PC-#08_Bill Wiesner Public Comment #08 – to the Leelanau County Board of Commissioners
Tuesday June 21, 2022 Request for discussion and research by the Board:
We Demand Honest Elections in Leelanau County! … by
Replacing Dominion Voting Machines with Paper Ballots that are local, secure, and easily auditable.

Watch the Video: Hacking America's Computerized Voting Machines (from 2016 – 2018 Elections) to see these quotes and know why we need to Demand Honest Elections in our Leelanau County! … by Replacing Dominion Voting Machines with local, secure, and easily auditable Paper Ballots: https://frankspeech.com/video/full-video-hacking-americas-computerized-voting-machines
[The video has just over 11,000 words of **Vital Quotes**; I'm only giving you ~1500 of the words in this Public Comment.]
[Also Note the names of the people – all concerned about Election Security – are listed below the photos, along with the time stamp of the photos.]

I know America's voting machines are vulnerable because

my colleagues and I have hacked them repeatedly. We've created attacks that can spread from machine to machine like a computer virus, and silently change election outcomes. And in every single case, we've found ways for attackers to sabotage machines and to steal votes across the country. … in every single case, where a US voting machine has been analyzed by competent security researchers they have found vulnerabilities that would let someone inject malicious software and change election data. Every single case,

"The better or the more efficient way of hacking machines would be to subvert them all through the machine that's used to actually program those machines. So prior to each election, the county election office or the voting machine vendor will actually program memory cards for that election. … And that gets inserted into the voting machine. If you can alter if you can subvert that machine that is used to program those memory cards, then you can pass rogue software to the voting machines."

Studies conducted in 2007 by the State of California State of Ohio State of Florida found security vulnerabilities that could take advantage of these two engineer viruses where one compromised voting machine could then infect eventually the entire fleet of machines for an entire county.

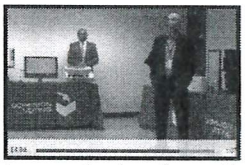
… They hacked within 90 minutes of being in the same space as the voting machines. … they can manipulate the tally, or they can delete the tally. And they could compromise the vote in any number of ways.

There are a number of states that outsource their reporting of elections to third parties, some of which are corporations based in other countries like Spain. … One of the things that hasn't been mentioned so far yet is supply chain hacks. There are components in these voting systems that come from foreign countries.

… But it's ultimately a reflection of the nature of complex software. It's simply beyond the state of the art to build software systems that can reliably withstand targeted attack by a determined adversary in this kind of an environment. The vulnerabilities are real, they're serious … You know, just as we don't expect the local sheriff to single handedly defend against military ground invasions. We shouldn't expect county election IT managers to defend against cyber-attacks by foreign intelligence services. But that's precisely what we've been asking them to do.

… The machine that I hacked is called the Sequoia AVC advantage now called the Dominion … , there are many kinds of voting machines and the same kinds of hacks are applicable to all voting machines and have been demonstrated at several other universities, including the University of Connecticut, Johns Hopkins, Michigan, and others … This is not just one glitch in one manufacturers machine. It's the very nature of computers. So how can we trust our elections when it's so easy to make the computers cheat?

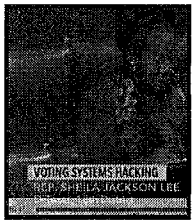
With parts made all over the world and software made all over the world. And as Sherry said there's only three or four manufacturers. The one core point that kind of election security experts and others have been making about why our votes are safe, was that the decentralized nature of our voting systems … We now know that's false, and that through a handful of simple attacks into manufacturers, not in the United States, the Russians could plant malware into 1000s of machines all at once and hack the entire US election without ever leaving the Kremlin.



Eric Coomer (EC): 'Strategy & Security' Vice President for Dominion Voting Systems [Conversation with potential Dominion Machine buyers:] Q#1: "what is the vehicle for the transmission from the ICP is a cellular modem versus VPN?" A#1: (EC): Well, it is a cellular modem that can be configured in a VPN. Right and we are currently in Chicago Cook County we've worked with Verizon to secure that network. Q#2: What wireless chipset slash modem does the hardware have? A#2: (EC): Ah, we support a variety. So it's really up to the jurisdictions what technology they want to use what's compatible with their networks. (EC-Ast): Currently in some jurisdiction, we're using basically a modem that is a 3g modem GSM but we can support multiple varieties of modems. (EC): … including latest 4g standards. Q#3: So the answer is the next question is that 3g or 4g Verizon, AT&T, and Sprint – I'm assuming all? A#3: (EC): Oh, yeah. All networks. Yeah, I mean, we actually transmit from the ICP in Mongolia as well. So we're not limited networks. (EC-Ast): In Puerto Rico there's three vendors because the island is not covered by any by any of

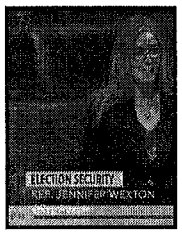
them completely. So we use the three different cellular vendors for some ICPs with these vendors are Clyro, AT&T, and MT Mobile, I think in the different parts of the island.

Hillary Clinton: Virginia just stop using touchscreen computer voting because it's so vulnerable. We need to look at all the voting machines every secretary of state needs to be you know, assisted in making sure that they are not being hacked and attacked. ... And they are still looking for ways to steal information about voter registration. ... because still, too many of them are linked to the internet. So we are still very vulnerable.

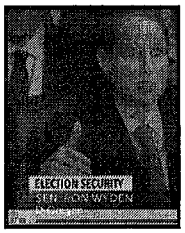


The Resources have repeatedly demonstrated that ballot recording machines and other voting machines are susceptible to tampering. ...

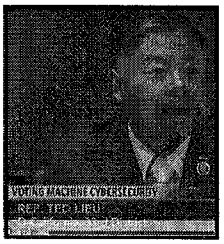
Even hacker live with the prior knowledge, tools and resources are able to breach voting machines in a matter of minutes.



In 2016. State election websites and Illinois Arizona were hacked by intruders who installed malware and downloaded and sent voter information. ... In 2018 electronic voting machines in Georgia in Texas deleted votes for certain candidates or switch votes from one candidate to another.

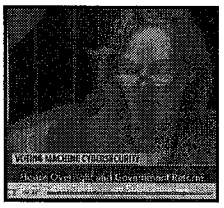


The biggest seller voting machines is doing something that violates cybersecurity 101 -- directing that you install remote access software which would make a machine like that you know a magnet for fraudsters and hackers. ... 43% of American voters use voting machines that researchers have found have serious security flaws, including back doors. ... These companies are accountable to no one. They won't answer basic questions about their cybersecurity practices. And the biggest companies won't answer any questions at all. Five states have no paper trail, and that means there is no way to the numbers the voting machines put out are legitimate. So much for cybersecurity 101. ... According to an exhaustive analysis by Associated Press, Pennsylvania Wisconsin, Michigan, Florida, Iowa, Indiana, Arizona and North Carolina, among others, are all at risk, even the state of Georgia, which just passed legislation to buy new voting machines is on track to buy equipment that suffers from the significant cyber security weakness, say the election decided by a small percentage of people in America don't think that the electrician was fair, the effect that would have on our 200 year experiment in self-governance. Our democratic system would take a real hit. Our elections weren't secure last week, and they sure as heck aren't secure this week.



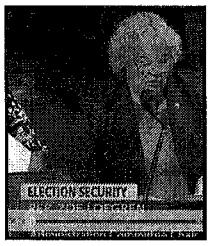
Abcde

abcde

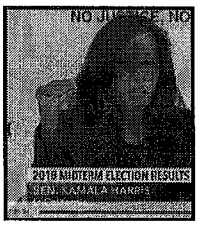


abcde

abcde



abcde



abcde

abcde

Bill Wiesner / Leelanau County Resident and
www.TCFamily.org Founder
(231) 313-6805