TRANSCRIPTION* RESEARCH ROUNDTABLE #4: MACHINE VULNERABILITIES PART 2: 9/19/22

ASG: We're glad that you guys are here. Welcome. I'm glad that you chose to come today. I see Colonel Shawn Smith is on with us. So hi, Shawn. Welcome.

SS: Hey.

ASG: I'll hand it over to you as far as continuing our discussion for how to characterize vulnerabilities in terms of severity.

SS: OK, so vulnerability, severity, there are a lot of different systems for doing this depending on whether you're using NIST's original system or risk declarations but the most commonly used throughout the cyber environment is CVE. I know NIST is trying to push their NBD, but they really use Mitre's, originally called "common vulnerability and exploit framework." So if you go to CVE under Mitre or you go to CVE details you can see the different vulnerability ratings, they rate from zero to 1, which is like the lowest end. This is basically something that's a very, very low level vulnerability, up to 9 to 10. If you see something that's a 9 to 10, that's basically like watching the guy who's packing your parachute throw lit cigarettes into the parachute while he's packing it. Nobody should be using any of those live, especially not for anything critical.

Under CVE details you can go see those. Those and basically the higher the score from zero to up to 10, and the more of the higher-level, anything that's, you know, kind of five or above, if you see multiple 5 or above vulnerabilities, to use that safely, you really have to know whether or not your systems have mitigated those vulnerabilities. Sometimes they just require a patch, sometimes they require particular configuration settings, sometimes you have to run some kind of a third party thing. You can't look this up for your proprietary software for ES&S Electionware or OVS, or you can't look it up for Dominion's proprietary software, but you can look it up for all the third party software and hardware that they're using, and sometimes there aren't enough of them.

For example, there's a motherboard on the ES&S DS200s and this motherboard is the Jetway motherboard. I think it's like NF90 or something like that. That motherboard is a tiny little…how do I describe this? It's not something that's typically sold like to consumers in a retail environment. It is something that is embedded. So if some vendor like ES&S is going to produce a system and then distribute it, they buy these components and they embed them. And even though the outside of their tabulator says DS200 and ESS on the inside, it's still using computer components made by these exact same manufacturers in overseas, primarily in China.

But you can look up, for example, if you pull up Windows Server 2016, which is used in a large number of our voting systems, what you'll see is that it has 26176 known vulnerabilities. And over almost 600 of those are a vulnerability that would allow the execution of code. So, gaining a privilege is a pretty significant vulnerability. And remember that attacks and vulnerabilities

are usually not just like a single vulnerability that's exploited. It's usually a chain of exploits like, you know, imagine this in a physical security environment. The first vulnerability might be that somebody doesn't log that a camera was turned off, and then the next vulnerability is something that camera would have caught. For example, somebody leaves a door open in the back of the building, and it isn't brought to the attention of security people. Then the next exploit is that somebody walks through that open door. And then the next exploit is that they find an unattended computer and they stick a thumb drive into that computer for 30 seconds. They pull it out and walk out, and now the network in that building is compromised. And so it's not one thing that occurs. It's typically a chain of vulnerabilities exploited, and this is where the APT (advanced persistent threat) groups and organizations are constantly building these architectures of vulnerabilities that they can chain together.

I want to say like in the Solar Winds compromise, not in Sunspot, but in Supernova, which was the second Solar Winds compromise, there was actually a chain of like 17 exploits that were chained together that produced that final result of compromise of the systems. And so, hygiene matters, but these little things that look like they're not very severe may in fact be the open door that leads to a more severe compromise. So the thing to understand about this is just that you can look up all of these third party products. You can look up Microsoft, you can look up drivers and stuff like if they're using Adobe Acrobat (which many are, if they're using SQL Server or post progress), if they're using any of those third party software, non-proprietary voting system software, you can look up the vulnerabilities for the systems.

The other thing to note about that, is that the only reason that all of these vulnerabilities are published, that they're available, that people are aware of them, is because lots of people were using them. So Graco makes infant car seats. Imagine Graco makes and sells a million of a specific model of a car seat. And then, you know, one person has an accident and the safety belts don't hold and the infant is injured or killed, and then another one does. They get to a certain number of instances of these vulnerabilities being discovered, of these deficiencies, product deficiencies, but you only get that exposure when the products are exposed, right? You only find out about those when the products are exposed to multiple consumers. So the fewer people using them, the less the chance. Now imagine if (and this happens, this is part of what the attorneys do) they try to get non-disclosure agreements. Somebody will have a car accident, their safety belt fails, or their airbag doesn't deploy and they get paid off. Right? Instead of the information then becoming public, those individuals are paid, they're signed under non-disclosure agreements and then the other 999,000 customers don't know that they're driving around with an unsafe product, and that has happened repeatedly.

Now translate that framework that lends to voting systems, with all the software that's on them. Commercial software, we can see the vulnerabilities for it because it's been exposed, right? Millions and millions and millions of users are using Microsoft Windows. I think actually hundreds of millions are using Microsoft Windows. So that's where you discover these vulnerabilities is because they get exploited and then there's a report and then it gets published and studied, etc. But for the proprietary software, there's nobody looking at it except for the voting system testing labs, which already told us that they don't have cybersecurity expertise.

And Clay Parikh, who did their cybersecurity testing, already told us that they do not do adequate security testing. They won't let them do really adequate or competent security testing. They're highly circumscribed.

So let me pause there for a second and see if anybody's got any questions about characterizing severity or the implications of it or why the fact that we don't have access to the voting system software, that proprietary software, what those implications are. Let me just pause for a second for any questions.

EM: I have a question. This is Elaine from Utah. I'm not up on all this tech stuff, so I want to make sure I'm doing the database right. So I went to the website and I put in the Verizon wifi hotspot that they use for all the poll pads and that they use for all of the Internet voting as well. And it came up with one vulnerability. So I could take that one vulnerability and document it and use that when I'm talking to the counties about different things and it says it leverages a position in the wide local area network, which is what our state brags about, having a wide local area network for their election system. So is that the correct use of this website?

SS: Yeah. Mitre built the website as part of their consultation and advisement to the federal government so that they could help facilitate and enable the sharing of vulnerability information among private and government parties. So keep in mind that's another thing. I'm glad you said that because there are lots of vulnerabilities that the federal government is aware of in some organization, whether it's within the Department of Defense or whether it is within the intelligence community, there are lots of vulnerabilities in commercial software that are not listed under CVE details. There's a whole executive order on this, which the bureaucracy follows in the spirit of someone who doesn't want to cooperate and figures out how to not cooperate but within the letter of the law. So the intelligence community sometimes will find a vulnerability that hasn't been published and then they sit on it for the maximum amount of time that they're allowed to before they make a notification with the determination to congressional oversight through National Security Council that either recommends that it be kept secret, covert, or that they they notify the company and the end users.

So for example, let's say, I'll just make up a three letter agency: the BSA, the (bs) agency. Let's say they find a vulnerability in Microsoft Windows or Microsoft Server 2019 and they don't want to tell Microsoft or anybody else about it because they want to be able to use that vulnerability to gain access to some foreign threat computer network. So they follow the letter of the law. Presumably sometimes not. But they follow the letter of the law in how long they can sit on it. You know, maybe they haven't provided notification because they're still analyzing it. If you could see me, I'm making air quotes, right? So we used to do this with satellites. Satellites are supposed to have a registered satellite number, unless they're debris. They're supposed to have a published orbit. But if they maneuver, or if you say that they're debris when they're not really debris, then you can defer giving them a tracking number. And when you do that, then you aren't publishing their location and it makes it harder for adversaries to find them. So same thing here. Government agencies may have a legitimate motivation, but not a legitimate conduct in in keeping this information. So keep in mind you're not looking at

all of the vulnerabilities, you're looking at the vulnerabilities which have been made public. What is that vulnerability mean on, for example, Verizon's wifi routers? First of all, keep in mind there is no certification or testing whatsoever. None. No federal standards, no requirement for testing for anything outside the voting system. So risk limiting audit software, the computers it runs on, your statewide voter registration systems, the polling pads, all of that is not being tested or certified to any standard. I'm not aware of any state where they are testing and certifying that equipment to any standard.

And then I know for example like in Colorado, the state legislative auditor has a responsibility to do assessments of information technology security and they've done some assessments on our statewide voter registration system and then they hid the reports. So they made the reports nonpublic, they did not disclose them to the public. So I don't know exactly what was in the report, but I know it wasn't good because if it was good, they would have been crowing about it.

Now back to your Verizon router. Yeah, you would look up those vulnerabilities. Your System Administrator should be looking at those vulnerabilities.

EM: They should be looking at what?

SS: So when you pull up a vulnerability it'll give information about whether or not it has been mitigated or is mitigatable. There'll be a link to references for it. There'll be signatures. If it's something that can be detected by intrusion protection detection or penetration testing software, they'll have a signature listed for it. And then if these systems were actually being tested and certified, what you would do is you would go to the test report and you would say, “OK, did you test it against commonly known and published vulnerabilities and exploits?” And they would say, “Yep, here are all the ones that applied. And this is what we tested against and this is what we found.”

And this is another way that you go and you can look at our test reports for our voting systems and you know that they're just wildly incompetent and inadequate because they don't even mention--they make an assumption that the vulnerability is that the third party software that they're using, third party software and hardware, is essentially secure. That is a completely invalid, unjustifiable, inexcusable assumption. And yet that's what our voting system testing does. I'm sorry, Elaine, that was a super long answer.

EM: You know, it was perfect. Thank you. I just have one follow up question. I do have copies of the not-so-great cybersecurity spreadsheets that they did. They're very difficult for me to read. But I could go in there and get little pieces of the system and the applications and software and then I could reverse engineer it to find the vulnerabilities as well. Is that what you're saying?

SS: Yeah, is there a particular voting system that you're thinking of?

EM: ES&S is our biggest one but we can't find anything on Unisyn either, so I mean, we could do either one.

SS: If you go to EAC's website, go to EAC.gov and then you click on the little hamburger stack that lets you pick menus and you go down to voting equipment. You can click on voting equipment information and then down at the bottom of that page you can click on certified systems and certified voting systems there will give you the ability to search by the voting system name, manufacturer, testing standard, etc. So for example, you could search for all Unisyn voting systems that have a test report on file indicating that they were tested by a VSTL and maintained certification and you'll see test reports in there for like OpenElect versions.

So let's say I go there now and I open up a relatively new system. This is OpenElect that was tested in 2021, it's 2.2. I can go down and scroll on that page to the open elect 2.2 test report. It was conducted by ProV&V. It was done on the 29th of October 21 and you can look for the list of hardware and software and it'll have the make and model in there.

Excuse me just a second. I get somebody's calling me a second time.

EM: That's perfect. I'm trying to figure out exactly what I can use because I'm not real technical, but if I can tell someone who is, what to do, they could go and look and know what they're actually looking at.

ASG: For sure, and I put the link in the chat where Shawn recommended to go look.

https://www.eac.gov/voting-equipment/system-certification-process

SS: Sorry about that. So looking at that test report, I can see it's using PDI ScanPage scan through ballot scanner. It uses Morex2699 computer chassis. The motherboard is a Jetway, the NF9D. Does that sound familiar? The NF9D, right? That's the same motherboard that's in the DS200. Isn't that funny? That's the exact same motherboard. Every motherboard I've found so far has been made in People's Republic of China. Which makes sense because almost all of them are made there. So yeah, then you probably look for something like that for the J and NF9D for that motherboard, you probably will not find a lot of vulnerabilities in there because their level of usage, they're, you know, just a fraction of how many people are using Windows. And then also most of these are going to be in some kind of an industrial application or like a third party or embedded application like the vendors use them, like the voting system vendors use them and they are not going to be telling anybody when they find a vulnerability if they even find it. That just doesn't happen because they're trying to protect.

Imagine if you're somebody who makes a television like Samsung, and they use a motherboard in the Samsung that is manufactured by some other company. Now if Samsung finds out that there was an exploit on their motherboard that allowed a third party to intercept data coming off that motherboard, including video of the inside of your house, or audio recordings, or audio and video recordings of the inside of boardrooms where those Samsung monitors are hung, is

Samsung then going to say, “Hey, guys our bad. We included basically malware on the hardware in all the TVs that you trusted us and put in your corporate boardrooms.”? Hell no, they're not going to do that, so it just doesn't happen.

But anyway, you can go to the EAC site and pull up the test reports if they're there. And if you can't find one for your voting system version that you're looking up, you can probably find a proxy. Like maybe you can't find 2.2, but you find 2.3. Then 2.3 will say in the report that 2.3 is a modification of 2.2, and it'll sometimes list what changed, and from that you can tell what you need to know. Some significant part of how 2.2 was composed or comprised, if that makes sense. Sorry if I'm talking fast.

OK. Any other questions before we move on to what you what's been confirmed and verified?

RR: Uh, yeah. Shawn, this is Rick from North Carolina. How are you?

SS: I'm good, thanks.

RR: Good. Real quick question. As we go through these and we see all these vulnerabilities in here from a strategy perspective, how are we handling this from a legal perspective? You know, you would think with all this, this information being widely available to the general public that somebody would be looking at this and taking it and building it against all that kind of good stuff and maybe trying to make it from a nation national perspective, some kind of a court order to resolve these issues. What’s your experience been with that so far?

SS: Well, so far we've presented some of this information in a couple of the court cases where there have been plaintiffs requesting injunctions against use of the voting systems. So in Lake v. Hobbs in Arizona and then again in and I can't remember the case name in in Alabama, but there were multitude of expert witnesses including Clay Parikh who's excellent and Dr. Daugherty talking about the vulnerabilities and what they've seen in terms of manipulation. So, so the vulnerabilities are basically the open door, the evidence that they've been that the open door has been used.

So, there's three parts. The vulnerability is the open door, then there is the requirement for there not to be open doors. That's the voting system standards. The systems are supposed to be secure, they're supposed to be configured so they don't allow unauthorized access or unauthorized manipulation or any action to take place without being logged and detectable and auditable. That comes directly out of the voting system standards. And then the third part is then the evidence that they have been used or manipulated, that those exploits have actually been taken advantage of. And then the 4th part is correlating that to a specific actor, to fraud.

RR: Has the third part been addressed in the courts, though?

SS: Yeah. So Dr. Daugherty, testifying in Arizona and in Alabama, testified to what they found in Mesa in report #3. So the report#3 in Mesa was the first time that I'm aware of that there was

a direct evidence from the voting system computer. So you had Antrim where the system flipped the votes, but where the claim was all that was an operator error. So like Williamson County, Tennessee, Fulton County, Georgia, there have been lots of places where there's this track record of scanner Tabulators that are scanning ballots not indicating they have an error and then not including all of those ballots in the final tabulated results. Well, in in Mesa County Doc Daugherty was testifying, but it was Jeff O'Donnell with Doctor Daugherty validating. And that report #3 the forensic report #3 out of Mesa County where they showed that you had tabulated vote databases on the election management system server that were manipulated.

So there's only ever supposed to be one active, essentially master, database with two sub databases that tabulated and adjudicated databases, and they showed because they could compare the before and after images, that the tabulated vote database that the system started the election with, was then duplicated but not completely and ballots were transferred into it, but not completely. And when those ballots were transferred they lost the chain of evidence so they broke the chain of evidence that would allow you to correlate the election results that the system reported at the end with the ballots that were scanned. So people have tried to refute it. The District Attorney out in Mesa County is a--I don't have any non-profane words to describe the guy--but he did a little dog pony show in front of the board of County Commissioners and I'm not making this up. First of all, he was not under oath, which is telling, but secondly, his report was that all of what the forensic examiner saw was explainable by the actions of the voting the election staff and their proof of that was they showed. Grainy incomplete video of the room and claimed that what the staff was doing on the voting system computers caused those changes.

Now we also have and, I have to be careful how I talk about this. We have another whistleblower who has confirmed, based on this individual's knowledge as having been an administrator for databases for voting system vendors, that what the what Doc Daugherty and Jeff O'Donnell saw in terms of the manipulation of the databases on that voting system and Mesa is not possible to create by the deliberate or inadvertent action of any operator on the system using authorized functions, which is what everybody else had concluded also. But now there's somebody from the inside also confirming that. So we got dismissed twice now on standing. But nobody has heard that evidence and refuted that evidence. So that's a shame.

RR: All right. Thank you.

SS: Any other questions or on to the next topic?

ASG: Shawn, I know you want to scoot on to the next thing, but just to kind of tie up this piece. I remember you put this specific talking point in the agenda, how to characterize vulnerabilities in terms of severity, and from where I'm sitting, they all look pretty severe, especially if they're published and we know about them, and then there's the severity of the ones we don't know. Is that what you intended to cover when you added this to the agenda, or is there something specific that you wanted to convey with this particular talking point?

SS: Yeah. No, I just want people to be aware that there are different sorts of severity. And also that something that looks to be a small thing could be big. It's that whole, for want of a nail, the shoe was lost; for want of a shoe, the horse was lost; for want of horse, the rider was lost and the message never arrived; that whole thing. Cyber is like that. So that's why I was trying to make the point that unsophisticated actors, like a dumb, opportunistic thief who walks up to a building and the building is secure, that's it, right? The doors are locked, you can't get in, you can't get in to steal things. If you're not dumb, then what you do is you have a longer-term plan, right? You don't just figure out that the building is secure, you show up ahead of time. You observe normal patterns of activity. You see that on their on their breaks, somebody leaves the building to go smoke in the back and when they do that, they don't watch behind them to make sure that door closes. And so you know, when you're the non-opportunistic smart planning thief, you actually show up and maybe you catch that door before it latches and you just stick something in that will prevent the tumbler from going all the way in. Or maybe you remove a couple of screws from the bolt so that when you pull hard on the door, that just pulls right out. I mean, there's lots of different ways, and I used to be kind of a miscreant as a kid, and so I've done some of this myself. But the thing to understand about the cyber vulnerabilities is even a small, minor, low severity vulnerability by itself may not be significant, but when you chain it together with other, even minor vulnerabilities, you can sometimes produce effects that are much greater than the sum of the parts. I just want everybody to understand there isa scale. There are thousands and thousands and thousands of known severe vulnerabilities even. I mean, Microsoft Server 2016 I think has what, almost 600 severe vulnerabilities by itself? That is running on most of our voting system election management servers. So, so the chances that the people with no cybersecurity background or experience who don't do adequate testing and are only testing to--at best—a 2005 standard, the chances that they have mitigated the vulnerabilities in Microsoft Windows or Microsoft Server is ZERO. The chances are zero. And there is no backstop to that, so you've got some people who claim to be IT capable and IT professionals within the county and state elections staff are accessible to them. But I've seen their work, I've spoken to some of them. They're just not good enough.

And, they're not even looking. But they're not good enough if they were looking, so that was the whole point of that.

ASG: Thank you for clarifying that. It ties back to what you said at the beginning about the chains that it's not like they're doing one thing and that's it. It's all chained together. A lot of them are chained together and that ramps up the severity. OK, awesome. What has been confirmed and or verified about our voting systems?

SS: Clay Parikh has confirmed that he was able to hack into every single one that they tested. So he tested for Wyle, then NTS, and then Pro V&V from 2008 through 2017. There wasn't a single voting system that he was responsible for the security testing on. He was a subcontractor to those labs because they did not have their own competent cybersecurity pros. He was not allowed to test at the level of kind of professionalism that he was accustomed to doing test work for the Department of Defense. He had been with Army threat systems management office. That's one of the, I would say, the two most capable red teams that are accessible to

Department of Defense. And you've got Air National Guard, the 177th, you've got some other cats and dogs. But most of the very good teams are coming from the NSA's teams and that's what he did. I think he was mostly an analyst and less a keyboard guy, but I haven't talked to him about that. But anyway, he did their security testing for Wyle, NTS and ProV&V and he said every single system he tested he could hack into in five to 10 minutes. Some as little as 2.5 minutes. And he said they never met the standards, they weren't secure for the standards and they never came back and tested mitigations.

So if I built a product like a hammer, and then I took the hammer through testing and it was supposed to be able to strike a metal plate with a certain amount of force 10,000 times without breaking and I struck it, you know, 5000 times and it broke, I'd have to go back and fix that problem and then bring it back for retesting before it would be certified. But that doesn't happen with our voting systems. Parikh explained that the systems would get certified anyway, even though he found all these vulnerabilities and nonconformance with the security requirements of the voting system standards. So we know for a fact, because he did the testing, that they did not meet the security standards. We also know for a fact like Williamson County, Tennessee is a perfect example. This is where we know that no safeguard for our voting systems is actually providing any reason for confidence that the voting systems are secure or accurate. And we know that because the voting system in Williamson County, Tennessee went through the whole certification testing. That whole regime of acceptance testing, of logic and accuracy testing, and in the conduct of the election it never gave any indication. No error message, nothing. No indication that it was doing anything other than an authorized function in anything other than accurately counting the election the votes that were tabulated through it.

This was ICP's Imagecast precinct scanners on a Dominion Democracy Suite system in Williamson County, Tennessee. The only reason that election officials became aware that there was a problem with that voting system is because there was one election judge who, you know, was like a card counter keeping count of the number of ballots that the system said it had scanned. So I can't remember what the number was, but she knew how many numbers it was supposed to show and then they got to the end and the election results showed a different number and she said that doesn't match. The county had to do it on their own. They went and ran the ballots that they had scanned through that precinct scanner through a central counter and then to make sure that that count was correct, they hand counted those ballots.

A couple of points: nobody would have ever known that that election result was wrong if that one election judge had not been keeping account in her head. When that's your system, every single safeguard has either failed or been inadequate. They're placebos, right, because they don't do security testing. They do security testing in air quotes, but they don't do the security testing you would need. They don't even come close. They don't even have a standard under 2015 or older voting system standards for supply chain anything. They don't even mention it--the first time they mentioned supply chain security is 2021 VVSG 2.0 and no voting system in the US has been tested to that standard. None. The newest testing standard that any system has been certified to in the United States is 2005, before anybody was even talking about supply chain vulnerabilities.

ASG: Did we lose Shawn?

SS: Was it something I said? On my end it said someone removed me from the meeting. OK, so anyway, we know that the safeguards are ineffective. They're a complete sham. Those are the same safeguards for all our voting systems now, every single time any independent forensic examiner gets to the voting systems, for example, Mesa or Maricopa, or in Georgia, in Fulton, in Georgia, where you have the Curling case. Where Alex Halderman, the computer science professor from University of Michigan got a hold of the ICX touchscreen device from the Imagecast XTouch screen voting system from Dominion's Democracy Suite. His examination--he tried to report this in 2021, and the both the vendor and CISA refused, and the judge sealed it. He finally did an unclassified declaration or an unsealed declaration didn't include the specifics.

When we finally got a hold of this report, it was then turned into a system notification over a year after he offered the information to them. In other words, CISA and the Election Assistance Commission and Dominion Voting Systems allowed US voters to vote on a system that they were told was vulnerable, that he tried to give them the information about, which they did not mitigate. They allowed that to happen in the November 2021 election. Never said a word to voters, not a single word. Never went back and examined all the artifacts and logs from those systems. And then finally the report, the notification came out and now everybody knows that there were these critical vulnerabilities on the ICX during the 2020 election, during the 2021 election, which according to Halderman would allow flipping a vote and the changing of election results.

Not just on the ICX itself, but because you move thumb drives in between the ICX and the EMS server, it could allow you to corrupt the whole voting system or install malicious code on other components because of that transfer and connection. So we could go into some more details, but just a bit as every time an independent examiner gets a hold of the voting systems, they find at a minimum vulnerabilities and then that election records have been destroyed. We saw it in Antrim, we've seen it in Maricopa, and we've seen it in Mesa, that the election records necessary to do the audit to verify that the system has only been operated in an authorized manner, those records have been destroyed. When the records are destroyed, then unless you watched it in real time, you don't know what happened on the machine. At that point the only way you can verify what's true about the election is to go back to the paper. I think it's the bottom line there. So our actions to get that done is going to be extremely difficult but we'll talk more about this in other forums. This isn't so much for research roundtable, but, there's a huge hurdle to overcome. Like the clerks don't want to do hand counts and people doubt whether they can. There's deliberate sowing of confusion and doubt, right? It's apparently not possible to do what our ancestors did, and it's not possible to do what Canada, Germany and France all do for their federal national elections, which is hand count. That is totally not possible for Americans to do according to all the talking heads, which of course is nonsense. It's nonsense. But there's a hurdle there that we're going to have to overcome.

So if you can't get rid of the voting systems completely, then at least press to do a hand count before certification. I mean, what's the cost to do the hand count if you have volunteers or use school teachers? And we've got a hand count guide that I'm supposed to be finalizing that we're going to publish. Everybody will have it available to them. It'll explain how we recommend doing it under video, how to set up the cameras, that kind of thing.

Any other questions?

?: Hey, Shawn, do you have a timeline on that?

SS: Yeah, months ago. The team's just waiting on me. I'm building this retaining wall and I'm getting better, but I'm super incompetent. As soon as that's done, I've got the table to do the demo of the precinct hand count set up in my garage. It's just covered right now with parts. So I'm going to pull that off, set up the cameras on the tripods, do the demo of the hand count procedures. I could probably say we'll be able to distribute that just the hand count guide without the video demos and training, I would say this week. I think it's basically, it's been basically ready for months. It's just that we wanted to do the demo videos and also all the cost estimates and the diagrams for how to set everything up and I needed to go through that proof process to make sure that our recommendations for camera positions were correct. This would be something that would be official. You set this up. Although I would also recommend that anybody be allowed. I mean the only thing that should be private is this correlation of a specific ballot and votes to a specific voter. Everything else I would say bring your cell phone camera, record anything you want. We don't care. It should all be wide open to the public. If you've got to hide it, it's probably wrong.

EDIE: Hi Shawn, this is Edie in Massachusetts. I have a question. I guess the question is what can we do to prevent intrusions or you said if you can't prevent it then catch them in action, like watch them real time. So is there any way we can do that?

SS: Here's what it takes. So let's say my desktop computer right here was a critical national security system, which would be terrible and hilarious at the same time. But let's say it was if you wanted. If you were responsible for the security of this system, and you wanted to make sure that nothing illicit or unauthorized was happening on it, you would have a secondary computer that had taps into it that could watch all of its processes. You could watch core execution. You could watch power usage. You could watch temperature. Levels for video card because you can use the processor on a video card just like it's a regular main board processor to run functions that would then not show up in the logs of the main CPU. You could use the hardware management engine or VPRO functions which is like a separate computer underneath the hood on the Intel 579 and Xeon processors to run functions that don't even show up in Windows. So Windows and the user using Windows would not even be aware those are happening. You would have to have that secondary computer with intrusion detection and protection software. And then not only signature monitoring like when you do like antivirus signatures that you know those are getting updated everyday. Not only signature monitoring, but heuristic monitoring of processes.

You would establish in a controlled environment, what does it look like when the system is operating normally. Every single process, every single user, every communications port and then you'd be monitoring deviations from those. So if you see intrusion detection protection and monitoring software and then you would have an operator that's then monitoring that software from that system. Maybe they only are warned if something is out of bounds or a trigger is set or whatever. But you have to have a person that's ready to act and so on systems that are really secure that are really critical, this is how we do it. For example on my radar system up in Massachusetts, running the radar down in Cape Cod. If our system reported something, a warning that didn't match other reporting systems, if there was a reason to question it, the first thing they did was cut our comm lines off at their end so that we could not send them any more notifications and that would begin the investigation process. That was actually the very first thing I did as a commander of that site was conduct an investigation into why our system reported something that it did, and it turned out to be a completely innocuous explanation, but they didn't trust the system until they got that explanation that explained the phenomena. So that's what you would have to do to protect the system. It's not possible to do it without that kind of access.

And then of course, having that access, now we can talk about something. So for Department of Homeland Security, for CISA, there's a nonprofit called CIS, and CIS provides a service or function called Albert Censors and they provide these to now thousands of jurisdictions around the country. And these are supposedly not monitoring voting systems, they're monitoring election systems like the E pollbook systems and the voter registration systems because if they tap into the voting systems, then they provide a conduit into that voting system, right? So it's a window. But a window is a window, right? Regardless of what you meant it for, if you create an opening that now becomes an attack surface. And honestly, you know, I don't have a lot of confidence in DHS or CISA to secure anything. They couldn't even secure their own networks. They didn't even know their own networks were compromised for 10 months and they never found out on their own; they had to be told by somebody else.

So the short answer is no, it's not possible to monitor without being tapped in, without having purposely built tuned software capabilities and trained cyber defenders that are monitoring them. It's just not even remotely possible in this threat environment.

EDIE: Alright, thank you for explaining that. That's very helpful.

SS: Sorry, I know it's a downer, but that's that's the truth.

ASG: Kathy, did you have something else?

KT: Kathy from Idaho. Shawn, thank you so much. We are going to have a Commissioner meeting on October 6th and I would dearly love to have the information you're talking about to present because we're going to ask them to do hand counts on three random precincts. And my question is, is it a problem giving the ballots over to the county and then maybe assuming

that I'm going to do the hand count somewhere prior to certification if they have those ballots in their possession? Is that a concern? Do we need to be doing those handcounts in-precinct the night of the election?

SS: That's what I would recommend. The precinct officials are election officials, and election officials under the federal statute are obligated to preserve their election records. So you have the ballots, which are election records, the precinct officials are election officials, and they have a federal statutory requirement to preserve the election records. Now they're permitted to transfer them to another election official. But they must maintain access to them, etc. What I would recommend is that the ballots be hand counted before any video is ever turned off. I don't, I don't want to hear from anybody about their security systems and their locks on their doors or any of that because I can personally bypass almost all of that and I'm not even at the high end on you know, facility penetration. I'm kind of more just that I can see the opportunities. I'm not the guy who brings the tools.

So I would say you want to hand count at the precinct. If you can do it, that's where you want to do it. And you want to have, you know independent monitoring of those ballots until the count is completed and also, you want video recording of the count if you can pull it off.

KT: How am I going to convince them to do that the night of election when they want the results, chop chop, and I can't get it done fast enough?

SS: Have you ever heard you can have you can have it accurate or you can have it fast? Pick one. So if you want to secure election, hand count it. So that's what I would say. Now a lot of places want early reporting. They want the results on election night. I've got no patience with that. I think it's totally possible if we hand count at the precinct level to do that because you're only talking about 4000 or fewer ballots in every single you know precinct in the US there isn't a precinct in the US with more than 4000, most are 1100 to 1200. So I think with 10-12 volunteers you can count a precinct in a couple hours but let's say they're stubborn or for whatever reason they won't do that. I think you could do the election night reporting and just require that you begin the hand count of the ballots the same time or maybe the next morning if you've got adequate security and monitoring in place to make sure that the ballots are preserved and secure, not reachable, not alterable.

KT: OK. Thank you.

SS: I apologize, I'm going to have to jump. I've got a call that I have to go respond back to from one of the attorney teams. But the people who are on, if you guys can talk maybe about any other vulnerabilities or issues that you're aware of that each other should be aware of, and especially anything you know? We'll start on these, explaining what kind of materials we have in the library on these topics. We're still going through some teething pains trying to get our library set up properly, but you'll be able to search for the documents and they'll be sort of predefined searches that will let you find things. And we'll try to make sure for the roundtables that we tell you what we've got on a specific research topic, but if you guys are aware of

anything else you want to share with each other, you know, approaches and techniques well, all that we're building with coming from the states. Our purpose is to share what each person or each state has with all states, if that makes sense. So I appreciate everybody coming and asking questions and I'm looking forward to having more discussion with everybody. And I apologize for having to jump, but I owe some answers back to these people.

ASG: Thanks, Shawn.

SS: OK, thanks, everybody. Take care.

ASG: All right, what else would you guys like to share? Maybe about vulnerabilities that you've discovered in your local systems? Yeah, Burl.

BS: Yeah, the link that I dropped in the chat to South Carolina research. What we did was we put together a Whitepaper both on the 2020 election system that is utilized here ESS 6.0.2.0 which was used in 2020 which ran on Windows 7 and W2K8 server, or 6.1.1.0 which is based on a Windows 10W2k16 platform. So what we did was we was we actually looked at all of the cyber security vulnerabilities associated with those two operating systems within that network and then we really paired it down to look at only the highest level issues and that would be issues of remote access and being able to gain administrative access. So if you look at that data you'll be able to see the methodology that we used in going and pulling down all of the applicable vulnerabilities.

As Shawn was just stating, he said for Win10, what what was he saying on the level of 800 or W or W2K16 on the level of 800 you'd be able to pare those down and identify which ones are most likely to be an attack on your localized system and then I guess the biggest issue for all of them is being able to make sure that the patches are done to those systems that at the county level to be able to counter that. And you know at this point I don't see any evidence of that here and so you know I have a great concern there. But even if you did make sure that all of the patches, security patches, were placed onto the system for instance and I'll just give one instance so for the system that was utilized in 2020 here in South Carolina, a couple of the largest vulnerabilities which was Log4J and Daxin weren't discovered until November-December time frame of 2021. However, they were having vulnerabilities since 2016. And possibly as far back as 2014. So the only way to identify whether those vulnerabilities had been exploited would be to do a full forensic audit of the system and be able to count every ballot at the Precinct level and then validate that through the entire system to the certification. Hope I didn't lose anybody.

ASG: Does anybody have questions for Burl about that?

?: I'd just like to know, how the heck did he get a hold of his machines to actually get into that kind of interrogation? That sounds very impressive there in South Carolina.

BS: Well, what you do is you go to the EAC certifications, you identify what systems are being utilized within your state, and then from that all of that information is available on the web, all of the certificates -- so-called certification data – as I've mentioned before in my findings, what I've identified is the laboratory certification is weak. I think we've identified that several lab certifications were actually invalid in 2020. The certification itself is weak and then the testing is weak and with these tests, there's an associated test plan and that test plan is for that specific build and then there's a test report that's written on it. So it's not only that you have a test plan and a test report that surrounds the certification of that specific unit and it doesn't matter what manufacturer it is or what build, but then it's also based upon the process of the use of that system.

So when Shawn states that there are literally thousands of vulnerabilities he's speaking to vulnerabilities not only within the systems themselves, but also the process by which that system is meant to be used. For instance within the system that we use, we depend heavily, heavily upon flash drives. The largest breach that I'm aware of, DoD was done on the Siprnet, which the Siprnet is a secure network that isn't tied to the Internet whatsoever. You always hear this, this whole thing, "Well, you know, we're not tied to the Internet." So we have to understand that you don't have to be tied to the Internet in order to be hacked or vulnerable. But my point is those flash drives, I don't know of anybody who has custody of them. You know where they strictly follow that flash drive, and did that flash drive ever get plugged into a contaminated system by which a virus or malware can be placed under that system? Has it been checked for that? That the flash drive doesn't have problems itself? And oh, by the way, if it does, if it got plugged into the Internet somewhere and then comes back and gets plugged into your system, you know that is the type of vulnerability that can be transmitted across the entire system and in fact other portions of the system.

ASG: Shawn said that during our last research meeting. On those thumb drives, you can have something behind a partition where it's hidden and it doesn't execute until it's plugged in. So even if somebody did check it, they wouldn't necessarily catch certain types of malware or firmware because it was accessing the print drivers or whatever else.

BS: Yeah, and another thing that I notice as far as that goes is when you look at the at the test plan and the test report, they don't identify the configuration within any information system. There's configuration management of that system that that denotes what that build is made-up of. And I don't know that all of the applications that are that are identified on that particular flash drive are resident within that documentation. We don't know unless we can go through and scan those and take a look at them. But that data is there for any of you to be able to access and go through. And if you have any questions on it, you know please feel free to contact us and we'll try to get answers back to you or work with you so that we can tell you how you can do the same thing on your system.

ASG: Great. Thanks, Burl. All right. Who else?

TP: This is Terry.

ASG: Yeah, Terry, go ahead.

TP: I'll ask that you put this on the agenda for Shawn to discuss next time. And the question is: is anyone aware of any legislation going on in any state that requires vulnerability testing by independent third parties as a condition for a system to be used. If we're going to keep using machines, and that's a big if and I'm not a proponent of it, you're going to have to have a requirement, a very strict requirement on not only the vulnerability testing, but on configuration control, and I mean configuration control on every piece of software and hardware. Just to give you a little-- my background has been a long time, but I worked for NASA. And I was not a software person, but the organization I worked with and flew for was the first to use an all digital flight control airplane. I guarantee you the configuration control on the hardware and software for any digital system going on to an airplane today is strictly controlled. There are reams of instructions both within the DoD and within NASA, giving all the requirements of how you do this. If we're going to keep using digital election systems, it has to be put under that same kind of control and it needs to be done at the state level in my view. So my question is, does anybody know of any activity in this area. So that's my question.

ASG: That's a great question. I think the problem is that the government claims that these VSTL's are independent third party, but they're not, but they're the only ones authorized to look at it and that's what's coming down at a federal level. I don't know of any legislation to change that, and if there was, I don't know how they would get around that, given how the whole system is set up basically to be rigged.

TP: I believe we still have at the state level control of elections. I'm in Texas. If Texas put a set of requirements on any election system that's used in Texas, that would require vulnerability testing by an independent lab. Not the national labs, but a vulnerability testing, then they would either have to do that, or they would not be allowed to be used in Texas. And I think they can do that.

ASG: And that's legislation that has passed in Texas, is that what you're saying, Terry?

TP: I don't know. It has not, I'm saying, but if it were, then Texas could say, “We're not buying any machines until it goes through this process of vulnerability testing by an independent third party.” I say you need legislation like that. I'm just wondering if anybody's working on it.

ASG: Well, we'll certainly open the floor so people can speak to their own states. I know something that Shawn mentioned last time was that when this comes up about how we need independent third party testing, the narrative response is, “Well, no one's qualified to do that.” Even when Cyber Ninjas came in with Maricopa with their massive amounts of cybersecurity experience, it was, well, they don't have any election experience. Well, nobody has election cybersecurity experience other than supposedly these VSTLs, which again are all part of the same sort of closed loop corrupt system. I'm not disagreeing with you, but I'm saying I'm not

aware of anything to that degree. Is anybody else aware of any legislation that's happening in their own state to this regard?

BS: Not that I'm aware of. However, if they if they did, they would fail miserably, right? So. It's probably one of those things where manufacturers want to ensure that the states are doing it themselves and they're not vulnerable. But I am in concurrence with Terry and totally believe that should be put into effect. Trying to get it done is something we have to work on collectively.

ASG: That's a good point, Burl. It would certainly not be in their best interest to have that done right, to have any transparency. And in fact, in Colorado, we've gone completely the opposite extreme to where our legislation, recent legislation, actually bans any independent third party from even looking at the systems in Colorado. So clearly it is needed, but how do we get there? Jane, you have a hand up?

JP: Yes, thank you. I want to point out that all these certifications are done at different levels. They're really designed to push the buttons and see if the system does what it is, what it says it's going to do. They're not really trying to break anything. I say that from the perspective of having developed and tested software. The other thing I want to say is just a big question. We're talking about vulnerabilities to hackers within all these systems. I really have a different perspective. I don't, I don't think that's not valuable. I think is very valuable. But I have a different perspective. I believe that these systems are designed to be used to select candidates and that despite any vulnerabilities that make them open to hackers, I'm sure there are configurations within the code that allow certain candidates to be selected rather than elected. And I believe that when those particular configuration parameters are not set right, that's when they come in with all the fake balance. That's my perspective, and I do believe that the only way we're going to win this is to go back to paper ballots and small precincts and hand counting.

ASG: Yeah. Thank you, Jane. Good point. My perspective is that all of these testing things are strictly to keep the public from asking any more. This is the party line in Colorado, gold standard, safest, most secure, blah, blah, blah, whatever. The risk limiting audit started here. A lot of these things started here because, “Oh no, look! Proof!” They pretend to prove that it’s safe when really it's just to placate people from asking any further questions. OK, Laurie, you’ve got a hand up?

LG: You hear me? Hello?

ASG: There we go. Now we can hear you.

LG: I’m Laurie in Williamson County, Texas. Thank you all for your time and talents. This has been wonderful and I was curious about Terry was talking about the independent testing. Now in Texas, the office of the Attorney General sends two examiners and the Secretary of State has three examiners, technical examiners, and all five examiners have reports that they post on the Texas Secretary of State website for each system, including Dominion Systems, that they

decided were not secure or good enough to be used in Texas. And so you can see why they did not certify Dominion and they have all those reports on there. Are you talking about additional testing Terry? I mean, because I thought that was kind of independent, but I guess those are their examiners and as Jane was saying, you know, they're there to assess if the system doesn't work and just make sure all the things are doing what they're intending to do. So we're talking about something outside of the Secretary of State, outside of the office of Attorney General site inspection.

TP: Yes, this is Terry. It would go much, much beyond them because they basically hire a couple of people and in my view, they just kind of see that it works the way it's supposed to work. There is no or very little vulnerability testing, and I mean that from the point of view that the whole system that's used, not just the ballot marking device and the tabulator. Everything that's used in an elections office needs to be together and connected as it should be connected, and then it would be subject to. Potential electromagnetic or radio wave kinds of vulnerabilities. Can somebody get into it that way? Can hackers get into it? Are there any? You know, independent hackers open the window and say, hey, here's this system. Can you get in it? And so this needs to be a fairly serious system testing. Just think about this for a minute. I mean, I know people who do this. I mean, I don't know them personally anymore. But if you go to Lockheed, they have an entire organization that will do independent testing of all of their digital systems and all the latest fighters to make sure not only did they operate the way they're supposed to, but they're not vulnerable to external forces threats that they have to face. So I'm saying that an election system is every bit as important and needs to be protected to the same level as digital systems in our aircraft or military aircraft, but even in our commercial aircraft, all the commercial aircraft you guys are all flying in today. They've got digital flight control systems that everything's digital and I guarantee you they're not subject to stray electromagnetic radiation causing changes within them. That includes all the sensors and everything that all have to be certified together as a citizen, as a system. And then of course, there's this strict configuration control. Once it's certified, you change one thing, there's a strict configuration control. There are people who have to sign off, there's part numbers, there's software releases, etc. There's complete traceability of the entire thing. And so, like I say, it's done in the aerospace industry routinely. So it's not that the country doesn't know how to do it, because we do.

LG: Were you aware of Brian McCann's discovery of the vulnerabilities in the ESS? Rush validation functions that we found in the 43 counties in Texas.

TP: Yes, I've looked at that.

LG: Christina Adkins from the Secretary of State said that SMS has been performing its own hash security testing and that they have been putting it in their contracts that if the authority, the receiving authority, the customer, the county, whatever you want to call them receive the systems and wants to do their own hash testing, that would void the contract with ESS. And so they've got a nice little situation where they're creating golden hatches and instead of matching the system, making sure that the system matches that what was certified with the EAC, those

hash number that they created a golden set of hashes and that's how they were passing that. So I was interested to know if anybody had looked into performing security checks and what other states were finding. I know there were 19 states, I think on Texas Secretary of State e-mail list, that were affected by that vulnerability. And I'm interested in in learning what y'all with those gifts have to say on that. So thank you all very much.

ASG: Alright. OK I show that we just have like less than 4 minutes left. So I think we should go ahead and wrap up. Thank you for being here today. I will send out an audio replay within the next few days, along with the cleaned up transcript and the dates for the next two roundtables and we'll pick upon the agenda right where we left off today. So thanks for being here and everybody have a great week.

**NOTE: This transcription was computer-generated, then human-reviewed and edited. Extraneous parts may have been edited out, and there may be typos and misspellings.*