TRANSCRIPTION OF RESEARCH ROUNDTABLE: MACHINE VULNERABILITIES 10/5/22

NOTE: This transcription was machine-generated by AI, and then cleaned up manually by a human. Neither is perfect; please excuse any typos or errors.

ASG: Welcome everybody to our Research Roundtable meeting. This is for Wednesday, October 5th, 2022. Today we're wrapping up our topic on machine vulnerabilities. So we have Colonel Shawn Smith with us because we have just really two more topics and then we can have open discussion in Q&A. The first piece of the agenda is: how can "regular people" identify these vulnerabilities in the system? And then the second piece is how can we share what we've learned? So with that, take it away, Shawn.

SS: I think we talked about CVE. Here's the problem with CB details. Even though it's massive, even though there's over, I want to say there's like 175,000 plus published known common vulnerabilities and exploits and—understand, to find its way in there, for the most part, those had to be exploited, so most of those weren't discovered. Some were discovered by white hats. A white hat will normally then notify the vendor or the company or the agency operating the system and give them some time to fix or patch or protect themselves and customers and notify customers. Or they tell the general public or announce it because if they release that vulnerability before the people have a chance to publish it, then it gets exploited by all the black hats, which I would include in that, not against the United States, although sometimes now against the United States, all of our intelligence community are not white hats. Or not even grey hats—they will find exploits and then they will use them before they notify anybody that they exist.

Now, there's a there's a whole presidential executive order that directs them to follow this particular process. But if you've ever been in government, you understand there's a million ways to introduce administrative delays, and they do. So many times, things are not reported until long after they have been used in the field, sometimes just long enough to install other exploits. My point in saying that is to keep in mind that as massive as the common vulnerabilities and exploits databases is, which would affect almost all of the of the commercial or third party non-voting system proprietary software and hardware that's used in our election systems, it's still not comprehensive and I'm gonna give you an example of that.

I think Amy and I were talking about this yesterday, so I won't go into all the details of how I would go looking for—as when I was doing targeting of adversary systems, not systems of systems, like looking for the most vulnerable nodes and places to affect them so that we could achieve our objectives if we had to go to war. Then, you do exhaustive research. I would go research the background of the engineers who were involved in the development of adversary weapon systems, because then I could understand what their specialties and tendencies were and I could go looking for like if they had done academic papers or if they had done other previous work I could go looking for the kind of things that they might have done, as possible avenues of exploitation.

And of course, all of our adversaries do the exact same thing, except they have massive resources and they're very good. OK, so now we've got some foundation for "as big as the CVE is, it's not complete."

Let me give you another example now of where it's not complete and I'm going to use--Can I share my desktop here? I think I can. Can everybody see what I'm sharing now? OK, good.

So this is the Dell support site. What I've done is I've got the serial numbers from the Secretary of State. She publishes, thankfully, and she'll probably change this because it's useful to us, but Colorado Secretary of State publishes this list of all the voting system equipment that's been certified.

It's actually not a complete list. She leaves a lot of things off of it that have to be considered as part of the specified configuration, but that's a whole other story. I don't think that's specifically her fault, even though it represents a dereliction of duty. But anyway, so this is the serial number embed for a Power Edge R640 that is one of the EMS servers. This was the EMS server that was brought into Mesa County, Colorado after the Secretary of State illicitly decertified the equipment that was there under the premise that it was somehow breached. It's pretty much ludicrous, but that's a whole story for another day.

So when you go to this page, you could do things like you can look up the product specifications and you can export this into an Excel file. For example, you can see that it's running a UEFI BIOS with a GPT, a graphic party general purpose I can't remember, I think it's graphic partition table. Uh, you can see that that it has, you know, a UM idrac installed. You can see what kind of RAID controller is being run on it. So you get the details on the components but you can also look up warranties like we found some of the equipment in Colorado had warranties where the equipment was registered in Australia.

That's a subject for another discussion too. I'll explain at some other point why that's significant, but you can also go over here and click on drivers and downloads and you'll find interesting things when you click on drivers and downloads. So this system was put in place in Colorado in 2021. And then you go down here into the drivers, this is Dell now recommending driver updates and you'll find all of these driver updates that are recommended here and the importance is urgent, right? I mean the pages of urgent driver updates just keeps on going now, some of those could be performance issues.

Like, you know, maybe there's some glitch where the raid controller inadvertently causes all of the raid control drives to erase themselves, but by and large, these are not going to be performance. A lot of these are going to be security issues that are not getting reported as security issues, so until somebody exploits them, compromises them in the wild, they're probably not going to appear in CRE details.

So this is the vendor pretending, oh, this is just a, you know, quality improvements. But if it's urgent, it's probably not a quality improvement. But so then you go down here and I'm going to look for one in particular just to give you the example. So here you have the Hynix firmware. Now if you haven't gone in and read the configuration, that doesn't mean anything to you. You probably don't think, oh Hynix firmware that that's critical, but this firmware runs UM raid control. It's part of the raid controller for serial ATA configuration and the and the raid-configured hard drives on that server are using the serial ATA to call.

So, here is from 12 July 2021. This critical firmware which is probably not on the server, the server for the voting system, which means whatever vulnerability is contained in this firmware, it has not been patched. Now if this was a vulnerability that could be exploited, you might think that you would come over here to CVE to see details. OK, so I'm just going to type in Hynix. Here, maybe, maybe not that one. Maybe some other vulnerability is in there. But there are no there are no Hynix vulnerabilities. So there's vulnerabilities that affect DRAM, like what is direct random access?

So there's there are vulnerabilities that affect the DRAM that are on the controllers that are like a sort of a buffering or cache memory for drive controllers, but it's not specific to Hynix so you're not going to find this vulnerability from the Dell support site driver update listed under CVE details.

Now having said that, the voting system testing labs, which are the only people who are given any opportunity to assert or to assess the vulnerability or security of our voting systems, they're not even checking common vulnerabilities and exploits. They're not even checking it, let alone verifying that the systems are patched or have been configured to avoid compromise or to protect against the vulnerabilities identified.

So my point here is that you can look in CVE details and find the published CVEs for the third party components you won't be able to find. And any published vulnerabilities in the CVE details for the proprietary components of the election systems, and the reason for that is twofold.

One, because they don't put them in the hands of citizens or the kind of people who would detect or publish those, and two, the entire election system infrastructure has been shrouded in this veil of the election integrity or the election infrastructure information sharing and analysis center. So this is in 2017, second area of Homeland Security, Jeh Johnson. Or putting election infrastructure as critical infrastructure in the United States underneath the government facilities, as a subgroup underneath the government facility sector, they basically blocked public access to information about the vulnerabilities that were detected. Which is why it was extraordinary when Alex Halderman, in his analysis for the Curling case in Georgia, determined that there were these nine critical vulnerabilities in the machines, and remember he didn't look at all of the equipment, he just looked at the IC access for that case and he tried to notify Dominion and he tried, and both CISA and Dominion refused to receive the information, while Totenberg, the judge, sealed it. And then he published a declaration which excluded the details.

And that still took another, I want to say, six or seven months before CISA finally published the acknowledgement that there were these critical vulnerabilities, and in that acknowledgement, they also stated that they weren't able to test any of the other systems that might have been affected, and they said that they found no evidence that the vulnerabilities had been compromised. But what they didn't say is that they didn't look for any evidence that the vulnerabilities in compromised. They didn't go inspect the axis. They didn't. Nor did, and this is the bigger issue, nor did anyone talk about the fact that those egregious vulnerabilities in those systems were allowed to run during elections, both before Halderman's declaration, and after his declaration. So they knew –the EAC and CISA, the federal government, as well as a couple of state governments—were aware of those identified vulnerabilities in the system that had not been addressed, not patched, not mitigated, and they'd let us use them anyway in our elections.

And what does it say about the entire regime of security certification and testing when those kind of vulnerabilities when one college professor--he's a smart guy, but he's not operating at the national security level of the red teams that we run like national security agencies or army threat System Management Office, or those very high end red teams. Mostly they don't even test defense systems to the advanced persistent threat like maximum threat level. They're mostly testing them to like a moderate APTL or advanced persistent threat level, and they still find tons of vulnerabilities if you take those kind of teams from NSA. And Tecmo, the Department of Defense red teams, or like 177th Air National Guard out of Kansas, you take those guys and give them access to a voting system, not only are they going to find so many vulnerabilities, it'll stand the hair on the back of your neck up. They will

install exploits like a Thunder spy exploit on the Thunderbolt ports on the motherboards that you can never mitigate. Once a threat actor has had physical access to the systems, you can never again mitigate that system.

This is why it's so significant that the motherboards on pretty much every single one of the voting system computers in our voting system suites are manufactured overseas. Everyone other than this running Intel drives that has Thunderbolt on them, we should be assuming is compromised. And you won't detect that without physical access, so let me pause there for a second, I know that was a lot and I kind of wandered around, so I apologize for that. Let me just pause and ask if there are any questions and check in with Amy and see if we're sort of on track for the subject.

ASG: Yeah, definitely on track. I'm really glad we're recording because you're talking fast and there's a lot of information, so that's great that people can go back and review it. We did have a question in the chat from Burl, who says, "Are you aware of any EMS certification with wireless connectivity activated on the system on Election Day at the polling place."

SS: No, I am not. And the reason I'm not? First of all, let me think about that EMS certification. OK, I'll give you an example.

So where do we start on this one? OK, when you look on the eac.gov site, you can look at the certified systems and see the list of them and when they were certified. Now not a single one of those systems has been tested or certified to any standard newer than the 2005 voluntary voting system guidelines, but some of the systems that have been certified do have—and this is what the DS200's purportedly had—the Tele LE910 chips on the motherboard was for unofficial election night reporting.

So when you have remote tabulators, whether it's a Dominion ICP image cast precinct, or whether they're using the ICE ImageCast evolution, which has that same sort of capability, it's kind of a dual purpose BMD and scanner; or whether it's a ES&S DS200 or DS6450 or 850 or 650 for the older systems, when you have a remote system that's not centralized, they have to figure out how to get the tabulated results and presumably the ballot records, which would include, you know, images on an explicit cast vote record and authentication documents that give you some some evidence of chain of custody, you have to get those to a central tabulator.

There's essentially two ways to do that. You can either use portable media, or you can transmit it. In the old systems they would use literally dial-up modems over a plain old telephone system like public kind of networks like, you know, the whole AOL modem sounds, that whole thing. And then they started evolving in when the Internet became more ubiquitous and there was there was connectivity, they used wired connectivity over those government networks that then connected to the Internet and through the Internet to other government networks.

Installing cellular and wireless technology is extraordinarily dangerous. It's extraordinarily dangerous. Not just because those are wide open, right? It's installing a screen door in the back of the submarine. That's how dangerous it is.

But the only way for you to know what has happened with those network networking devices, including wireless, is to monitor them in real time. Now, it is a measure that can be effective to have full audit trail enabled for the systems and the networking devices. And if they have the auditing properly configured

and they don't have malicious software or other illicit functions that are erasing the audit logs, which you know, I mean this is a common feature of advanced malware is to erase their tracks.

Sorry, I'm talking in circles. If you can watch it in real time, you have a chance of detecting its use. If you cannot watch it in real time, you have a far diminished chance of detecting its use. If you have logging enabled and then somebody who actually is capable; not a single election official—maybe Hayder Garcia maybe has the background, but then who's the former Smartmatic guy from Venezuela who is the elections director in Tarrant County, Texas? But very few, you know, probably less than 100th of a percent of election officials in the country or anybody supporting them has the capability or the proficiency, skill, knowledge, and capacity to go through the logs to determine that that no connection, no connection has occurred, that there hasn't been an illicit, unwarranted use of any of those networking capabilities to go outside the voting system suite to an external connection, whether it's the Internet or not.

It doesn't matter if it's the Internet. People keep saying the Internet is a connected Internet. It's not about the Internet, it's about anything outside. It could be on your phone, your phone could have malware that that runs into it. It could be a watch. If you have a Bluetooth connected watch and there's a Bluetooth device, or there's a Bluetooth device that isn't even running a Bluetooth protocol, like running Zigbee or something like that.

So bottom line is: there are systems that are certified with the capability to—and it's usually not directly into the EMS, it's usually into another system that is running like with Dominion the software or the software component is called remote listener. Remote listener is in any state that has ImageCast Precinct for Dominion or in any state that is using DS200s.

For example, there may be a remote listener that is connected either wirelessly to a cellular network or is connected to a local area network that the county or jurisdiction runs that then receives in theory unofficial election night reporting from these remote scanners while they're theoretically bringing the full data, including ballot records and images on removable media that they are then supposed to stick into the central systems download and then preserve the thumb drives themselves as part of the chain of evidence that you have election records. The problems with that—we could talk about for another two hours.

But once you take that removable media and stick it into another computer, especially the ones that's run by the same vendor, you have no guarantee that that what is on it has been preserved as a chain of evidence. You can overwrite things on there, you can alter them.

The EMS, instead of reading from it, could just be writing onto it and if your proof of what was done at that tabulator is supposed to be what's on the EMS, while the EMS does what it wants or what it's been programmed to do, and if your proof was on the removable media, unless you make the reader that reads into only like a forensically verified read only device, you can't protect the removable media from being overwritten or altered.

Sorry, I feel like that was a really long, complicated answer. Did I answer the question?

ASG: I think you did. If you disagree, Burl, jump in with another question. And in the meantime, we have three new questions. Shawn, Elaine in Utah said, “I was wondering about this. Some of Utah counties

pay for offsite election support and I was told ES&S remotes into machines to evaluate and fix any issues. What wording for this type of audit would you use to ask about this type of log audit?”

SS: So, what logs would you ask for in order to obtain evidence or artifacts that would indicate that the systems had been remotely logged into for any purpose, is that the question?

ASG: She says correct.

SS: OK, so here's the thing. If everybody was on the up and up and the systems were properly configured and you were logging everything and the logs were preserved then then you could just ask for the communication logs.

And if you asked for the communication logs, you should get logs of all port data as well as internet and network type connections. The problem is that they're not on the up and up, and the testing is a rubber stamp. I wish it was just incompetent, but I don't think it's just incompetent. They don't require specifically, as part of the certification satisfaction of the voting system, standard requirements to basically log everything you can log on the systems and then to preserve them unperturbed and unmolested for 22 months. So if you're a forensic, and I'm not, I'm not, I've seen this done. I'm not this guy. But a forensic examiner will take all the data they can get off the system.

And I've used this example before so:

With the quieting, the silencing of ballistic missile submarines with high level capabilities in the world, basically former Soviet Union, now Russia, Germany is very good, Japan is pretty good, China has been buying a lot of technology, United States, our ballistic missile submarines are so quiet because you know, under the ocean, generally speaking, subs hunt subs with sound.

Our ballistic missile submarines are so quiet that you can't hunt for the noise of the submarine. You hunt for the hole in the noise of the background noise of the ocean, and now they're adapting to even that. And so an optical shroud will actually essentially take the image from one side of the object that it's shrouding and project it on the other side, so you can't even see that the whole is there.

So you have to do the same thing when you're doing the forensic examination of a system that may have been delivered really altered or targeted, you can't just look for what should be there, you have to look for what should be there and isn't.

To do that, what a forensic examiner will do is get all the logging information and artifacts from the from everywhere they can get it on the system, for example, and then and they'll correlate all of it in a massive sort of database or spreadsheet, like a relational database, and they'll correlate it by time.

So let's say you see at 10:28:04 that a user process used a hard drive, but you don't see any service on the system that was being used to access that hard drive. Well, there's something wrong there. There should be a correlate beause the user doesn't have any ability in Windows to just reach in and touch the hard drive. They have to use a different service. So what service was running that touched the hard drive?

That's my point that you can ask for the explicit logs that should give you the information, but it's far better to ask for all the logs they have and then to correlate all the activities and events that occurred on the system at that time. If you had complete logging data, you'd be able to see things like a processor or

a core in the system processor being used, and then not being correlated to an activity or a sub function that is associated with power usage and management of power usage.

Like let's say you see system temperature rises but for some reason the core logs are not present while somebody has obscured the record on the system, but you see the temperature. So my point is, you need all the artifacts if you have a real forensic examiner and if you're not a real forensic examiner.

If you don't have that background training and proficiency, the best you'll be able to do is give yourself a false type 2 error, like a false negative like you'll think there was no illicit activity, when in fact you don't really have the evidence to show that.

ASG: So then Shawn, having said that, is it worthwhile to request the logs or not unless you have the forensic abilities.

SS: I think it's worthwhile to request them, and part of the reason it's worthwhile to request them is if you go look at the at the 2002 voting system standards or the 2005 voluntary voting system guidelines, and so the standards in particular, when you look in the section that pertains to general purpose computers, which it defines, it essentially all of our EMS servers, all of our tablets, any workstation or tower, if it comes from Dell or Hewlett-Packard, it's a general purpose computer, meaning it's capable of running lots of different software. It has multiple cores. It can be running simultaneous processes in the background. While you think you're doing one thing, your computer is basically having its own life, that's our voting system.

Computers and the standards in the voting system, standards that apply to those it specifies three additional safeguards for those type of computers could remember this was written back when? When voting system computers were a lot more primitive, right?

I mean my desktop today would have been a supercomputer years ago, and this would have been, you know, probably protected by a national security order. You carry routinely in your hand more computing power now than we had 25 years ago. Thirty years ago, the world didn't have as much computing power as most people carry in their hand now, so the standards are pretty old. They're still mandatory standards, so those are those standards in the voting system.

Standards are telling vendors and election officials what they should be preserving for an audit trail, and they tell them you have to as one of those 3 safeguards for general purpose computers or COTS. They're not really COTS, so it's a whole other discussion, but they're telling them preserve the record of any user activity, log in, log off, System start, system stops, error message, normal activity warnings, all of it. So in other words, log.

And your voting systems are supposed to be logging all of that, and your election officials are supposed to be protecting all of that from every single computer that is running voting system software. So this includes the touchscreen devices, the degrees, the BMD, and no jurisdiction in the country is doing this because they have all been lied to.

Some of them may know they've been lied to, but they've all been lied to either out of ignorance or I fear deliberately, that they only need to preserve the election project or basically the proprietary log files that are generated by the vendor software, well, those are just a tiny, tiny fraction of the log files they're supposed to produce.

So at the very minimum when you go to the to the election official and you request through open records a copy of all of the log files that they're supposed to be preserving, and they don't have them, you have the evidence, and this is how it should be framed:

If they don't have all those log files, it should trigger an immediate hand count of the paper ballots for that election.

In other words, the log files are the only thing that proves that, the election result that came out of a voting system computer is tied in any way, let alone accurately, to the paper ballots cast by voters. And it's a little bit more complicated when they use that diary, because then there's not even a paper file. You know, even the voter verifiable paper audit trail is, I mean that's ludicrous. It's produced by the computer. It's like you're trusting the computer that its output on paper is proof that its output digitally is accurate. That's just dumb on its face. But that's what some jurisdictions do.

ASG: OK Rick I will come right back to your question but Shawn I wanted to say first, you know something we were talking about yesterday. Earlier in this call when you were talking about when you went on the Dell support site and you were showing us specific components and like the recommended fixes, right, like the updates that were recommended under drivers and different things. If those updates were actually done and if the system was working, they should show up in the logs, correct?

SS: Let me think about that. You're asking if the vulnerabilities that are discovered, like patches, whatever, have been mitigated through driver updates or some kind of a software update, they should see evidence of that in the logs. Is that what you're asking?

ASG: That is what I'm asking because what you told me yesterday, and I'm paraphrasing, was that if there's any, **any** change to the software or to the systems would actually include these fixes, would violate their certification and require testing again at the state. And when you said that to me I thought, “Well that sounds like a piece that people could go after in their state because there's evidence where they can say, ‘well here these fixes are required and they weren't made.’ Or if they say, ‘Oh no, they were made,’ then ‘great, when did you recertify?’” Because that then negated the certification, right?

SS: So OK, so let's talk about this in general. So first of all for a federal certification, this is a standard under EAC for a federal certification if there is any alteration whatsoever in the in the system, in other words, when you certify, when you test for certification and the certification of a voting system testing lab. The certification they give is a certification of conformance to a specified voting system standard, either 2002 voting system standards VSS from the FEC or 2005 voluntary voting system guidelines. So they're certifying that the voting system conforms to the voting system standards, whatever standard is specified. If you alter the documentation, the software, the hardware, or the configuration in any way, it's supposed to go back for federal certification, it's supposed to go back to the voting system testing lab.

So in other words, the vendor says we're going to change X and then they submit it to the to the voting system testing lab. Now if this was legitimate, what they would do is say we have a change and they would submit it without comment to the voting system testing lab and the testing lab would then assess that change in its potential impact and then they would make a recommendation that either the system needs to be completely re tested, partially retested, or the change is a de minimis change, meaning it is of such little importance that it has no impact on the certification in the system.

When you look through the engineering change orders that have been approved by the EAC, VSTL makes that recommendation to the EAC and then the EAC 100% of the time goes, “Yes, we agree.”

What really happens is the voting system vendors say we're going to change out the motherboard. I'm not kidding, we're going to change out the motherboard. We're going to change out the central processor or we're going to change out, etc. These are the most critical things on the entire computer, right? You can't change. That's like saying I'm going to swap out his legs, it's a minor surgery. We're going to take out his heart in his brain and that's, you know, should be in and out within 20 minutes.

It's ludicrous on a modern computer. You cannot change anything on it other than maybe the key on a keyboard or you know, the placard on the outside.

If you tell me you changed out a system fan, I'm going to want to know whether that system fan is being controlled by software, because if it is and it has a driver change involved, then now you're talking about introducing new software. There's no such thing on a modern computer as a de minimis change.

So this is the dilemma; a double edged sword. They're in a threat environment that is evolving rapidly so the threat environment is severe. The threat environment is pervasive and if you do definition-based malware detection, meaning like we've seen this malware like that's John, I recognize John, he's a thief, that's a malware. I recognize the signature in that malware. In order to recognize the signature, you either have to have made it yourself or you have to have discovered it. Usually, you don't discover it till it's in the wild and being used.

Those are zero days, right? You've on the very first day it's discovered, you may be vulnerable to it because it's unpatched. So the dilemma for these vendors and the computer manufacturers is you have all of these constantly evolving, developing, emerging threats. So, how do they keep up with those threats when the process that they're required to go through is this incompetent? Corrupt voting system testing lab review to determine whether their patch is dumb is going to change anything significant on the voting system and make it more vulnerable, right? The patch itself?

This is something to understand. The patches and updates themselves can be malware or can bear malware. This is what happened with Stuxnet. This is what happened with SolarWinds. Supply chain compromises are prevalent, these are common and so like we talked about the Hynix update for the driver, update for the controller for the data controller on the RAID controller within the EMS server.

Hynix is a South Korean company, but they manufacture in multiple countries including the People’s Republic of China. If somebody working for the People's Liberation Army in China installs malware into the driver update that then Hynix distributes, it gets installed on our voting systems. Right?

That's a deliberate and so they can leave a vulnerability at manufacturing or initially that is its sole purpose is to and it can be a mild vulnerability, right? It can be a not very significant, not severe vulnerability, you know, you just patch it with an annual update or whatever, but its sole purpose may be too cause the update that then is the carrier for the Trojan horse for the really severe vulnerability once you've already trusted that system.

Because those driver updates by and large are just getting rubber stamped by the VSTL at EAC and you can see if you look up that engineering change orders or those on the EAC site you'll see, I don't know,

100 and 5000 and 70 echoes that have been approved by EAC without significant testing, in most cases without any testing.

And the people reviewing them to determine whether there is any risk or threat or alteration to the voting system are literally the same people that couldn't detect the vulnerabilities in the asks that Halderman detected, they couldn't detect the wrong software in the Williamson County system.

I mean, it's Jack Ryan, right? Who says that he has no particular background in cybersecurity. This is not someone who can credibly assess whether or not a software change, whether it's a driver or firmware or BIOS settings or whatever, whether that is going to affect the security configuration and vulnerability of a voting system, let alone the function.

So OK, so now back to the question. Should you ask for the log files? For all of them. They won't have them. It's proof that they don't have the chain of evidence necessary to rely upon the digital records and results from the voting system. Now, we haven't won that assertion in court yet, but we will and we have to keep pressing it. The problems, and there are these barriers and comprehension, like people are a lot, a lot of places. People are still very trusting of their government, not understanding that election officials by and large have no idea what the hell is happening within the machines. And we're afraid to admit it for the most part, so.

Sorry that I felt like a kind of a diatribe.

ASG: No, that was really good in my opinion. And it is complicated. There is education required. I mean, look, all of us here on this call today are researchers, right? And it's still 45 minutes of complex explanations, right? I would bet most people on this call are taking notes right now, so it's very helpful the way that you break it down for us. So as promised, let's come back to Rick's question:

Are there any RF scanners that poll watchers may be able to acquire inexpensive that would reveal any communications of the scanners?

SS: It's possible. Sometimes you run across one of those funny stories, not the Darwin award ones, but the ones where, like, you know, thief leaves wallet in the jewelry store that he broke into. You run into one of those stories where the prosecutions of crimes rely upon the criminals being idiots. Very, very smart criminals are rarely caught, right? The people who are stealing massive amounts of money are by and large in government so it's possible that you will be able to run a sniffer, you know, like a broadband RF monitoring device. It's possible that you'll be able to run that and see evidence, but that's only if the people who are doing it are idiots or so sloppy or arrogant that they didn't bother to use even, you know, secure low detection likelihood protocols.

I if I was doing it, the only thing I would be transmitting would be triggers and brevity codes and those would be transmitted so quickly and you could use like distributed spread spectrum frequency hopped or random hopped you could use signal structures and modulation that would just be below the noise floor. So unless you're a bum, I mean you can try. You can run an RF scanner and look for in particular Bluetooth and Wi-Fi frequencies, but obviously we already know that there are cellular modems on some, so you really, if you wanted any hope of detecting RF usage, illicit RF usage on the machines when they're being used for elections and by the way, "being used for elections" begins at the point, in theory, that they are doing the logic and accuracy test right on ends after they have certified the vote.

So a lot of times people just want to just want to monitor during the period when votes are being cast or tabulated but the software changes or the malware, or the software functions, all of that can be altered and loaded. It can be preloaded, right? Part of it could be loaded, it can be disaggregated software. So there's the idea of software compiling is when you have software that is written in essentially machine language, it's written in a higher order language that makes sense to human beings and it has to be compiled into machine language and other it gets converted into a purely digital, not semantic language that then the machine can execute efficiently.

That compiling in the old days took place in between you writing it and it being run that like, you know, when I was when I was young, I, you know, was working Fortran 77 as part of my degree. I was programming in FORTRAN 77. It was painful. You just prayed that your software you wrote would compile.

Now there's not only compiling that occurs before the software is installed on the voting system, there's also compiling that occurs in real time, so you can have executable software. It is split up so that it doesn't even look like executable software. It might look like 3 different driver files or font files, and you just have one little piece of executable software that recognizes and goes looking for those fragments, assembles them in real time, compiles in real time, executes whatever it's been told to execute whatever instruction is present. Or has been transmitted and then is disassembled again, and the critical piece that doesn't look like a font file or a driver file can be on the hidden partition in removable media.

Rick: But Shawn, the reason I asked the question about the RF is because of the fact that, you know, I understand that they could run some code into these machines, make any changes they want to be real quick in and out and you wouldn't, you'd have to be on top of that machine 24/7 to see that kind of stuff going on. My concern is more towards the ideas. Are the machines transmitting? In other words, are they turning off whatever their Bluetooth or modem, whatever, whatever they've got in these systems or are they turning it off? You know, until it comes such time that they might want to update the code. My question here is not so much to catch the code, I just want to see if there's any wireless communications going on between these devices at all during the course of the day when people are voting because if I can go in I can see that. There's a wireless modem in this thing just by showing looking at the frequency whether it be Bluetooth or Wi-Fi or cellular because there's devices out there go from 1 megahertz to 12 gig. So I'm thinking we could see the code or see at least some transmitting going on at the time. And you know, I'm looking at these cheap RF devices out there you can get for less than $100 and I'm wondering if they're worth trying out. So that's kind of what would govern.

SS: There's a small chance if they've been sloppy or arrogant, there's a small chance that you would catch it. More likely is what you do is have is get catch nothing and then have somebody assert that there was nothing there because you didn't catch it.

So there's you could even have, you could even have the system itself be kind of using a passive like backscatter, if you had a brevity table of codes in the software on the system that—if it receives A1A it does this, if it receives A1B it does this. Those transmissions that would trigger those different configurations or changes. And the system would be so fast, I'm talking about, you know, microseconds, and they would look like noise if these guys are doing it right. So I'm not saying don't do it; I'm saying don't get your hopes up. And if you if you aren't extraordinarily sensitive and you don't know what you're looking for, like if you haven't configured the sniffer or scanner to eliminate noise floor in that

area to be able to see what is the difference between spurious and hidden, there's a low chance that you'll see it.

Rick: Good. Thank you.

SS: You bet.

ASG: Alright, awesome. Anybody else have any questions about how to spot machine vulnerabilities before we move onto the next part?

Elaine: I have a question. This is Elaine from Utah. So I'm working on trying, I have sheriffs that are going to work on investigating our stuff, and what they are trying to do is investigate the voter registration database since we can't have access to it. We're trying to get that looked at. I now have enough sheriffs on board that they're looking at doing a sealed investigation. But I have to get the information to them so they know what they're looking at, so they take it seriously. How can I put some of this information about the log files and things in a way that they can understand it that's quick brief that they could use and understand that this is part of the investigation or an investigative tool.

SS: So we haven't really talked about the voter registrations too much and voter registration systems. In theory, the voter registration systems and the voting systems are discrete and separate; they're not connected. There's nothing in them, right? There are systems like automatic signature verification machines that are reaching through an API or application programming interface, dynamic random access memory; sorry, that's what DRAM means. Sorry, that just popped into my head.

Elaine: In Utah, they just redesigned it so that every part of the logging system in the EMS system is logged in the voter registration database. And I was able to find this out when meeting with our election directors and they would take my data and they could go into the voter registration database in specific parts of the system. We're logged as it would move through systems in the voter registration database, so I was hoping they'd be able to look at some log issues that way, no?

SS: No. I'm shaking my head because that's insane. There's no way to secure it, if you do that. There's no way to secure that. Basically every vulnerability in your voter registration system becomes a vulnerability in your voting system.

Elaine: That's what I'm trying to expose right now.

SS: Only a maniac or somebody extraordinarily corrupt would do that. Um, let me let me back step for a second. A lot of people have heard the term before and I'm sure we'll cover it in one of the sessions, and hopefully we'll get a lot of participation from people up in Washington state because I think they've done more research into the Albert sensors than I have. They have a lot of the data and I want to find out who else has data on it.

So the Albert sensors are in theory a security device that is intrusion detection. Albert sensors are provided by CIS, which is a nonprofit that works in a public private partnership with CISA, and they provide the sensor network that goes into election offices and is monitoring election infrastructure. Now, in theory it's not connected to the voting systems, it's only connected to the voter registration systems, poll pads, things like that. But you're putting it into the environment, like adjacent to the voting system.

And the problem I have with that, other than you know, it's secret; they stick it inside these partnerships in with the private organization like ERIC, and then it shrouds the information from the public. You can't get transparency. And also every one of them that says their nonpartisan, ends up being leftist, but that's a whole other issue.

The Albert systems are using cradle point routers. This is extraordinary if you if you haven't heard cradle point before, look up cradle point the cradle point routers. The significance of them is they're not just Wi-Fi and Bluetooth, they're Internet, meaning they're allowing this sort of unlogged connections. They are allowing the connection of Internet of devices. You know, this is televisions, refrigerators, thermostats, etc.

You could have extremely low power, low bandwidth, very brief communications that are that are accessing external networks through those cradle point routers and you'll have no because that's controlled by CISA and CIS. You won't get access to those log files, and so you won't see how they've been connected. It's extraordinarily dangerous to hear that they've connected in a state deliberately, a voting system and the voter registration system, is a new level of disturbing.

Elaine: So how do you get to that evidence?

SS: We were just talking about this with canvassing earlier. I was talking with Doc Frank about canvassing because we got a lot of people getting more interested in canvassing now. And sometimes they want to go and do verification. You know, they want to do targeted canvassing where they're looking specifically for fraud as opposed to the random sampling where we were looking for anomalies, and then you go investigate to figure out which ones are fraud.

So I think what I need to do, Elaine, is look at as much details as you can find about your voter registration system, about the technical details of it as much as that are available and sometimes it's obscured and you have to find it like through contract documents or things like that and then we can talk about the best way to go after the data that would show that they are not only, you know, I mean the inaccuracy is easy, they're all inaccurate but, and you can prove that with canvassing, but then lack of security is a whole other issue.

And you really have to know the technical details on the system to be able to talk to the security if they've connected it to the voting system, though, that violates the certification of the voting system because it had to have been certified with that external connection present.

Elaine: So what we found is the Davis County clerk, Brian Mackenzie, is one of our top experts. And then you have to remember Ricky Hatch in Weber County. He's the one who started the Isaac or whatever it's called. He's on the CIS board. He's on CISA, on all of them. And so he's like top of the food chain of all this stuff and he's designing all these systems for our state. So one thing when I was talking with the sheriff's is like I said, they were able to take my canvas data and they were trying to prove it wrong on just the voter registration logs from the EMS system and they would tell me about it and I said here's what I have and you can decide what this is and how you investigate it.

So then they started asking me, well, as sheriffs we can subpoena the full information from the voter registration database and that we can use that to then get to the other logs in other systems. So I think this would be very helpful. There's actually kind of a blessing I've been delayed in getting this to them

and present it because it's getting it presented in a way that they can just go out and start working on. It is difficult because they work on other crimes, not this.

SS: Elaine with all you've got, I know you've given some documents, your open record stuff to Amy for the library. And I don't know, it may be Amy, when you're talking about when we have the session on open Records requests, you can talk about what we've already got. But if you have anything, Elaine, specifically about configuration or technical details on the voter registration system that I can look at, I'll start doing research right after this call. I'll spend about maybe 15-20 minutes on it and see what I can find.

I think you can give the sheriffs generic descriptions of the things they should be asking for but there are technical details like in some states you find out they're using they're using that Citrix front end still, I mean that's right that normal company stopped using that at least 10 years ago because it you can't secure them. So I guess I'll try to give you some more explicit language that they can use to ask for specific records and files that would help them correlate. And then the other thing is of course, I don't know if they have cyber investigators or cyber forensic investigators if they don't, then connecting them to somebody competent who can go through that for them and tell them what they're seeing.

Elaine: It's the most vote motivated county. We were actually in a county Commission meeting with all the elected officials and he saw what I presented and how they treated me and he's the one that approached me and they are specifically hiring specific investigators to look at this in their office. So I just need to get enough information to them so that they can do it. It’s in works and it's not my fault that the ball was dropped, if you know what I mean. But I didn't give him enough to go on.

SS: I do. So the good people, I've said this before, the good decent people cannot imagine how immoral and unethical other people can be, and because of that it creates a vulnerability for them. So keep that in mind when you're working with public officials. If they are ethical and/or they are really trying to be public servants for example, and they go looking for or asking for like a forensic examiner, help them.

If they don't know who they can't trust, they will sometimes end up getting people who are not trustworthy. For example, you know, Matt Crane or Ryan Macias keep showing up as experts to evaluate things and these guys have no forensic chops, they don't have the cyber background, their job is to rubber stamp.

So keep that in mind when you're dealing with election officials or county or public officials that you have to help them understand that if they ask the wrong people, they'll get the wrong people, they'll get somebody who will tell them everything.

ASG: Awesome. OK let's move to the last part of the agenda, which is “how do we share what we've learned?” And Laura in South Carolina put together well, she and her team took a clip from our last Research Roundtable when Shawn was talking about specific machine vulnerabilities and they put together this really beautiful, very professional looking video. And Laura, hopefully you got my list of edits from Shawn?

Laura: Yes, I did. I don't know what they use to get the type, but yeah, we'll, we'll make those changes to the punctuation and all that.

ASG: I think they used the transcript, is what it looked like to me. And so that when the transcript comes, it's insane, right? It's like 180 pages so but of just stuff then I clean all that up. Of course I'm on the call, but don't have photographic audio sense, so I don't remember every word that Shawn said, but I want to make sure that what it said was what Shawn said and that it was what he actually meant, so that's why there was so much to clean up.

SS: I really appreciate you guys doing it because I tried to do a video for the Arizona people and the audio was terrible. I think I was using the MIC on this other camera instead of the headset mike.

ASG: Laura once your team has those edits made, if you could send that back and I'll make sure that everybody has access to it. And I know that other teams have put together, you know, I just saw an amazing graphic come out of Washington about the vulnerabilities all throughout the process of the ballot lifecycle kind of thing. And it was really clear and easy to see and really well done. So anything like that that you guys have put together, I would love to have those to add to the Library. And we can also share those types of things in our little Research Roundtable section of the Cause of America website as well, so that people have access to it for each other or to model something similar in your state if it's state specific or whatever.

So why don't we kind of open the discussion here? Of course, you guys can certainly ask questions but also share what you know or maybe there's a specific type of share that you need that someone else might have done in their state. Let's just kind of open the floor and let people jump out. Who would like to go first, either sharing something that you've created or some resources, or requesting something that you need in order to go to the proper people with certain information, or even just to educate the public.

Rick: So my apologies, I had to go onto another call but when in South Carolina when you go to a polling place and you open up your phone and you see an SSID of a wireless connection that you know does not belong to that polling place because it's because it happens to be a church, and oh, by the way, it says SCC on it, which is our South Carolina Elections Commission stamp. We need to be able to educate the public on a how to how to see that and then how to recognize this. You know some vulnerabilities associated with such a connection that we don't necessarily find within their certification when we utilize the information that we get from from EAC. Can you expand upon that? How do we do that? What's the best approach?

SS: Are you asking how do you convey to the public the vulnerabilities associated with having wireless connectivity and devices present and accessible in the vicinity of your voting systems? No jurisdiction in the country is preserving the log files that they shared. End of story. It's not happening there. There's not a single place where they're preserving the log files that they should. Almost nobody is reviewing the log files. They tried to get the log files in the Maricopa audit. They couldn't even get the log files from all the systems, the board of County Supervisors or election board MBTI or whatever would not give them everything. The auditors never even got all the equipment, they never got the ICX devices. If you didn't get the ICX devices and the log files off the ICX devices, which by the way almost universally had wireless networking present on them, then you don't know what happened. You can't know what happened.

So imagine for a second, you've got an election management system server. It doesn't matter the voting system vendor. You've got a server, and then you have a device that is trusted, has a trusted relationship with that server.

It could be wired to the server, hard wired. It could have a wireless connection to the server, like the unofficial election night reporting wireless connections, which is a ludicrous reason to have such a gross vulnerability. Or you could be moving stuff back and forth between them using removable media. Well, if any of those devices has a wireless connection and you aren't monitoring that that computing device with the wireless connection in real time, you don't know if it's been accessed, and you never will. If you even get the log files, you might not know, but nobody is even looking at those log files. Nobody even collects or preserves those log files from the remote devices, they don't do it.

Again, if you haven't gone through those log files to verify that the system hasn't been accessed remotely or operated in an unauthorized manner, or had unauthorized uncertified software running on it, then you have no proof that the election results at the end are even remotely accurate. They don't even have to correlate, right.

So this is where risk limiting audits come in to give the imprimatura, the false sort of sense of confidence like oh, we did a, we did risk limiting audit and therefore we know that the data is correct.

No, you don't. You can't sample that. If you know you're going to do risk limiting audit, you can configure the data in a way that you never sample what would show that the that the results were inaccurate. Right? And that's what I'm afraid is happening, but certainly it's possible and we shouldn't have any confidence in it.

So, so if somebody has wireless, I mean if there's wireless access at all present anywhere near any of the voting systems you have, you have no evidence that the systems have not been connected to wireless.

And I've had this discussion with very high level officials at the National Security Agency about our nuclear Command and control systems. When systems are critical, you don't accept not having proof of their complete security and assurance. On critical systems, you either have proof that they are secure or you can't use them, because if you don't have proof that they're secure, it's not good enough, right?

Just not having evidence that they were corrupted isn't good enough. You need proof that they're secure. That's what it should mean. And This is why Clay Parikh when he was talking about being restricted as the security tester for voting system testing labs for 9 years, they would not let him test the way he knew how to test the way he had tested under Tisma army threat Systems Management Office for critical Defense systems that were facing the same threat as our voting systems and election systems. They wouldn't let him do what he should do because he understood intuitively and when I talked to guys who are really cyber guys, not like me, but really cyber forensic people or cyber, you know, defense people, they understand these things intuitively.

A system is either proven secure or it's not secure.

There's no “hasn't been proven insecure.” So how do you communicate that? It's hard because the general public has no idea how complex and pervasive and serious the threat environment is and what level of capability and capacity our foreign adversaries have developed. I mean a PT1 advanced persistent threat team, not one but 17 in the People's Republic of China compromised networks and systems in 11 different industries in a single month. These guys were out at first, I don't know, seven years. And in one month they got to that many different industries that now each one of those industries might branch into, you know, 50 different companies or might get you into state governments or federal government agencies.

People know about SolarWinds. They don't understand SolarWinds was a drop in the bucket. And it's, it's a result of a massive threat that is arrayed against our critical infrastructure. Public officials are never going to be able to defend these systems against them. They don't have the capacity, they don't have the technical proficiency, and they don't have the expertise necessary. They don't even understand the threat they're in. They're like a newborn baby that crawled into an MMA cage match.

Rick: I mean that's what they're telling us in South Carolina. They're saying, well, these are Verizon hotspots and it's an intranet and it's secure because we have it covered. It's just this hotspot that's ours, and so it's totally secure.

No, I've said it and I mean it and you can look it up the security technical implementation guides for the Department of Defense if you're going to bring a computing device of any kind into a secured area. You can't use administrative controls, you know, like settings, BIOS settings or anything to disable wireless connectivity in those devices. You have to physically do it. You literally go in with wire cutters and snip the portion of the board that is connected to the component or you take a drill to the actual like if there was a Telit chip that LE910 cellular modem on a motherboard of a device that you were going to bring into a secure area, you would take a drill to it before you ever brought it into the area and you'd literally just drill it out, till there was no more device inside it. That's what you have to do.

And this is with people who, I mean the Department of Defense spends I think at last point I added up $11 billion a year on cyber security and cyber defense, right? $11 billion. And that's what they have to do because administrative controls aren't good enough with their people. And I've seen it. I mean, I I've seen, I've seen exploitation, active exploitation happening on Department of Defense Networks that were actively defended. In fact, I've directed it for weapons systems testing.

Rick: Can you give an unclassified Supernet example?

SS: Uhm, Supernet, I will because it's been fixed now. I will tell you we were testing space based infrared system, ground system. This is our ballistic missile warning network, right? These are infrared detection satellites that first detect missile launches worldwide. So the thing that gives us warning to shelter, the thing that provides the threat that we will launch in retaliation, that is ballistic missile warning satellites, cyberspace-based infrared system. We were doing operational testing on the ground system upgrades and—again, this has been fixed now and that's why I can say it.

The very first thing our Red team did was penetrate and compromise the console that the cyber defender was using and monitoring the intrusion detection and protection system so that he couldn't see what else was happening on the system and he had no idea. That's an actively defended system with cyber defenses that were designed to protect that system and a guy who was trained, monitoring it 24/7. And the red team wasn't even emulating an advanced threat, they were emulating what I would consider a mid-level threat when they did that.

So if your systems—and cyber pros know this, people who deal on national security understand this again intuitively, the same way that you understand you can go to the grocery store and get milk because you've done it before—these guys understand that a system that is not actively defended with intrusion protection and detection systems that are tuned to, that system they're protecting cannot be defended. It's compromised, and you have to assume it's compromised, and even that system will be compromised.

Yeah, they do that layered defense, but they focus on trying to protect the mission and preserve the mission and the data integrity, not on trying to keep attackers out, because the systems are too complex.

You know the smaller you make the attack surface, meaning the more the fewer places and adversary has the opportunity to affect or insert into a system, the better chance you have to protect it on these caught systems. You know, Dell computers, HP computers, wireless connections, you know, moving portable media blackboard, your attack surface is massive. You have a voting system in a county with 70 different computers, 100 different computers, every single one of them has potentially you know 102 hundred different attack vectors. That's after manufacturing their vectors and we're not checking that, AT ALL.

Our voting system testing labs aren't checking that at all. Nobody is checking that at all. This is why I say it's not possible. These systems cannot be secured.

It's the idea of trying to convey the level of the threat and the risk and how vulnerable they are and how likely that they're compromised to public officials is the hard part, because again, many of them are decent moral people and they don't understand the threat environment.

ASG: Shawn, when you refer to “COTS” systems, how is that spelled, is that an acronym? What does that stand for?

SS: COTS is commercial off the shelf. It's really a misnomer for coding systems. So for example, like Dominion uses HP computers, and Dell. Hart Intercivic and DS both use Dell computers as part of their standards, so when they when they get those computers, they don't go to a Best Buy off the shelf. If they did, that would be commercial off the shelf (COTS). What they actually do is order them explicitly configured.

That's not really COTS, that's really boutique or bespoke systems that are configured. That's why when you when you see like the Dominion systems, and they've got, you know, 36 wireless networking devices in the voting system suite for account, it's their fault, right? They knew they were doing it, they ordered them. That way you could order a workstation that didn't have iDRAC in it. You don't have to get the server with the iDRAC in it so the fact that they order it with iDRAC, the integrated Dell remote access controller, is deeply, deeply suspicious and troubling.

But our public officials don't understand that. So those systems, technically speaking, are not COTS if they have ordered them specifically for a specific customer and ordered and specified the configuration because the other part of that is the manufacturer of those systems knows who they're making them for, right?

So let's say I was a thief and I wanted to be able to get into a bank and I operated a company that did lock changes and the bank ordered a lock change. That's it. It's done. I'm in. I have the key because I'd put the lock in. Dell doesn't make their own computers. They're made under contract in China for the most part, assembled for the most part in China of Chinese made components, right? All of their laptops, all of Dell's and HP laptops were made from 2013 through 2020 in China in a couple different locations, mostly by Western, which is a Taiwanese company. They're a fabless semiconductor company, so they don't operate their own factories, they just do design and quality work.

Well, who's there all the time? Liberation Army representative. So they're building the computers and they know they're building them for Dominion or for ES&S. So if they want into the voting system, they just build it in. Right? They're in control of the hardware, too.

ASG: Alright, cool. Does anybody else have any last question for Shawn.

Elaine: So it's my understanding Shawn that's that at times that that the election manufacturing organizations will tell people that or tell states that they can utilize different functionality that's not necessarily or hasn't been necessarily certified within its testing so uh, being outside the configuration management of that, that would mean that that system is no longer certified if they use that outside application.

SS: Yes, I would agree with that. There's some Gray area like their machine configuration files that should be present on some of the devices that configure them in accordance with their certification, and those are supposed to be controlled as part of the certification. So if you change those settings, it should invalidate the certification from some of the software you know if you for sure if you change executable code or drivers, it should invalidate the certification. The system should be re certified. That's 100% true whenI talked about the federal before.

You have to really look at the statutes in your own state. Sometimes the state statutes are extraordinarily explicit. And then, you know, the election officials, usually the secretary states, just violate those anyway. I've lost count of how many violations right we had. We've got multiple states, for example where they had executable software loaded on voting systems that was not part of their certification, and they continue to use them. It's totally illegal, right? It's totally illegal.

You would presume a law enforcement body, given that information, would do something about it. None of them has done it yet and I think this is part of what Elaine is talking about. You know if you if you have constitutional sheriff's and you can explain to them what has occurred. They should be arresting people. They should be arresting secretaries of state. That should be happening.

ASG: I think we might have time for one more quick question, anybody? If not, I have one through e-mail from Burl. Shawn, Burl said, “Any information today on connect within S&S would be helpful.” I don't know if that's something you can cover in a couple of minutes?

SS: First of all you have to look at the company and everything they're involved in. They are not just involved in sort of management of election workers. So what True the Vote—and I'd have to go back and look at the details, but what True the Vote exposed was that Konnech was keeping databases of all of these election workers and election location and system information on databases that were maintained in the People's Republic of China. Now that on its face is deeply suspicious because there's lots of places to keep data. You don't have to do it in China now you could maybe make an argument for a stupid, if not innocent explanation or rationale that you know, he had business connections and so that was the cheapest thing for him, got a good deal, whatever doesn't really matter.

We don't want any of our election information kept overseas or controlled overseas. If it's kept overseas, it's controlled overseas, right? There's no such thing as private industry in China. It doesn't exist. If the government wants access, they have it. They control the entire nationwide network, so all data going in and out is exposed to them. And if it was encrypted, you know in transit, they may have access to that and probably do because I don't think they'll allow data that they don't have access to and

if it wasn't in just encrypted in transit, they probably have the keys to that. They probably have access to the hardware, so that's the gist of the Konnech issue.

From that information, Konnech is involved in election management, system management and maintenance. You have to look up their site.

So all I'd say is that you know the lying media had taken their shot at True the Vote with the Konnech data, in slandering them and gleefully celebrating the lawsuit brought against them against True the Vote in Texas about what they looked at, but I'll just say life comes at you pretty fast. So all these publications that talked about how it was ridiculous and it was, you know, racist and whatever else, well, I guess I also have no confidence that Eugene Yu, who has been arrested, means there's going to be an adequate investigation.

If I was guessing, I would guess there'll be a cover-up, in the same way that there has been a cover up of almost every other compromise and vulnerability that the FBI has been involved investigating. I mean, now we know, right? We know now from the testimony of the former DOJ employee that Bill Barr, former Attorney General, lied when he said that they had investigated and found nothing. As it turns out, what they did was not investigate and find nothing. Surprise, surprise.

ASG: All right. Well, thank you for that, we are now out of time. Thank you for being here. Look for an e-mail by the end of the week that has the replay link and the transcript and we'll see you guys back here in two weeks on October 19th. Have a great week, everybody.

SS: Thanks everybody. Take care.