TRANSCRIPTION OF RESEARCH ROUNDTABLE #3: MACHINE VULNERABILITIES 9/7/22

ASG: Today we have Colonel Shawn Smith on to share with us specific information about machine vulnerabilities, because I know one thing that we hear often is that people want to be able to speak more confidently about these issues and it is a lot of a lot of information. I think Shawn does a great job of simplifying this super complex subject, but it is a lot to write down so we are recording, so rest assured, you can always go back and catch the recording. Shawn, with that, I'd love to turn it over to you to start the categories of vulnerabilities for the voting machines.

SS: Good morning, everybody. With all that hype I will probably under deliver. But so the intent is just to for this to be a little bit of a primer discussion and then we can start talking, you know in future roundtables about specific vulnerabilities and voting systems, what to look for, what they're vulnerable to. We're just going to talk through some examples in the commercial world. Easy enough to look up these examples.

I've seen examples of all of these in in DoD systems. Usually we're the first to see them because the APT, the advanced persistent threat teams that are developing and they're not just like one thing, you know, the teams that are developing the more exotic and refined and complicated attacks are not doing them so that they can hack your phone, right? They're doing them to go after national security systems. There are some exceptions where they're like a commercial hacker group that's doing it for profit or something like that. So many of those are at least affiliated with or co-opted to government agencies particularly in Russia or China. But most of these are being are being tested and tried out first on national security including financial systems before you ever see them in the wild or on commercial systems. Although occasionally they'll kind of go sideways. We've seen advanced persistent threat teams use as many as 17 or 18 different chained attacks and compromises to try to get to what they want. We're talking about these sort of in isolation, but that's not where the threat exists. It's one small thing that might be a low severity issue and then it's a combination of those where you get them combined and you and then suddenly you have a system that's wide open or exposed or you get something involved and it's not just you know new systems or old systems.

I'll talk about one of these in particular, but these compromises are sometimes being discovered a decade or more after the software is either put into the field or no longer being supported by the actual vendor. So we're going to start with hardware and if anybody's got a question just raise your hand or whatever and Amy can tell me if I need to stop and answer because I'm on my phone so I may not see everybody's questions, but I don't mean this to be a one-way thing. I'll just start with an example for each one of these categories.

We'll start with hardware. So Super Micro is the most public. I will say I've seen hardware compromises within weapon systems where an attacker was able to either compromise the design that was being produced in the United States, or they were able to manufacture a counterfeited or compromised system or component that was being produced overseas. A great example of this is Super Micro. So if you if you search for any of these things you'll be able

to find these examples. Super Micro is an American motherboard manufacturer and like a lot of you know, most of the advanced semiconductors in the world are being made by Taiwanese companies. But most people don't realize that many of those chipsets and components are not being made in Taiwan. A lot of the of the companies in Taiwan are what they call “fabless,” meaning they don't have their own fabrication facility because like in the United States if you try to create a fabrication facility you're dealing with all sorts of red tape in terms of environmental regulations and compliance certification, etc. and it will cost you twice as much to or more to build a fabrication facility for semiconductors or integrated circuits in the United States as it would cost in China.

So what happens is these companies directly produce their own facilities in the People's Republic of China and now they're starting to move more of them to Singapore and South Korea and the Philippines because they realize they're in jeopardy of having their supply chain dependent on China. Or they license another company. Wistron is a great example. Wistron's a Taiwanese company that manufacturers the majority of the Dell and HP laptops that are sold in the United States. They manufacture those in China. I think their headquarters are in Palo Alto or San Jose or down in southern or central California or the Bay Area but they manufacture their motherboards overseas.

This came out publicly, I want to say in 2018 is when this first was being reported, but it turns out that it was at least 2015, maybe as early as 2013, there were indicators that their motherboards had been compromised. The ones manufactured in China had a device about the size of a grain of rice, smaller than the head of a #2 pencil, that was a power coupler, like a power conditioner, just a tiny little device that regulates low voltage on an integrated circuit motherboard. Except that it wasn't that it had embedded within it. Essentially like a transponder, but not radio frequency. So it was taking data off of the motherboard, modulating it onto other outbound traffic so that the motherboards were compromised and were passing traffic off of those motherboards to the specified attacker’s destination.

And the importance of this is Super Micro had sold just tons of these motherboards to major tech companies, like Amazon, Google, Microsoft and Apple. And they were using these in their server stacks, which means that everybody's traffic that was moving through those server stacks was potentially affected, and nobody knows really how much of that was compromised. The federal government started watching at a certain point, warned some of the bigger companies, but didn't warn smaller companies because they were monitoring it, and this is common in the Intel community. They will not. They will discover a vulnerability and then not tell anybody. Because they want to see who's using it or they want to use it themselves. That's a very common, it's called an Intel gain loss assessment. In my experience, the Intel community almost always decides that the Intel they'll gain is more important than whatever vulnerability they can protect against. They have perverse incentives so they protect us less so that they can monitor more because the Intel, their instinct is always to get more information. So that was Super Micro, which infected hundreds of millions of people by going into specific companies. We don't even know all the people who are affected because they weren't all notified that information was collected. That's one example of a hardware compromise.

Next, a software compromise. A great example of a software supply chain attack was Solar Winds Orion, so everybody has heard of SolarWinds. The product was actually Orion, which was a suite of enterprise management tools, including hardware and software. Services that an enterprise network manager for a hospital system or for General Motors or for every major department of the federal government. Every cabinet level agency in the federal government, they were all using Solar Winds Orion. Before that they had used some other like Jupiter Networks. So every time there's a built in inherent cultural vulnerability. The government wants to save money. They're not particularly innovative. So they say here are products you can use. Here's a specified approved list or here's a contract and you can get these under that contract. So imagine for example federal government is going to issue cell phones. Federal government doesn't just say, OK, all you guys go out and buy your cell phones. They negotiate prices with particular carriers and then they have like a GSA number or something like that. And so you end up with this vulnerability because all those government agencies will get the same products, outside adversaries will know they're going to get those products, and they'll have the opportunity to insert something into the supply chain for those products.

It's exactly the same with our voting systems because the vendors are ordering these systems directly from Dell and HP and the Dell and HP people know that they are coming to the voting system vendors and the factories ship them directly. So it's not like they get manufactured in China like in in Wuhan or Jing Xian. It's not like they get manufactured there and then they ship to an unknown location. They're shipping them. It's like drop shipping. They're shipping them directly. So the voting system vendors are ordering specific configurations so they're not off the shelf. They're specified boutique configurations and then they're being manufactured by people who know they are manufacturing them for an American voting system vendor. They know that at the point where they get the order and then they're shipping them directly from those facilities, to the customers like Dominion or to ESS or whatever, sometimes directly to counties, but usually directly to the voting system vendors.

So Solar Winds was a software update that involved an attack against Solar Winds, the company that compromised one of their software updates. So when all their customers downloaded the software update, you know, trying to do the right thing with cyber hygiene, they downloaded the malware from the trusted vendor. Of course they installed that malware, and the malware is extraordinarily sophisticated. There are actually two, at least two series known: Sunspot and Supernova. Sunspot was much less sophisticated than Supernova and you can go and look at. It issued instructions to government agencies if they thought they might be compromised, if they found the indicators of compromise that were identified with the vulnerability. And the very first thing they tell them all to do is image your system. So there's the very thing that Tina Peters in Mesa County, Colorado is being prosecuted and attacked for, and the same complaints against the Coffee County people in Georgia. Image your system and then they basically said take it offline. Just don't allow it to reconnect to any government network.

And then they're trying to get around to them to, you know, pull data off because even they—the cybersecurity community and the government, and the even the commercial side—don't completely understand all the different aspects of the compromise. So typically the very first thing is to get access and then to escalate privileges on a network and then to move laterally. And then you start loading all kinds of other tools you get into. You know, your rootkit, you get into. Drivers you get into, you load stuff into, not storage, but memory on the systems. You change out firmwares. Basically, once you get they get a foothold, they try to never lose that foothold, and so they propagate multiple different vulnerabilities and compromises into the targeted systems. So that was SolarWinds Orion.

ASG: Shawn, we do have a question. Can you speak of cybersecurity vulnerability of ESS 6.0 point 2.0 and 6.1 point 1.0? Win 7 versus Win 10, etc.

SS: That is a very timely question because the next software compromise or vulnerability I want to talk about, these are all supply chain, right? So this is you're an end customer, like you probably got a smartphone on your desk or in your hand right now, or maybe you're using it. Supply chain is everything that produces the goods and services. So the hardware of that phone, the screen, the driver that runs the screen, the driver that runs the USB port in your phone or the Lightning port in your phone, it's a double edged sword. Either you don't get updates and then you're vulnerable to what's discovered or you get updates. And the update itself may have a vulnerability. That's what happened with Solar Winds. It happens a lot and so the next one example I want to talk about is Print Nightmare.

Print Nightmare is a Windows Server spooler service, like for print spooler services. I could get into detail about spooler services, but it's basically it's the way that your computer communicates with the printer, because your printers, the old ones especially, didn't have enough memory for all the documents and so the computer would kind of hold this buffer like a stack of the files that wanted the printer to print, and it would feed those digital files to the printer in a sequence in a volume that the printer could handle. So the printer would, you know, open its bird mouth again when it needed another document when it was ready to keep printing, and the and the Windows thing would feed it. But those are those. Some printers or one of the earliest functions and so a lot of the functions within a principle have really primitive core access to Windows and computer hardware services like they could access memory directly, as opposed to having to go through a bus or go through some other Windows service.

So Print Nightmare is a relatively recent, about a year, year and a half old vulnerability discovered that that affects literally every single version of Windows since Windows probably RT. So Windows 7, Windows 88.1, Windows 10. Windows 11 when every version of Windows Server 13 or Windows 8, Windows Server 8/12/16 and 19. In other words, Print Nightmare as a vulnerability affects every single Windows version being run on any American election system and no update was published to fix it until over a year after it was discovered. What Print Nightmare does is it's the first compromise in what was a privilege escalation. So remember that the voting system standards require—although I haven't seen yet, a single voting system

that actually complies with this even though they're all certified only the 2005 standards—but the voting system standards require voting systems not to allow users who aren't like admins or whatever to manipulate or alter tabulated votes in the tabulated vote database. They shouldn't be able to touch it at all. That election is underway. They should not be able to go in there and change values. But if you can escalate, even if you control that to administrators, if you have a software service and compromise that allows you to escalate privileges within Windows, then someone who is just supposed to be a user could be escalated to an admin user. An admin user on the machine could also be changing software and firmware.

So this is where it gets to combined or hybrid attacks. Let's say on your system like ES&S, you have a memory stick, a memory device. It's probably a thumb drive. It could be a memory card, but it's probably a thumb drive on the newer systems. So that's a thumb drive provided by the manufacturer, right, or by the voting system vendor and they claim that they're secure, they secure them on their own system. Immediately I'm suspicious of that. So you get that thumb drive and you plug it into the tabulator, the DS 200 or the you know 450 or 850 and then you come and plug it into the EMS system. They can have a hidden partition on that thumb drive, and we'll get to that with portable code and remote access and when you plug it into the EMS server or when you plug it into the scanner tabulator another application. That computer can run, can access and run what is in the hidden partition. And so it can run software and this kind of bridges into portable code. It can run software only on the USB.

In other words, it never installs anything on the Windows system and because it never installs anything on the Windows system, it is not creating log file entries as an application the way other applications would. In a Windows system, Windows 10 or 11 or Windows Server, you can go into an event viewer and you can look up under Windows or applications. You can see if the logging is properly set up as it's required to be by the certification standards and has not been in any voting system that we've seen so far. In the log, all activity log, users logging in, logging out a process, start, a process, stop, an error message, a communications port access, something gets sent to a printer, there's a log entry, and so you're supposed to have log file sizes and folder sizes large enough that you can record every single event that occurs on that system. Anything that happens, any memory access processor, you should have all of it for the time that the system is being used for election purposes, which means starting from the time that the election project is defined on the EMS server typically, or on election event designer software on a on a workstation. From that time until you have certified and archived all the records, they should have every single event that occurred in the log files. And that just is the beginning of being able to have an auditable record that you could go through as a forensic examiner to see what happened.

When you have portable code, it's dangerous to have portable code because it does not have an installed application you can have. And if you look up patents for Dominion soft voting systems engineers, you'll find that they have patterns for self assembling applications. In other words, these are applications that are split up into components so that they don't even look like executable files. So you might have a couple different code segments or sub apps that are disguised as a driver file or as a font file and they just look like a font file. You can scan them a

billion times with an antivirus program or malicious software detector and it never recognizes them as a threat, because they're not executable. It literally just it looks like a plain text or whatever.

Then you add this third component that is only on that thumb drive and the hidden partition. When you plug it in, you know an application on the voting system that looks innocuous, reads that hidden encrypted partition, pulls that piece of code that contains the pieces that are actually executable, assembles it with the pieces resident on the voting system, runs the application, which could do anything from changing out which drivers you're using to change and configure settings in the scanners or in the software applications that are tabulating or it could execute changes like they saw in Mesa 3, the forensic report from Mesa County, the third one where they saw that databases had been duplicated. It can do anything if it's an application, and it leaves no trace in almost all the log files and especially the log files that are configured on our voting systems being saved in the election projects. It leaves no trace because it's not installing anything or running an installed application. And I'm still just talking about within Windows. We haven't even got to hardware level where you have the integrated Dell remote access controllers that have access to the Intel active management technology like AV Pro or management engine that are installed on the Intel I-57 and nine processors that are on almost all of our workstations in the voting system.

So anyway, Print Nightmare allows privilege escalation, and has been for a year, so we've run elections on systems that were vulnerable to this and not patched. So was that run on there? We have no idea. We have no idea. And the only way you would know, even have a hope of knowing this by being able to access and review all the artifacts and log files on the voting systems. Nobody's getting access to do that. The government isn't doing it. The public officials don't even know what they're doing for the most part. I've yet to meet a single election official who really understands their systems and you can understand why because the people you would need to do that are people who get paid you know 6 figure salaries that that's the level that our threat is operating at. So it's like we're trying to guard Fort Knox with children but they don't even have the skill set or the experience or the proficiency. Most of them are so far below it they can't even comprehend the threat level that is facing them, let alone do anything about it. But they're being, you know, propagandized by the government and all these institutions that are telling them, oh, we're sharing threat information with you, right? We've got the EIISAC right. The Election Integrity Information Sharing and Analysis Center. We're giving you threat warnings, right? Well, they can't do anything with them. It's like, you know, it's like if you tell somebody there's a tornado approaching them. They can't stop the tornado. All they can do is shelter.

Let's see, firmware. I want to give this example because this is a really serious example and I'm trying to just use examples of things that you could find public sources on and not any of the other ones. Firmware is not user accessible software. It's essentially a small set of code that tells a computer how to interface with a device, an external device. That's firmware. It's like software, but it's very specific to a piece of hardware typically, and it is not user accessible or user executable. It's more like, you know, you turn on the light switch and in between the light

switch and the light bulb is firmware that tells that light bulb how to operate. And that's actually true on the LG Advanced light bulbs that change colors and things like that. Those have a tiny little microprocessor that's controlling them and they have firmware that they're running. So you know, this is everywhere. There's firmware in your refrigerators, your microwaves. A lot of cars have like 10 or more computers on them now, they're running firmware.

Well, that firmware can be hacked so that it does unexpected things, including responding to commanding. That is what we call out of band. Let's say I've got my computer hooked up to another computer and I expect to send messages back and forth--that's in band. That's planned. Known deliberate connectivity. But if somebody can then send a signal over that same communications line that isn't coming from my known or trusted sources, or is triggered sort of in a way that would be opaque to me, that's out of band. It could also be *applied* out of band, can be applied to frequencies and things like that, but broadly out of band means it's sort of outside of the controlled channel.

Stuxnet was an open source. In the public reporting, Stuxnet is possibly Israeli, possibly a US, possibly a collaboration. It was a spoofed driver certificate. It was downloaded onto administrative computers as an update on those administrative computers in Iran that were controlling networks of centrifuges at Natanz and another facility. Stuxnet then enabled the download of other malware, and the insertion of that malware into the hardware devices that were the centrifuges that were then remotely controllable or triggerable. Then what Stuxnet did was it slowed down the centrifuges at first so that the centrifuges were producing enriched uranium at a lower rate than they were capable of. So in other words, the Iranians were sitting there trying to produce weapons grade uranium and instead of it taking an hour to produce a gram or whatever, it was taking like 10 hours to produce a gram with no external indication. So it was affecting the hardware performance. Because the centrifuges are mechanical devices, you know they're subject to mechanical degradation and deterioration. What Stuxnet then did was induce massive accelerations and decelerations like rapid pulsing that was designed to wear out the bearings and microcontrollers so that the centrifuges would fail. So first it slowed down the Iranian uranium production and then it started destroying the centrifuges. So you can imagine lots of people other than the Iranians would want to do that. So that's an example of what you can do with firmware.

Firmware could also be altered for our ballot scanner, so you could alter the firmware so that they no longer loaded settings, configuration settings that would discriminate between ballots without signatures or ballot envelopes without signatures and ballot envelopes with signatures or so that they would automatically substitute an image from a file that some other application was generating for the image that they themselves are creating. So it could look normal on your election management system. It could look normal on the tabulator workstation. It could be telling you that it's doing what it's supposed to be doing. Everything could look fine. But it could be substituting illicit or, you know, fabricated files for the ones that it's telling you are coming from. This is why it's so critical to go back to the paper ballots and to be able to go back to the paper ballots. So anyway, that's firmware.

Portable code, we already covered a little bit. It's easiest to do it covertly when you have a hidden encrypted partition, which I don't want to say exactly where, but we have confirmed. We've confirmed that hidden, encrypted partitions have been used on the portable removable media thumb drives used on US voting systems in US elections. Whatever you think is on the thumb drive is only part of what's on the thumb drive. You could be thinking that you're just moving, you know, election records back and forth. The machine could be telling you that the thumb drive is formatted and cleaned, but what you're actually doing is moving triggers and data back and forth. They're altering what's affected on the tabulators, or altering it when it's on. Because a lot of those things. If you've got a thumb drive that has security features in it, it's not just a storage device, it's not just a USB device, it's a computer in its own right. So that's portable code you can also have.

I talked about self assembling. Self assembling is triggered by something. It has to be triggered by something. Could be time, could be the users that are logged in, could be other applications that are running, could be combinations of those binary or tertiary triggers, could be a remote trigger. And this gets us into remote access. Remote access is, I would say, the most dangerous of all possible vulnerabilities and compromises because remote access means that either an application or a server or an individual or a team has the ability to change anything, anything on the computer that it to which it's given remote access. Once you have that access you can then run through different exploits until you find one that's unpatched. Or maybe one that other people don't even know about. Like I said, the Intel community keeps these secret. Well, suddenly so do other organizations. Furthermore, when you start talking about supply chain, if I had the ability to be the manufacturer for our potential adversaries, weapon systems, or critical systems, I would sure as hell be building backdoors and compromises into them that I could exploit when I needed to. Of course that is being done to us. I've seen it over and over again in defense systems and we're pretty confident that we're going to find those when we get access to the hardware in one of our voting systems or multiple.

And it doesn't have to be in all of them. You could have just one system in a suite or a county that's compromised. Although like we saw in Mesa where you have 36 separate wireless devices in a single county’s voting system. I mean that's, you know, they really went overboard. They're making sure they had access that they were not supposed to have, right. There was precisely zero authorized purposes for remote wireless capabilities into the voting system in fact because they weren't allowed to be used. And this is part of our problem, you know, the Election Assistance Commission's accredited VSTL probe BMV they didn't even look at the wireless devices in the voting system. For like 5.11, Dominion Voting System, 5.11 Democracy Suite, 5.11, or 5.13, they didn't even look at those telecommunications devices to see if they were secure or accessible. You know, in the US government facility, a secure facility, if you're bringing in a hardware and it has a wireless device, you disable that. Not through settings. You disable it with a drill or wire cutters. I'm not kidding. You literally strip that hardware off of it or cut the connections going to it. So that cannot be used because we've seen the administrative controls bypass and compromise. So let me stop there because that kind of covers the remote access.

A good example by the way of remote access is from 2000 to 2006, ES&S had and they admitted this in like 2013, I think in response to a congressional inquiry, ES&S had installed remote access software called PC Anywhere on their election management system servers. Never told a single customer. Now that's not a company I would ever trust again, but then they installed uncertified devices in 2007. They were sued in California over it in 2000. Then probably in '15 or '16, they started shipping DS200s with the Telnet LE910 4G cellular wireless chip on the motherboard and they told customers those were tested and certified they weren't. So this tells you how good the whole regime and how good election issues are. You could easily, easily have looked up that hardware and looked at the voting system testing report and seen there was no test report from a voting system testing lab that that showed certification testing, let alone certification for that configuration of the DS200.

And yet not a single one of the customers did that. Not one. And the AC didn't discover it, Pro V&V didn't note it, and ES&S was sticking EAC certified stickers on the side of those DS200s. So then when they were called out on it 2020, a nonprofit notified EAC and notified the media. Because the media had been notified, EAC then sent a letter to ES&S and said, hey, you know, you guys are marketing these. They've never been tested or certified. You have to correct the record. ES&S responded, basically said, well, we didn't mean to do that and we've advised our customers to take the stickers off. So which, you know, betrays the idea that they didn't mean to do it. So anyway, let me pause there for a second because I think we've covered the those are the broad categories of vulnerability. Let me just see what questions we've got.

ASG: Shawn, we had a question a little while ago from Burl in South Carolina. Is Jackson or LG4J a concern?

SS: Daxin is for sure. The important thing to know or one important thing to know, if not one of the important things to know is that our voting systems are phenomenally complex, right? They're modern reconfigurable, multiprocessing, multitasking, you know, if you have a modern server. You might have 16 different cores running in the chipset. On the processor alone, and those processors like a Xeon processor and the Intel I-57 and nine, they all have active management technology built in. Which means they have a whole separate computer built like under the hood that is designed for network administrators to be able to do remote management of those machines so they can do maintenance on them, configuration upgrade, software changes, user access, etc. They can do anything. They can do it while the machine looks like it's off. That's what they're built for. So when you combine an election management system server IDRAC, the integrated Dell remote Access controller, which has only one purpose, and its remote access for a network administrator to manage that system and anything connected to it, and then you have these other chip sets that are built in. You built a system that is designed to be controlled and manipulated by somebody other than the people sitting in front of it. Now all you need is a channel. Whether it's a wireless device or anything else.

If you haven't looked at CVE* details, I would look at CVE details which is like a like a private

** CVE = Common Vulnerabilities and Exposures NVD = National Vulnerability Database*

nonprofit sort of explanation of what is on CVE. Now they're calling NVD. Nobody uses NVD, they're using NVD from my perspective to try to be relevant in something that miter has already dominated and other partners have already mastered, but you can look up known common vulnerabilities and exploits in the CVE databases if you just search for CVE. I prefer that site, but you can look at it at NVD NIST site if you want. They'll show you all the known published vulnerabilities for hardware and software.

You know you'll find thousands for Windows 10. You'll find thousands for lots of Windows products. Umm. Sorry, did I answer the question?

ASG: Well, I think you said Daxin is a threat, so yes you answered that. Doug posed a question in the chat, but before that, Laura had her hand up. So go ahead, Laura.

Laura: Yeah, thanks. I'm going to preface this by saying I'm not an IT professional. I just stayed at a Holiday Inn last night. Right. So I'm, I'm probably asking stupid questions. OK. But what I get back from the election officials there are two comments and I just can't answer. And also legislators, by the way. And one, is that, OK, we have the physical poll tapes at the end of the day, and those then match to whatever the machines tabulated. But we all know that they're also messed with sometimes afterwards, like after the polls are closed. So how is it that the poll tapes correlate? That's my first question. And then the second one is in South Carolina, we have new legislation where we have 3 precincts, I believe in each county that are hand counted and they're claiming that they physically look at certain races to inspect and determine who actually, you know, on that physical ballot, they're counting them, they're claiming. I'm not sure if that's true. I've never viewed it. And that, gee, we checked it and that correlated with what was on our tabulator. So how is it they're doing that? Because we know they're cheating. So how is it that? Those two things are matching up.

SS: So, a couple things in principle. First, anything that isn't done in front of you or under video that you can review, I don't trust it. I don't trust it because they don't know what they're doing. At best they don't know what they're doing. Worst they’re you know, not really checking anything that is sampled is not sufficient. So for example, risk limiting audits are not sufficient. You go back and check a few of them depending on how you select them. So if there was a 50% rate of fraud in the election and you checked the other 50%, you wouldn't see the fraud, depending on how that has been distributed, and obviously you don't need 50% fraud in most races. Most races are less than 10% of the margin, and they claim it's random, they claim it's random and they claim it's not risk limiting anymore. They're fully hand counting. But I, I don't know. I just don't buy it. I don't know. I mean the video, that's all I've got to say about that, you know, under video.

So we can talk at a later about different hand count techniques and that the hand count, the precinct hand count guide will go into a little detail about that. But there's no comparison for a hand count. Hand count should be done by read and mark. Or by sort and stack and then read and mark, but not by reading by, not by sort and stack alone. Sort and stack alone has the

highest error rate if it's not done under video, where you can see for yourself what was counted, how it was counted. I wouldn't trust it. You know, there are lots of ways to compromise that sampling of any kind. So if it's truly random and it's a large enough sample size, it might be sufficient. None are so.

When you use like risk limiting audit software like RLA that was developed by Democracy Works, which of course is a nonpartisan but left-wing organization that's funded by Pew Research and by Bridge Alliance, Democracy Alliance, basically, funding and lawfare groups. When you use risk limiting audit software, you're using something that is completely opaque, right? So you could have looked up on GitHub and seen their original development, but you don't know what they're running now. And then they purport to use a random seed, which is supposed to help guarantee that it's a randomly selected set of ballots that they're checking. But in Colorado, for example, that random seed isn't even done correctly. And then who knows what it does with that seed? It's software, right? So you could put in 20 digits, and then it just ignores that and picks whatever it needs to pick. I could get into detail about this too, but I think there are lots of ways to bypass the random selection functions within risk limiting audits and within limited sampling audits.

Now poll tapes. So it's produced by the machine first of all. If the machine is compromised, it can produce anything, right? You had Imagecast precinct scanners in Williamson County, Tennessee and down in Georgia, that were giving no error message whatsoever that were accepting and processing ballots, but then not counting the votes from them. So if you looked at a poll tape from that machine, if they were producing poll tapes, those would match the numbers that showed up at the end. They wouldn't match the number of ballots that came in. And in Williamson County, they only figured out that the Imagecast precinct scanners were not properly tabulating because one of the judges—a single person. One person happened to be keeping a count in her head like a card counter of how many ballots have been processed.

When you have a system that's so fragile or broken that that's how you have to detect errors, then no, there's no safeguard at all. It's just a joke. Then you have to ask yourself, why are we even using poll tapes anymore? Is that how primitive our capabilities are, that we can't, you know, have something that is produced that is more amenable to review and reconciliation than a thermal printer tape this wide? And so, those are stunningly hard to reconcile and everybody knows it. The fact that they're still using it would be like if you went to the customs house and you were buying stuff and we're using a scale and they wouldn't let you see whatever was in the middle of the scale. They only let you see the two ends and they told you, yeah, that gigantic rock is 2 ounces. You can see everything in between. It's not ethical or moral or permissible to use it. And that's where we're at now.

So should we have people actually there when we're poll observing, like taking account of the people that come in? Apparently, yeah, that's a good idea, they call it. Election officials will call that balancing by the number of ballots that that they had supposedly accepted with the number that the machine say they think that's a big deal. Balancing it should be the basics, right? If you think you processed 100 ballots and the machine says 80, that's it. You should hand

count, not run it through another machine. I don't even care what happened at that point, right? I mean, I only need one to know. It's like, how many times does the bungee cord have to fail before you stop jumping with it.

Laura: Well, thank you so much and I appreciate everything you do. You're awesome.

ASG: OK we have Doug next and then George. Doug says, would having PC Anywhere allow for disabling the production of the CVR statewide?

SS: That's a good question. So it was on the EMS servers. If they actually had access like at that time, so when they were using PC Anywhere, they didn't have Internet yet. I think it was dial-up only, but they were probably connected and they probably claimed that that connection was so that the scanner Tabulators could provide early unofficial results, which you know, I could not care less about unofficial results. Anytime anybody says unofficial results, so you're telling me you compromised the integrity of the voting system so that you could get an early result to give to the media. You're fired, right? Any public official that would tolerate that has to be fired. They're too stupid to be safeguarding our elections, or too corrupt, and I don't even care which that that should not be tolerable.

So, PC anywhere. No, no. We don't know if that's being used. Now keep in mind all these safeguards in terms of Voting System Testing Lab and public officials. They have failed over and over and over again. They're not a safeguard, they're a placebo that we're told is a safeguard but clearly is not working now. All we don't know is what is the full extent of the compromises, noncompliance and fraud. We don't know that and we won't know until we get full, independent forensic audits on the machines, which, if we took every single IT pro like a cybersec pro, in the United States that was capable of doing that kind of a forensic audit on systems as complex as the voting machines and the voting suites are, if we took everyone in the United States right now and had them stop whatever else they were doing, I don't think we could do all 3000 counties in the United States over the course of, say, six months. There's zero chance. Zero chance of that happening for any election. It cannot be done. We don't have the cybersecurity professionals in the country. Even China doesn't have enough people to do it.

Because when you can scale the threat but you can't scale the mitigation or examination, it's a lot harder to find the issues than install them. And that's why the prevention is so critical and the prevention is just non-existent. It's a joke, right? So back to the PC anywhere. At that time from 2000 and 2006, when ESS admitted that they were using them on the MS servers, they were using them on the MS servers. You know, in some entire states, I don't know how long it's going on, but like Nebraska I think only uses ES&S, and some states, like Colorado, almost exclusively used Dominion, others use combinations, so it would be harder to do statewide. But remember, you don't need statewide, right? Unless you have to affect the local election, you only need the biggest counties, right? That's where you have plenty of additional voter margin and if you have either inaccurate that are not, you know, fraud, or you have fraud if there are either errors or inaccuracies, that's enough in the larger counties in most places to change the statewide and the national inputs from that state.

ASG: All right. Next up we have George. Go ahead, George.

George: Shawn, great segue. I'm concerned about the accuracy of the machines. I have actually requested all the ballots for the four precincts in my county, along with the ballot images, the cast, vote records and all the print tapes. Why is nobody going after the accuracy? If you've got a ballot and it comes up different and you've got the accuracy requirement is 1 in every 125,000? Now they've found those, but no one is pursuing that. Is there anybody out there that you can recommend me to that is pursuing a kind of checking to verify the accuracy of these machines like with the legal case?

SS: You mean legal, or just trying to isolate the accuracy?

George: One of the things that I'm finding there's nobody out there looking at that. But if it's got a ballot, and a ballot is either changed or misread, it's an inaccuracy. Now if it's changed, the company needs to support wise change if we can show proof that the valid numbers do not match the output numbers. And I did. That's the route I'm going down. I'm hoping to have next week, the four precincts and all the information, and then we're going to be able to go through and just determine whether the roughly 8000 ballots were given the right information to the EMS.

SS: I would say there are people pursuing it, although in every state the paths are different, like in Georgia you might go to the state election board or County Election Board in Texas, you might go to an election judge or try to go to the Secretary of State and then there's court filings to try to do it. But we've had very little success in court so far. The courts don't really want to for the most part touch anything election and voting related, but we're going to have to keep hammering at them because they're supposed to be our recourse to the law and the public officials aren't listening. But I'll use DeKalb as an example. In DeKalb County, Georgia, you had Michelle Long Spears. What was the error rate in that you know where the ballots were improperly tabulated? Or were improperly counted 3000 was the difference in votes. That by itself is a high enough error rate for that voting system that it should have halted its use in all of Georgia until they got to the bottom of it, as well as resulted in notification, an investigation by the EAC and investigation by the state election board, notification to every other customer of a potentially affected device.

And yet none of that is happening. And that's how you know the system that we're operating under is completely broken. It's focused on assuring us of something that is not true. So this is part of the challenge is conveying these ideas to the public so that we get kind of a visceral understanding and emotional level understanding for the public that we are not served and our voting rights are not protected by this system. We're told they're protected and anybody who says, hey, they might not be protected is immediately labeled as an extremist or a conspiracy theorist or whatever, but the BS artists are the people telling citizens that their voting rights are actually assured under this system. They are absolutely not, and they cannot be. And that's the important point, right? Although, like Jack Ryan Cobb, the lab director at Pro V&V who has no

particular cyber security background experience, is not going to be detecting cyber security vulnerabilities in voting systems. And he's the only guy who tests them, right?

This is Clay Parikh's point. Clay Parikh testified in Arizona and again in Alabama, and he was at the Moment of Truth Summit. He was the one who did the security testing on the voting systems for 9 years for NTS, Wiley and ProV&V, and he says the standards are weak. They barely test sufficiently to them, the systems don't meet the standards and they don't ever mitigate the vulnerabilities that the security testers discover. And yet every single public official you talk to is going to tell you, oh, these are federally tested. Well, it's nonsense.

So back to your point of pursuing the issues within accuracy. Absolutely, absolutely, that standard is not met. If your state has a statutory requirement that your voting systems meet that federal voting system standard and you can show that example, you should be able to take that into court. Now, we're still trying to get legal resources organized so that we can get people counsel and advice. And we're just like right on the precipice of being able to put up the legal library. With all the known cases and exhibits and then the non public ones will be within the partnership, protected areas, privileged areas. But we're trying to get legal help to people, it's just we're trying to do it along with everything else. So I would say keep looking for those paths, whether it's local officials, whether it's convincing, spreading awareness in the public, there's going to be some more you're going to hear about this week. Every week citizens are finding new ways to try and press these issues and we have to.

George: OK, one last question. We're running into issues with the state of Illinois that the QR code on the Dominion system is vulnerable in our state. It requires that a recount that they hand do it, but they're not doing it. Can you give us some background information on that QR code being read by the tabulator?

SS: Yeah, so in theory the QR code, and it depends on the vendor and the specific jurisdiction, but in theory, the QR code for a ballot produced by like Image Cast X or Image Cast Evolution, where a voter can use a touchscreen device and it's a ballot marking device and then prints out a ballot. In theory that QR code is machine readable information about the vote selections and the ballot style and the precinct etc., that can be read by the scanner Tabulators. So you take that out of the ICE or the ICX and then you feed it into the ICP or the ICC, the precinct or central scanner. But you have to ask yourself: if it can read a normal human marked mail out ballot, then why in the hell did they have a computer code on it? I don't see a valid reason for doing that. Furthermore, there's something called steganography. Steganography is when you embed a digital code or digital file in an image. There are different ways to do it.

One of the ways to do this is an example of a letter. *(Shawn holds up a physical letter.)* This is from my local District Attorney telling me he's not going to do his statutory duty. I'm going to fix that here shortly, but this letter could have a digital code in it. So imagine that you could overlay over this page a grid of 8 inch squares so when your ballot scanner scans it, it then digitally overlays a grid and then if it finds a little yellow fleck in this square and in this square and in this square and in this square, then that's a one-bit change, and that one bit is a trigger

that then tells the machine to do something differently. So now imagine this is a ballot and you have almost undetectable yellow ink printed in the right pattern on there. It's not even visible to the human eye, right? All of our home printers do this right now, if you have a color printer, it's putting a pattern on there that is the serial number of your printer, so that if you go on trying to reproduce or counterfeit currency, that currency is going to have a pattern. That printed paper is going to have a pattern on it that gives you away and indicates your printer serial number. We have the same kind of thing. We have hidden markings on actual US currency and European currency. So you could put a pattern onto a ballot that is one of the first ballots that you run through or is the ballot that you run through. Most jurisdictions have a requirement that they verify like the 1st 100 ballots or something like that against the machine counts. That or they'll have some number that they're checking. Well, you could have a ballot that you feed in as ballot #101 that has a digital trigger on it that because there is a QR code reading application or service running on the scanner tabulator it will read that code. And then it will change the way the machine behaves. So it doesn't matter what you put in is a configuration, doesn't matter what you verified in logic and accuracy testing. That trigger is just the same as if a user, a super user or admin went on to the machine and clicked the right sequence of things or ran an application. So QR code is extraordinarily dangerous, but what's dangerous isn't the code on the paper. What's dangerous is having anything running on a voting system that can read or interpret QR code because it can be completely hidden on anything fed into that machine. Say you have a QR code embedded in another QR code. A QR code could have a secondary code, and that's what I mean by steganography embedded within it that your normal software doesn't read that you wouldn't see was there. That would look like noise.

George: Thank you. That scares me a lot. Thank you for your help.

SS: It should.

ASG: Yeah, I think we heard the collective sound of jaws dropping on that last one. So Shawn, I have a question actually about this rank choice voting that these states are trying to push out. Is this requiring all new software and all new machines or…?

SS: The software they already have already has the capability. It's already there. They just like flip a switch essentially in programming to be able to do it. Yeah, and here's the thing. And so, so back to the issue of remote access and back to the issue of secondary and out of band commanding. Back to the issue of network management and separate chipsets and unlogged and portable code. Any software that is resident on a voting system can be run on that voting system without the authorized users knowing it is running.

The problem with rank choice voting is having the software that runs rank choice voting, which you can distill lots of different ways. Here's how I distill it: one does not equal one. That's all I need to know. So when you have a corporate board meeting, you know, for, I don't know, Microsoft, let's say everybody on here had shares of Microsoft and I had one share and Amy had 10,000 shares. We don't each get one vote. We get one vote per share. So the software

and tools used for corporate shareholder meetings reflect that and allow for someone to have more than one vote or only one vote.

Once you can say a vote counts for something other than one, you can say a vote counts for anything. A vote is, you know, one vote equals 10,000. So you could have, like every vote for Trump is actually 10,000 votes for Trump, and every vote for Biden is actually 1/10 of a vote for Biden. And you could do that for just a certain window –you could have the trigger be a threshold. Right? So until votes for Trump equal 51% and votes for Biden equal 49%, all votes for Trump equal 10,000. Now, if you go back and count all the ballots, that count is not going to match your final count. OK, unless you go back to manipulate the paper, but if you look at the cast vote record, it's going to match your final results.

This is why there's no point in looking at a cast vote record without having all the other artifacts. It might show you a pattern, but it could also just be a completely fabricated sort of verification of what is not true, if that makes sense. So the danger of rank choice voting is the application that allows you to count one for something other than one. RCV (Rank Choice Voting) modules have been resident on our election management system servers for at least five years. So Dominion, they're all in servers. They're just not authorized for official use in all locations.

ASG: Wow, because that's something that I feel like never really got addressed after November 2020 was the totals had fractions/decimal points and we weren't doing ranked choice voting then. And a lot of people questioned it and then nothing kind of ever happened with it.

SS: It's hard to see in reporting sometimes because what they do is they'll report in percentages and then try to convert back to vote numbers. Yeah, just use raw numbers, right? We don't need to know the percentages. Show us the actual numbers. If you find that you have a decimal place for votes and it's not authorized rank choice voting or weighted voting, you should have a federal investigation to voting rights. I mean, it should be immediate suspension of those machines being used there or anywhere and investigation and a full hand count of all paper. Of course, none of this happens because it's, you know, the most secure election in the history of time and stuff. So gold standard.

ASG: OK, so thank you. Amber says we (Oklahoma) has a time traveling voter I found that showed up given voter credit for a future election on voter registration, which shows the last 10 elections a voter has been given voter credit. How could this have been done?

SS: So your centralized statewide voter registration systems which are required either deliberately as an act against U.S. citizens or as an inadvertent well-intentioned but poorly conceived mandate. So all states require centralized statewide voter registration systems. They technically, I think they can actually keep a whole separate voter registration system for statewide non federal elections, but the states have all gone to either top down or hybrid systems. So every vulnerability that's true of a voting system is true of the centralized statewide voter registration systems and worse because most of them are you know 8 to 12 years old.

I think a good example of a newer one is Avid in Arizona, but they use the same people who are, who were involved in all the other voting registration systems like they used to be in that company or something like that that was part of what was bought up by Runbeck out of a California company. There were these sort of, you know, it's just like the voting system vendors, they kind of they, they collapse into and expand out again and then share software and hardware. And you think you're looking at different companies, but you're really looking at the same company or the same hardware or software engineering or the core and the same thing with the same people, right.

Like I've said before, you get a guy like Talbot "Tab" Ireland who went from like Deebold to premier, to ESS, to Clear Ballot. Well, what are the changes? Change it to Clear Ballot and suddenly it's a new voting system. Technology? No. It's the same core set of services, kernels, you know, and modular approach, same sort of structure they used everywhere else. Umm. Sorry, I lost the plot.

ASG: She asked how did that happen? Did you address that? SS: The statewide system, it's just a computer system. They're not secure. There's no certification standard for public officials and so—the short answer is the machines are garbage.

SS: Yeah, right. So like you can do anything.

ASG: OK, cool. Erica says, "Can I share this video with my research team? Where will I be able to find the recording? We have some Shawn Smith fans, plus I think some of them would better know what to do with this information." So Erica, I'm working with the website developer to figure out how to set us up like an area where these types of files are only available to the researchers. So once we have that set up, which should hopefully be in the next day or two, I'll send an e-mail out to you and everyone on this call as well as including the date for the follow up call to this and we'll have the instructions on how to access that. OK and then Sharon says one of our county commissioners knows there were 16 votes which came in between the end of early voting and the actual day of our recent election. How could this have occurred? All absentee voting is not counted until Election Day.

SS: So they might be able to look in your voter registration system depending on how your master voting history works. In your state and Colorado, there's a specific file that --it's public record, right? It's public information. It didn't get produced without public funds. Every person touching it is public, paid by the public. And yet you can't get access to the data without paying additional. So we do that anyway. We pay for it, and then we share it with everybody, because it makes me laugh. Because anybody would give it to you. Is this something that the state is being deprived of funds for, right? I think everybody's entitled to it anyway. So I share with some of the Democrat election integrity activists in Colorado, too.

But anyway, so there's a master voting history file. And so at the moment where that ballot has been accepted, in other words, either an individual or a machine has verified that the affidavit,

if that's required in that state on the outside of the ballot on envelope or the security envelope. Inside the security envelope, as soon as they verified that that's an eligible elector and accepted that ballot for counting, then it updates the voter registration system that person has voted. And so you might be able to look at something like that and see for particular county or precinct, you know, this is how many ballots were received in that. Because it'll have a day when they were accepted.

That's not how I would do anything. I would do everything on Election Day. I would have all your ballots validated on the same day. If you're going to accept like mail in from UOCAVA or something like that, from overseas citizens or however you're going to handle people who are disabled and can't come in. I would do that probably with judge teams, you know, sworn teams that went to their home because you don't have that many. Maybe it's 1000 or a couple thousand per state. Most of the disabilities are not actually verified disabilities like if you can go to a grocery store, you can go to the damn polling location and cast your vote, but anyway, so that's how I would do it.

How they actually do it is they're logging that information when they come in. And they might also use a secondary service like BallotTrax or one of those companies that is getting the US Postal services, IBM TR data that shows when those ballots have gotten back to a county or gone through a polling location or something like that. And so they might be seeing that and that's how they know how many votes were cast on what days. Should we cover severity or are there more questions?

ASG: We only have about 15 minutes. If we cover that next section, it may prompt many more question. So I would say if you guys have questions, let's get those in. Erica says we have received the logs from some counties in Washington. There are entries on there which were not on the 2020 logs. It appears this is the Cron job running on the 17th minute of the hour. Could this just be a change in their logging?

SS: Yeah, but I'd think back and look in those precincts or counties and see if they had changes in the voting system versions, including any approved engineering change orders, and then ask if not. Then if so, then did those approved changes include configuration changes? Because remember, a certified voting system configuration is not just hardware software versions, it's configuration and it's the technical data package. You're not supposed to change anything in them. It should have like machine and device configuration files. Those should not be changed. Shouldn't have a driver that's changed.

Really, if we were serious and our people were competent, you would never load an antivirus or malware definition file update without having it thoroughly tested. Because as we've already seen with Stuxnet and with Super Micro and with Solar Winds, anything could be in it. And it's not like there's an election official in the country. Other than maybe Heider Garcia in Tarrant County, Texas, that has any comprehension whatsoever of what those potential vulnerabilities or attack factors are. You should be looking to see if there are engineering change orders or version changes that incorporate that change to logging.

And then what does it mean? What is the Cron job? You know Cron job is something that runs on a specific time schedule. So it could be every 15 minutes or every hour, or it could be at specific times like 2:15. If you set an alarm on your phone, that's technically a Cron job. If it happens every day, now it's a recurring Cron job. So why is it different? I mean, that's a fair question and you should be able to find and they should be able to give you an explanation for that. If not, who knows what app is running or what services are in? This is part of the problem is these are such complex systems, without having access to be able to watch them in real time which would be better and also not complete and then without having access to all the log files and artifacts and actual capable skill professional cyber pros to look at them and audit them. Here we have no way of knowing what's happening on those machines. No way whatsoever. This is why they're so complex. What they require for verification is more than we have as resources. But one way that you can be relatively confident, at least that you're counting correctly, is to go back and look at the paper ballots. So if you don't go back and look at the paper ballots, you really don't know what the election results are. And if you have to look at the paper ballots to know what the election results are, you might as well just do the paper ballots. Why are we spending billions of dollars on our voting systems if we can't trust them and we can't, we can't trust them so?

ASG: All right. So Alan asked what is the most common vulnerability for DRE machines?

SS: So a DRE is a direct recording electronic machine. It's like a touch screen or ballot marking device except that it is not printing out the ballot. It's producing as electronic file which will then be transferred either over a connection or through some kind of removable media device to the central tabulator or election management system server. So it depends on the basis of the DRE. The older DRE's were not, you know, they were running like specialized limited operating systems and things like that. They could be compromised, but they were simpler hacks. The modern DRE—a good example would be the Galaxy Note Pro and Tab, or eVision SSID and HID 15 and 21 inch devices used for ImageCast X.

On Dominion systems, so those are a computer and they run an operating system, typically Android, although it could be in some older cases Windows CE or a Linux distribution. So anything that affects any of it. So when you look up in CVE details or CBE or MD when you look up vulnerability details, just look up Android operating system for the version that's being run on your system. Then remember on top of that there are hundreds of other applications and drivers and files installed on there, almost none of which are actually being inspected or verified or tested by Voting System Testing Labs. So the most common vulnerabilities are probably going to be operating system related. And I've done this for a couple systems where I've looked up, like if you look at the declaration that I filed or that the attorney teams filed my sworn declaration Arizona and in Alabama, I list out some of the known published vulnerabilities for software that's running on our voting systems, including the operating systems. And so you can see some of that. So I would say the short version is probably operating system vulnerabilities because the wider the distribution, the more likely it is going to

be to be exposed and compromised by hackers, if it wasn't exposed and compromised when it was originally made. Sorry, I don't have any short answers. I apologize.

ASG: Thanks. Alan, did you have another part of your question or is that it?

Alan: No, our biggest frustration is with Microvote and it's like a secret. So we just got a county commissioner elected and hopefully she can get access through directly from the vendor.

SS: In Tennessee right?

Alan: Yes.

SS: We're going to, we need to do a better job of communicating some of these principles so that everybody understands them and can repeat them until everybody gets them. Our current system of voting systems is absurd. The whole idea that you would have proprietary anything, that you would have anything hidden from the public. Obviously it's not permissible to have a single thing hidden other than an individual specific vote choices. Nothing else in that entire process can be hidden from citizens or they have no control. They have no control over the system, so having any part of software be proprietary or hidden, having citizens restricted from being able to see every part of what's on a voting machine, what was running, what applications were executed, how the count was done, anything that is obscured is untrustworthy. There's no way that should be allowed in our voting systems. And yet that's our current system.

Alan: Oh yeah, Microvote is the worst case. Even the manuals are proprietary.

SS: Yeah, so micro vote is, I think that's an old enough device. Now you're talking about Clint Curtisville, right? Those were proprietary hardware. Now when it's proprietary hardware mostly they didn't build the whole thing. They might have put an outer enclosure, but it's kind of like the DS200, the outside of it is you know, proprietary. Oh, we're the only ones with DS200s. But you start looking at the insides and that motherboard, that jetway, I think motherboard that's on there, the NF9D's that those are access that you can buy them directly from the vendor. Figure out how to hack them. Or if you're in that factory because you're the People's Liberation Army, you can install anything you want on that motherboard. What would a voting system person know? What would a public official know? They wouldn't know what's on there, supposed to be on there. They don't even know what the thing’s called or what's inside the case.

So yeah, proprietary. Anything that's completely invisible should be intolerable for our elections. Obviously it should be. I mean, imagine buying baby formula. What's in it? It's a secret. Well. I have some vulgarity for that, I have some profane words for that. And yeah, open source is highly vulnerable. So open source is only a protection. The only protection of open source—true open source is that you can see everything in it. But if it's so complex that you can't, or they then take open source and then modify it, which happens a lot so that then

becomes opaque again, there's no protection from open source, right? I mean, how many people on this call are actually coders? I've coded. I wouldn't call myself a coder, not anymore. It's been a long time and I was never, you know, I've got friends who are hyper, hyper capable. I've never been at their level. I don't even understand what they're doing. Sometimes these are people who code without having to use remarks or notes because they remember stuff that they wrote 14 years ago, like character for character. They'll be able to tell you if there's a missing exclamation point in a 200,000 line sequence of codes. I'm not that guy.

ASG: OK. So we have just a couple minutes left. Any final questions for Shawn? I think Part 2 of this will go a bit faster in terms of: characterizing vulnerabilities in terms of severity, what has been confirmed and verified about our voting systems, which Shawn's already touched on, we can kind of go into that more, and what a person would actually have to do in order to identify vulnerabilities. And then Shawn, I'd love to add "How to communicate what we've learned," because that's taking all this knowledge and putting it into practice. So I think that will be super useful as well.

SS: All right. Yeah. So just, I'm not a cyber professional, OK? I'm not. I've been, I've been exposed to the threat. I've seen what our adversaries are doing to our national security systems, like in detail, I've been responsible to direct testing to evaluate vulnerability and compromise and I've been, you know, down in the technical details for that, down to what does a particular application do, when can it run? Who has access to it? I've seen all of that. And so for me, when I look at our election systems at this, this landscape, this ecosystem of certification and testing and reporting and all of that, it's ludicrous to me. It's ridiculous that anybody would assert that this is secure or has integrity. And that's why for me, I know 100% when I'm talking to an election official and they think it's OK, they're either lying or they've been lied to. Which is true--and they believe it, which is possible, or they are corrupt. There is no choice for me as somebody with a background in what I have. And now when you get somebody who's a real cyber pro, like the guys who are doing the forensic reports, you know, somebody like Doug Gould or Jeff O'Donnell or Doc Daugherty, with all this experience, they haven't necessarily—some of them have, but not all of them—have seen kind of the threats, the advanced threats and the results that I have. So they don't always necessarily see the exact capabilities arrayed against them, but they know in general and they know this is ludicrous. And so we just need to get that point across to all of our public officials and to the public. This isn't secure and can never be made secure.

You cannot secure these systems, especially built overseas, that they were built in the United States and they were reduced instruction set and they were verified by people that we could trust and then available for verification. We'd have a slight chance and still be, you know, in what I really disagree with, we'd still be reliant on professionals. Right now we're relying on professionals that are outside of the industry of voting. We're relying on them to say, look, I am the guy and I did look at this and this database. This is Jeff O'Donnell already. The database is manipulated. It was copied. Not all the ballots were copied. The chain of evidence is broken. You cannot trust that vote result. And yet that's being derided by, you know, guys like this DA Rubenstein in Mesa comes out there with his clown show and says we verified that the report's

incorrect. You're looking at video. This is the environment we're in. We have to understand the reasons why it's inadequate and wrong, and then we've got to be able to convey those. In some ways, we're sort of, we're playing on our adversaries' terms when we are continuing to try to go, you know? That all the evidence like trying to get all the CVR's to look at them. If you don't have the artifacts from the machines, to verify that the CVR's are an authentic representation of what occurred, they're kind of meaningless. But right now it's barriers everywhere, right? Public officials are keeping us from getting CVR's, the log files, they're incriminating and going after public officials who try to make copies so that the images can be examined. It's all uphill battle from here. The good news is, in the end, we win. It's just a matter of how much pain it's going to be between now and then. And part of that will be how many people we can recruit to our perspective so that they understand what's being done to them and will help change it by implementing a system like we recommend, you know, hand count under video at the precinct level. You don't need experts. I really want to see elementary school teachers to do the counting of votes under video because they should be able to count and it will be, I think, good for their reputation to be involved in doing their civic duty so.

ASG: All right. Awesome. George is asking: Shawn, do you have a website?

SS: Just CauseOfAmerica.org. That's where all this stuff will go. So the guys have been working on this --it's been a long time coming but we've got people working on getting the website the way we want it and then we'll be posting links to all the kind of videos that we've done and we'll be producing some more explainers of what's wrong with risk limiting audit, etc. What's wrong with the body system testing lab testing. What's wrong with the fact that we don't have a single voting system in the country certified to a standard newer than 2005. I mean, seriously.

ASG: Alright, awesome. Well here we are, right on the button. So thanks you guys for being here and I'll get an e-mail out to you in the next day or two. And thank you so much Shawn for sharing all of this information with us. I see a lot of appreciative and thank you comments that are all directed towards you in the chat. So thanks everybody. We'll see you next time.

SS: Take care, everybody.