation-state cyber-attacks. Maybe it's time to split the ROV off as a separate entity so they can focus more on security.

High-technology is not the answer to counting ballots and maintaining the voter rolls. Any cyber security improvements made today will be obsolete tomorrow. Protecting electronic voting systems is an unending impossible task, especially when combating nation states such as China and Russia.

Department of Homeland Security (DHS) Secretary Jeh Johnson released the following statement on January 6, 2017: "I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law."

https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) assess that People's Republic of China (PRC) state-sponsored cyber actors known as Volt Typhoon (also known as Vanguard Panda, BRONZE SILHOUETTE, Dev-0391, UNC3236, Voltzite, and Insidious Taurus) are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

Chinese cyber actors have already installed code to manipulate critical data or take down critical networks. This is even more disturbing when you read CISA's Election Infrastructure (EI) Subsector Cyber Risk Summary report for 2020. It reveals many security vulnerabilities.

From the report's Executive Summary, CISA's analysis of the available data for assessed EI entities found:

- 76% of EI entities for which CISA performed a Risk and Vulnerability Assessment (RVA) had spearphishing weaknesses, which provide an entry point for adversaries to launch attacks;
- 48% of entities had a critical or high severity vulnerability on at least one internet-accessible host,4 providing potential attack vectors to adversaries;
- 39% of entities ran at least one risky service on an internet-accessible host, providing the opportunity for threat actors to attack otherwise legitimate services; and
- 34% of entities ran unsupported operating systems (OSs) on at least one internet-accessible host, which exposes entities to compromise.

These results are less than adequate. Since a security chain is only as strong as its weakest link, CISA's own report indicates an overall security failure rate as high as 76%.

Now CISA has rolled out Project 2024 to help election officials and election infrastructure stakeholders protect against the cyber, physical, and operational security risks to election infrastructure during the 2024 election cycle.
https://www.cisa.gov/topics/election-security/protect2024

It's not clear how CISA plans to address the fact that Dominion sources election equipment Motherboards with built-in wireless modems from China as revealed in a recent internal Dominion email dump.

Let's pray that they have made some improvements over the 2020 election. Just last Friday, July 19th, a massive Microsoft outage sparked chaos around the world. Flights were grounded and hospitals, train services, banks, stock exchanges, TV channels, etc. were knocked offline.

The technical fault was caused by an update pushed out to customers of cybersecurity firm CrowdStrike which caused Windows software to suddenly shut down. The CEO for CrowdStrike reportedly said "the internet shutdown was successful test run for the real thing coming in November".

CrowdStrike was hired by the DNC in 2016 to investigate the suspected server hack that led to WikiLeaks publishing DNC emails. CrowdStrike attributed the hack to Russian intelligence, fueling the Russia collusion narrative. The truth, supported by Julian Assange, is that Seth Rich leaked the data to WikiLeaks. The DNC used CrowdStrike to fabricate a Russian intelligence connection to undermine Trump.

In my opinion, the Dominion IT technicians that will be assigned to Ventura County will be no match for nation-state cyber attacks that will compromise the 2024 election. The attack hardware and software is already built into the machines.