Debbie Cohen
Ventura County Citizen, District 4

October 29, 2024

Ventura County Board of Supervisors
800 South Victoria Avenue, Hall of Administration
Ventura, California 93009

cc: Clerk of the Board - for Agenda Item #8, Board of Supervisors Meeting, Oct 29, 2024

re: Request for Expanded Audit of Nov 2024 Presidential Election with a minimum random sampling of 25% of ballots cast

Board of Supervisors,

Election integrity is not a partisan issue, and for many years, both Democrats and Republicans have warned about voting machine vulnerabilities.

In a 2016 episode of the progressive TV show, *Democracy Now!,* investigative journalist Henry Wasserman warned voters about electronic voting machines, and claimed he had irrefutable evidence that both John Kerry and Al Gore won their respective elections. He said that electronic votes cannot be verified and believed that the only solution is paper ballots. He claimed that voting machine problems have existed since 1988 and have "flipped elections" and "stripped black and brown people of their vote", and said, "it's a nightmare and it's not democracy".

In March of 2018 at a Senate Hearing on Election Security, Sen Ron Wyden (D), Oregon said:

> *"43% of American voters use voting machines that researchers have found have serious security flaws, including back doors. These companies are accountable to no-one. They won't answer basic questions about their cyber-security practices, and the biggest companies won't answer any questions at all."*

In June of that year, then Senator Kamala Harris (D), California, during another Senate Hearing said:

> *"I actually had a demonstration here at the Capitol where we brought in folks who before our eyes hacked election machines, those that are being used in many states, but are not state of the art, from our perspective."*

In the 2020 Documentary "Kill Chain: The Cyber War on America's Elections", Senator Amy Klobuchar, (D) Minnesota said:

> *"We're very concerned because there's only three companies, you could easily hack into them, it makes it seem like all these states are doing different things, but in fact, three companies are controlling them."*

The three companies she was referring to were:
Dominion Voting Systems, Election Systems & Software (ESS) & Hart Intercivic

So that was back in 2016, 2018 & 2020.

One might argue that in 2024 we've somehow "fixed" all the hackable points.

Not so fast.

Just a few months ago at the Def Con conference in Las Vegas, some of the best hackers in the world gathered once again to try to break into voting machines that are being used in this year's election – all with an eye towards helping officials identify and fix vulnerabilities. They worked on hacking into voting systems at all stages of the process, including network security, trying to get past firewalls and other security measures.

They found a lot of problems. The man who founded the Voting Village hacking event, Harri Hursti said:

"If you don't think a place like this is running 24/7 in China, Russia, you're kidding yourselves" … *"We're only here for two and a half days, and we find stuff…it would be stupid to assume that the adversaries don't have absolute access to everything."*

Voting Village organizers were also frustrated that voting machines vendors and government certifications aren't moving quickly enough to implement fixes.

Harri Hursti added:

"There's so much basic stuff that should be happening and is not happening, so yes I'm worried about things not being fixed, but they haven't been fixed for a long time, and I'm also angry about it."

Today, there are 11 vote centers open across Ventura County with thousands of people casting their votes in person at each one. Each vote center is connected to the county offices via high speed wireless connections, using hardware and encryption technology that is owned and operated by a foreign company.

These wireless connections and the machines at both ends of them, encrypted or not, are absolutely 100% hackable by bad actors – foreign and domestic. We have all heard of hackers accessing "secure" systems with the highest levels of encryption – including banking and healthcare systems and even federal agencies like the Department of Justice and the Department of Defense who were just hacked last year. Not to mention candidate campaigns – like in 2016 when Russians hacked into the Hillary Clinton campaign servers and leaked a bunch of internal emails, and the most recent hack of the Trump campaign by Iran.

How do we address these vulnerabilities? How do you plug all the holes? The truth is, you can't. It's impossible because it's a never ending game of cat & mouse. Do you want to certify an election based on this apparatus with only a 1% audit? As an IT professional of 40 years, I wouldn't *dare* do it.

The ONLY solution available to PROVE that these systems are reporting accurate results is to conduct a significant hand count audit with a minimum 25% random sampling of ballots, then cross-check the audit results with the elections systems results. If they match, then each of you can vote to certify the 2024 election results with a clear conscience. If they don't match, then we'll know there are issues and we must face them, and not sweep them under the rug and pretend they don't exist.

Sincerely,

Debbie Cohen

Debbie Cohen
Ventura County Citizen, District 4