Cause of America – Research Roundtable
January 25, 2023 TRANSCRIPT: ePollbooks Feat. Col. Shawn Smith

ASG: Let me go ahead and just welcome everybody to our research roundtable. Today is Wednesday, January 25th, 2023. And we have Colonel Shawn Smith here who is going to continue to educate us. Last time we talked about Runbeck and signature verification. So we're going to continue that conversation and also talk a little bit about, I think Shawn, you were also going to talk about Epoll books today, electronic poll books and then next meeting which will be Wednesday, February 8th, we're going to have DataJeff out to share with us a presentation. He actually sent me a slide recently of a presentation that he did. He said, "I think this one slide would be really good for the library." Well, he sent the whole presentation, so you all know me. I read the whole presentation and I said, Jeff, this is really good. Would you like to come give this presentation to the Research Roundtable? And he said yes, so. So we have him at the next meeting on February 8th and then at the end of today's meeting, I want to share something with you guys. Shawn and I have been working on a special project and I have kind of like a little one-minute teaser that I can show you. I mean, assuming that I could figure out how to share my screen to show a one-minute video, but we'll do that at the end after we've covered all the Q&A because I just wanted you guys to know about it first because it's pretty cool. And I think it's something that's going to be really helpful for everybody that's trying to help educate other people in their area, whether they're elected officials or, you know, just regular people. So, with that housekeeping out of the way, take it away, Shawn.

SS: Good morning, everybody. Let me just take a look and see who we've got here. OK, usual suspects. So, I'm hoping this can be a little bit more of a discussion, but I'll be happy to talk about a few of the things. There's some thought, some kind of provocative points I want to make about Runbeck and signature verification, how this is being done and how it should be done, and what's ridiculous and absurd and unethical about it. OK. So I want to talk first about operation bullpen. Does anybody know what operation bullpen is? Does that sound familiar to anybody just off the top of their head?

(VARIOUS): No. Haven't heard it. We haven't either.

SS: So the FBI has a pretty advanced forensics lab. Law enforcement agencies and jurisdictions across the United States rely upon FBI forensics. The oldest subsidiary or compartment lab in the FBI's forensics lab is "questioned document examination," which is the name of the domain or field of scientific analysis. Presumably so it should be scientific. It has scientific approaches, they've developed methodologies, they've developed instruments, and they should be applied scientifically and methodically on the basis of all evidence, which is what forensic means. So, the FBI's oldest compartment or oldest segment of its crime lab or forensics lab is the questioned document examination, which was established in 1932. Operation bullpen was the second or third in an ongoing FBI operation targeting fraudulent and forged sports memorabilia in the United States. I want to say it was from like 1996 or 7 or 8 I think until 2006. The FBI conducted this massive investigation, you can look this up. Conducted a massive investigation

into fraudulent signatures on sports memorabilia. So they literally, at the FBI museum, they have this huge display on these baseballs that they detected forged signatures by people who were selling these sports memorabilia.

Now I'm not against sports memorabilia, I'm not against collectors of sports memorabilia. But what I am against is the massive, the massive allocation of FBI resources to an obviously niche problem. In the United States, not just in the US, in the US economy, it's not—I mean, I don't care what you do with baseballs unless you start shooting them at our elected officials out of cannons, it's not going to be a national security issue or unless you fly billions of baseballs over U.S. cities and drop them. And yet, our Federal Bureau of Investigation had the assets and the wherewithal and the intent and pursued this multi-year investigation into fraudulent signatures, forged signatures on sports memorabilia. And the reason I want to bring this up is because our law enforcement at the federal level and then lots of state as well that have crime labs, they know exactly how a serious person and organization would go about verifying the authenticity of a signature. If you have an individual who is a "questioned document examiner" as their profession, they are likely to have professional certification standards. They're likely to have an undergraduate at least four-year degree in one of the physical sciences. They're likely to have both education and training a period of at least six months where they were under the supervision and mentorship of an experienced questioned document examiner in the profession and then the professional certification, all to ensure that they meet the minimum standards for someone who's going to give their professional opinion about question documents. They also don't just go around looking at signatures with the naked eye. That would be absurd, if you brought a questioned document examiner in to verify a signature's authenticity or to certify its inauthenticity in a court of law.

I've said repeatedly that a serious judge would probably sanction an attorney and the attorneys tell me that's not true, although I think if it was a conservative attorney, they'd be sanctioned. But anyway, that's another story. But if you tried to bring someone into a court of law as an expert to certify the authenticity of a signature on the basis of examination, and they were not a certified professional questioned document examiner and had not used the instruments available, including electrostatic detection devices which they use to look for indentations because you could have something written over the top or printed over the top of an actual signature, or you could have no actual signature and just printing over the top and an electrostatic detection array or ESDA would actually show you that there was no indentation in the paper.

So if you go to sign your ballot envelope affidavit on a mail in ballot and you sign it with an ink pen or even a pencil or any writing instrument, it is going to leave an indentation in the paper. It has to. There's no way. Even with a felt pen, there's going to be some tearing of the fibers. But, or part of what Jovan Pulitzer was referring to by, I don't know why he uses this term. I think he invented this term and it's sort of like a, you know, copywriting approach, but he calls them "kinematic artifacts." So you can't crease real paper, a dollar bill, which is largely cloth fibers or a ballot paper or the fold, the flap on an envelope. You can't crease them without leaving an artifact of that physical, mechanical action. And you can't write on them with a

ballpoint. It will leave a dent with a felt tip pen if you write very lightly. Even if you write extraordinarily lightly, if it's heavy enough to leave marks, it will necessarily tear fibers along the path.

And so the questioned document examiners will use instruments like an ESDA. They'll also use like Foster Freeman, wait, Freeman, Foster. Think it's Foster and Freeman. They will use their light tables. So they have various devices. Some of them are very fast. Some of them are very precise. They can change the angles and magnification and the spectral band of light that they're putting on to a questioned document. And they can determine from that whether it's an original signature or they can identify a spectrographic signature for inks and they can then match that in a catalog and the FBI contains a catalogue of those inks. If you're using those instruments, I want to say are 17 different criteria that they can compare to determine if handwriting, including a signature, is authentic. And that's just for handwriting, not for signatures. Then there is this entire sort of technical approach to comparing the dimensions and the spatial relationships of different strokes and the signature. Now, all this to get to us.

The point is, if you wanted to verify that signatures from mail in ballots were authentic, or for mail in voter registration or anything else, if you wanted to verify they were authentic and you were serious about making sure that no inauthentic signatures were accepted and that authentic signatures were accepted, this is what you would do. You would use these kinds of instruments and these kinds of professionals. Now there is a company that does it called Paris Script. Their technology is used by Runbeck which I believe is the largest vendor of automatic signature verification machines. So on the one hand in the process for mail in ballots you have judges who are doing signature verification. Now, I'm not saying this in a denigrating manner. I don't intend it to be denigrating, but I don't care. You know, if you have two hours or 20 hours of training, these people are not qualified to be determining whether they're looking at the authentic signature of a voter. Not only are they not qualified to be making that determination, just prima facia, they don't have the technical ability, or experience, or training. And the training they do have is from like, secretaries of state and their staff, which are largely technically illiterate and incompetent. And the evidence of that is that they are promulgating these pamphlets and this training to use amateurs for signature verification. But anyway.

So even if they were experts, they don't have instruments that any professional in the questioned document examination field would be using or they would be drummed out of the field. If you were an expert QDE and you went into a court and said yeah I've looked at that signature. Like if you go get a speeding ticket and they have the officer coming up here in the court to testify about your speeding ticket. They're going to talk about their radar gun how they calibrated their radar gun the technology used in the radar gun. Imagine a questioned document examiner in a court case up on the stand. OK, so you examined this? Yes. It's authentic. Yes. What did you use to examine it? Well, I've got eyes. Then it'd be the end of the case. But this is exactly what we're doing.

So the judges not only are not professionals, they're trained by non-professionals. And it's all part of this sort of propaganda about this being an acceptable tolerance, tolerable sufficient,

adequate means of signature verification for one of the most important functions performed by our government, if not the most important function. So the entirety of our form of government rests upon its credibility and authority granted through delegated power, conveyed as a result of the will of people through their elections and this vote question of whether this is an authentic vote from the authentic voter—that is the fulcrum upon which the question of the authenticity of election results hinges! Not just that, but also the voter roll accuracy and tabulation. Clearly, if you accept votes, it is a very serious undertaking. But we don't undertake it seriously.

So you have on the one hand election judges with no instruments, poor training from people who are technically illiterate. Then they're looking at signatures in a database, typically a voter registration system, which has accumulated this pile of signatures. Like in Colorado, I have had judges who served as judges in elections confirmed to me. They have seen at least as many as 13 different signatures for an individual that they were trying to compare signatures for. But then some of those signatures are also collected on these low-resolution electronic tablets. And then the signature databases, which are part of the voter registration systems, are centralized. Systems are neither secure nor accurate, and the proof of their inaccuracy is in canvassing at a minimum as well as instances where their active voters exceed the population of their state. That seems hard to do authentically. I do this with my hand, how many fingers am I holding up, right? If it's a blurry image, you have such a poor basis for comparison that it really becomes arbitrary as to whether the election judges are going to accept or not accept. It's not about whether it really conforms to the signature of the purported voter that's with the election judges now, the automatic signature verification machines, and we've talked about this a little bit before.

Runbeck I believe is the largest vendor of automatic signature verification machines used in elections in the United States. Their system, the Agilis system, is also a sorter of ballot envelopes, so it's checking, it's scanning the IMB, the Intelligent Mail Barcodes where they have those verifying the IMB information in the voter registration database. Because the system has live connections to outside networks, purportedly to Runbeck the vendor, which seems completely unethical and unnecessary and intolerable. But that's what they do as well as I believe, based on what they submitted in RFP request for proposals to state secretaries of state, that we're asking for the capabilities. Runbeck's documentation stated that they needed an API or application programming interface from their automatic signature verification machines into the state's voter registration information. So if I get an envelope in the Agilis machine that's fed in, it comes up, it scans that intelligent mail barcode, it looks at the information. Now it's looking up that IMB information that correlates to a specific voter in the state's voter registration database. And it's also looking at the back in some cases where the signature verification affidavit of the purported voter is, and it is checking that signature on the affidavit on the envelope to the signature in the database. That's the theory, but it's scanning that signature and correlating it to the voter that that correlates from that intelligent mail barcode or the address information that's on it, so it has the name of the voter and the signature and access to the database.

So with no certification, no testing, no oversight, and no auditing of the auto, I'm probably doing it the wrong way. This is the American way. I think that was the European way. So with none of those things for automatic signature verification machines, we have no assurance that the automatic signature verification machine is not building up a database of any signatures it did not already have, or injecting those into the voter registration system. No one is supervising the system. OK, so there's one problem.

Another problem is that they're using this software from Paris Script. Which is a Colorado company for the signature matching. The public has no insight into the criteria or configuration for that software. So in theory, this is being used by banks for signature verification. You know a check is typically a wet signature. A bank typically has a wet signature. You're comparing apples to apples. Now we're talking about comparison of digitally captured and signatures of unknown providence in centralized databases to the signature on the ballot envelope by this machine, with criteria that the public has no insight into, that election officials can modify, and if that signature verification machine has a live connection to the outside, whoever is connected to it could modify the configuration. So imagine now you have two precincts. Let's say a county in the United States has just two precincts and all the all the left-leaning voters or the majority of left-leaning voters are in 1 precinct and the majority of right-leaning voters are in the other precinct. If you wanted to harm the left-leaning voters, all you have to do is when you have a ballot from that precinct come in, and you can verify that with the information on the outside of the ballot envelope, you apply one configuration setting or standard for signature verification to that ballot from that precinct, because it's from that precinct, or from that voter, or from that voter affiliation, all of that information is available in the information that the that the company and the machine have access to. So the idea that we are getting equal treatment of voters is completely without warrant or evidence. The idea that we're actually getting verification of signatures to some scientific and technical standard is completely without warrant or evidence. No one is verifying it, no one has specified it. It's basically entirely on the hearsay and assertions of the company itself. So let me pause there for a second and see what kind of questions people have about the topic or if anybody's got comments or examples of things that they'd like to bring up and talk about or if Amy if you've got a different direction you want to go.

ASG: No, I think this is great, Shawn. George from Illinois did post in the chat and he said in 2020 Wisconsin found 40,000 driver's ID numbers in the voter rolls. Did someone upload the registration info along with a signature file? And then he says I heard that there was a possibility that the signature verification could take the scanned signature and install it into the files and verify that the ballot returned machines which what is in the file? Return matches what is in the file.

SS: Yes. 100% I don't know if this happened, I know it's entirely possible. How did signatures get into the database to begin with, into the centralized statewide voter registration system? Nobody knows. In a lot of states, they're using software and software configurations for the voter registration systems that are like amnesiacs. They can't tell you what the database previously showed. They can't tell you the provenance of each data element in the database.

There are collisions and audit trail failures in the databases. So if you connect a machine to that database, that machine can potentially change. And a lot of them are older; they use older technology. I've looked up a couple states' hardware and software configurations that I could find from their documents, from proposal and technical evaluation documents for their voter registration systems. I've looked at Avid in Arizona. I've looked at the system being used, you know, with votes in Wisconsin. I've used it. Looked at Colorado and Wyoming and a couple other states. There are thousands upon thousands of published common vulnerabilities and exploits CVE's, in other words, you know, cyber vulnerabilities in the software and hardware. A lot of them are older systems from mid 2000s to late 2000s. They weren't using particularly advanced technology at the time. The cyber threat has evolved exponentially and a lot of times the people who built the systems are not particularly trustworthy to begin with. Then you have the administrators, then you have the expansion of Internet access and voting and voter registration. Like you have public Internet portals to these systems. So these systems which were not particularly well defended architecturally to begin with, have been since connected to the public Internet, and then poorly monitored and poorly defended because they're doing the best they can do. It's like trying to make a tank out of a Yugo, there's only so much you can do to it, and it's a certain point even the most skilled people couldn't make it secure. But they don't have the most secure people. The most secure people are working in Department of Defense and Defense industry and some of the high-end tech companies and they can't defend their purpose built architecturally secure systems, right?

If you look at cyber security as a domain, the people who are really fluent understand perfectly you cannot defend any system indefinitely, especially with an attack surface. It's exposed to public Internet, right? That's like having a bulletproof vest on and saying shoot at it all you want. The first bullet won't penetrate it. The second bullet won't penetrate unless it's like 50 caliber. The third bullet won't penetrate it. But even a 9 millimeter after the fourth or fifth round, you have the ceramic plates are going to give, they're going to fracture and they're going to start to separate and at a certain point you're going to get penetration. It's the same for cyber systems. If you expose them to the threat, they are going to be compromised. Now what did they do in in a specific case? I don't have the evidence of exactly who did it because they don't audit them. It's not public if they do audit them. You know, the last survey I read about election officials said that about 50% of them were employing the most basic cyber hygiene. These are not experts. They're not of the caliber that private industry or national security are using, which cannot defend their systems, right? We've seen that. And so, what can be done in those systems? Anything, anything could be done. This is why I say you cannot, you can't clean the voter rolls in a centralized statewide voter registration system because in a millisecond you can swap out every single name and any piece of information, including signatures in that in that database. And it's entirely possible that automatic signature verification machines, whether it's from the company itself or from some malevolent or malicious actor, whether it's an insider or an outsider, have been configured in a way that they are populating voter registration systems with the information off the envelopes, instead of comparing the envelopes to the voter registration system, that information could also be coming out of the IMB TR data at the post office. The informed view mail, track and report data, which is scanning election related mail front and back, including signatures. So if you have ballot envelopes again

and it doesn't have a security envelope when it's being returned and the signature is visible outside the envelope, then that's being scanned at the post office. And that data is being sent to the public officials that own those IMB TR accounts as well as any proxies they've designated like ballot tracking applications, like Ballottrax, which was a subsidiary of I3 logics and I've talked about this before but that you know, I I think they were I3 logic, which was like a medical and healthcare data company, started I3 ballot I think is what they called it and this was around 2013, 2014. And the guy who came over to lead the transition from I3 ballot to Ballottrax which now so many states are using to send voters information about their ballot status on the basis of information coming out of the centralized voter registration systems and IMB TR data. That guy who came over to head that project under I3 logics to transition to Ballottrax David Moreno, who was one of the Smartmatic guys on the Dominion Voting Systems uniform voting system proposal team in Colorado.

So yeah, could they have done that to the database in Wisconsin? 100% and nobody's watching it and nobody's defending it and the public doesn't have access to it. And even if we did, the number of cyber professionals we would need to look just at the voter registration systems in 50 states outstrips our available workforce with that kind of skill set. That was a very short answer, I apologize. But yeah, yes, it's all possible. There's nothing you can't do to a data system if you have access to it.

ASG: And George also commented in Illinois, the counties do not give the signatures to the state. They keep them locally on the epoll book systems which they don't. You just co--OK, go ahead. I was gonna say you just covered how not secure the epoll books are but go ahead.

SS: Yeah, yeah, so. The Department of Defense operates networks and computer systems at a lot of different classification levels from unclassified networks all the way up through special access program and highly compartmented systems. So you have unclassified confidential networks, usually those are just held on secret networks. They call it SIPRnet Secure Internet Protocol Router Network. Then you have Nipper. That’s non secure SIPRnet, then you have top secret SI networks, multiple different top secret networks, some for command and control, some for intelligence, some for general purpose use administration, etc. Then you have compartmented systems and with all of these networks and systems you have all sorts of needs for comparison or for data exchanges. Like you may have a global hawk UAV unmanned aerial vehicle that's collecting surveillance from overhead in a foreign theater. And you want to get that data and the analysis of that data, which is collected at the secret level depending on what it's observing, back into a U.S. intelligence network and then accessible to analysts and different units and locations around the world. That data may move between a secret network and a top secret network or a top secret SI Network. So you have this need for one way data flows. You want to move data from one to the other without the ability for that lower classification network to get to the top secret data or configurations on the top secret network. So we were using I can't name, I don't think I can name the tool. We were using a piece of technology that was designed to only allow one-way connections. And a friend of mine is the guy who demonstrated after we had purchased probably $400 million worth of these, and we're using

them all over the world. A friend of mine who's one of the autists that I talk about, demonstrated how the system could be hacked to facilitate 2-way interaction.

What I'm saying is that if you have an ePollbook connected to a centralized database, and if it's connected to multiple databases, the people who are responsible for these systems cannot secure those connections, so any connection must be assumed to be a two-way connection. Even if it is intended not to be and designed not to be, the technology does not exist for that one-way connection in most cases. And the people who are responsible for these hardware and networks do not have the capability to ensure they don't have the skill set and, in some cases, don't have the authority to ensure that those systems are not connected. And you know, a lot of times the ePollbooks are using wireless networks within the counties or the precincts or whatever, and those wireless networks are not secured to the extent that they would need to be to avoid that kind of data spillage or unauthorized access.

ASG: All right. I see Linda Rantz has a hand up. Go ahead, Linda.

LINDA: OK, thanks. Hey, Shawn. OK. So quick question. Uh, the some of the counties, because they're rural, don't have ePollbooks and of course they update them back at the main center. And I have a feeling that's going to be the answer. But their point is they don't let them. They don't even have Internet connection at the polling places where they're at. Does that help at all or does it just not even matter?

SS: It doesn't help at all. So just to kind of frame everybody's understanding of the threat. The People's Republic of China's Ministry of State Security, the MSS, their advanced persistent threat teams, they have built a massive architecture. This is just one country and one approach, a massive architecture for cyber threat. They are scanning almost every Internet address in the world every day. They are looking constantly for new IP addresses. If it pops up in a routing table, if they see traffic for it, they scan it. They are hitting every single address. They say they hit Department of Defense, National security, government, all of those addresses multiple times a day. They're looking for vulnerabilities, misconfigurations. They're looking for any sign of equipment on the other side if they don't already know it. So they understand what susceptibility there might be to exploitation if you were targeting electronic voter registration systems, including ePollbooks, you would compile device address and location information. You would be scanning the IP address ranges for those devices every way that you could. And the moment one of them popped up, your resources would turn on to it, like the eye of Sauron. And in that microsecond or millisecond of connection, they might spoof DNS routing and pretend to be the authentic site.

Or you could have a situation like up in Wisconsin where they found voting systems that were connecting first to a non-government network supposedly enroute to the virtual private network connection back to the election management system server. So not being connected all the time is no protection. The only protection from that kind of vulnerabilities and attacks is to never be connected. If it is open to any public Internet or wireless network at any time you know it's going to be vulnerable and I'll give you what it looks like the other way. So we used to

have in certain environments in the government we have what we called Hello Phones. So we would have what are called secure telephone equipment or a secure telephone unit. So we could make secure phone calls and discuss classified information. This is before VoIP phones or secure computer-based phones and so you would have a phone line, you would dial that phone line and if the if the office on the other end was a sensitive office and you were a sensitive office, you called those lines Hello lines because you would literally you would pick up the phone and you would say hello and that's the only thing you would say. Nobody would ever say anything but hello and then whoever had called would initiate the secure call and the two phones would sync up. That would be difficult to hack. But nobody is doing that. They're doing handshakes. They're doing all sorts of header information in the packets. Even in the VPN you can encode information into headers, that's free tax, or that's executable that can change routing. And again, if you're an adversary and you're watching for a connection or traffic from a specific IP device like your phone, your phone probably, do you know an IP when you're connected to a network? If you're watching for that and you see it come up, they turn their resources on it so there's not a time that you can connect it and be safe. If it's targeted, it is vulnerable, and if it's connected it will be exploited.

ASG: All right. Linda, did you have anything else or did that answer your question?

LINDA: Thank you. Thanks.

SS: You have to imagine all our computing devices are like a person hiding in a room from a sniper. And the sniper is just sitting, looking through the scope at the window into the room, waiting for the person to appear in the window. If the person doesn't appear in the window, the sniper might try to shoot through the walls. But if the person appears in the window, there's a headshot coming. That is what the cyber threat is like 24 hours a day, seven days a week. This never ends. We are at cyber war for the rest of the time that we have and use computers.

LINDA: Wow. OK, that's exciting.

SS: And the weird part for me is that, because I wasn't looking at any of this stuff before in the Department of Defense and the intel communities I was part of and came out of, this has been well understood for at least 10 years. We were talking about it 20 years ago in some communities. But within 10 years everybody in cyber and Department of Defense understands this--people who are actually cyber they understand there is no longer peacetime in cyber. Cyber is at war forever until there are no more computers. You know from a gamma ray burst or electrostatic discharge, a big solar flare or something.

ASG: Wow. All right. Anybody else have a question for Shawn? Is I don't see any more hands up, but you guys can unmute and just jump out. Or if Shawn has other stuff he'd like to talk about.

SS: I see there are a bunch of comments in there. I don't know, Amy, if there's anything we need to address, but—

ASG: So George did add: EAC and Illinois SBE have no certification standards for epoll books. And then people had questions about how to access the chat.

SS: So yeah, there are a few states with certification standards. There's no federal standard for ePollbooks. They have some recommended guidelines. It's all nonsense, right? It's happy talk. Like when you have a guy like Ryan Macias come to court and profess to be an expert and talk about layered defense, without understanding. And it's funny because I've been accused of this by people on social media, which is fine, people can accuse other people or whatever, but guys like Macias who was responsible for certification and testing program within EAC for a few months. He was the acting guy there for a few months. I think he succeeded Brian. Can't think of Brian's last name, Hancock maybe? Maybe he's the Commissioner. There was another guy there named Brian and then Lovato followed him. Lovato of course came out of Colorado. He was the risk limiting audit kind of project lead. So these guys are not technical, they do not have cyber proficiency or skills.

In a lot of cases, what we're seeing is that the ePollbooks are being connected over FirstNet. So FirstNet is this AT&T, DHS public private partnership that was supposed to be for first responder like emergency fire, police, etc. communications, so that they would have their own dedicated cellular bandwidth and not get overwhelmed by all the traffic in a disaster like imagine, you know, a mass casualty scenario or a disaster or natural disaster where everybody's lighting up all the cellular networks. They get overwhelmed and then you know, emergency medical and service providers can't get through. So they have dedicated frequency bands within the United States that are allocated to FirstNet. AT&T manages that. This was the data center in Nashville. AT&T manages that well. A lot of epollbooks are now being connected via Cradle Point, Internet of Things routers to FirstNet. So they're using. This compartmented segregated cellular bandwidth, it's being kept from the public. The public doesn't see who's on it, the public doesn't see where that data goes. Those same internal county networks, supposedly not the voting systems themselves, but other election related networks within local jurisdictions are being monitored by Albert Sensors, which was like a follow on or extension the Einstein program under again the public private partnership of CIS with DHS. CISA and CIS partnered on this, they provide it at low or no cost, sometimes a subscription cost from CIS to the governments. They're providing these monitoring where supposedly CIS on behalf of this partnership for the federal government or CISA is doing intrusion detection for those election networks. Well, what they did for from my perspective, what they did was provide a single centralized access point to election networks throughout the United States. So the moment you connect all of them now if there's any vulnerability at CIS and of course they will tell you oh there's no vulnerability here we're perfect. That's what CISA would tell you too.

And for people haven't heard me say it before, CISA’s own networks were compromised for at least ten months without their knowledge by the SolarWind supply chain hack. They had no idea until Mandiant fire eye told them that their systems were compromised at Mandiant and want the signatures. Then CISA found them. Then CISA started getting advisories out to the rest of the federal government and national security community. CISA are the same people that

wouldn't publish the ISA or the industrial Control System advisory on the Dominion vulnerabilities until almost a year after Halderman found them and stated other versions of this voting system were not, were not able to be, tested. In other words, we didn't test anything else. We don't know what else is vulnerable. CISA are the same people with the AC who then allowed those same voting systems that were affected by the ICS a potentially compromised, definitely vulnerable to be used in US elections that whole one year. And subsequent. So there were recommended actions. Nobody forced anybody to take those actions. Almost no state has taken any of the actions. A few have taken some, none have taken all the actions that were recommended. So keep in mind when they say, oh, we're protecting, we've got Albert sensors, all they did was provide a conduit for malicious actors to get to those election systems and if the ePollbooks are connected at the county level or on wireless networks or at any point connected to centralized systems or to public Internet or to the county systems, that's it! They've been compromised because again, the public officials do not have the skill set or the capacity or resources to defend or protect those systems. They don't even know what they're looking at. They're more like the average iPhone user. Do you think any one of them has even the slightest idea what services, apps or connections are occurring on, for example, like Knowink tablets that they're using? They don't. They don't even understand the difference between software and firmware. They don't know what software is running.

So these statements, the happy talk narrative, vapid assurances from public officials that the systems are secure, are total and complete rubbish. They have no capacity to even know. They're just regurgitating what they've been told, and what they've been told is not plausible or credible. At least that's my perspective on it as somebody who, you know, dealt with threats.

ASG: Right. Thanks, Shawn. Erica said: I was surprised to learn that our EMS is considered an ePollbook as well as other things. Does that sound accurate? We have AB Pro EMS.

SS: Hmm. Yeah, that's insane.

ASG: So I think that's Erica from Washington. So she's talking about Washington state.

SS: Yeah, AB Pro. I'm trying to remember if the AB Pro guys were the ones out of Nebraska or Idaho, but they were also involved with the Avid system in Arizona. And in California's system there are only maybe five or six companies. Even where you have states that say, oh, this is organic. We developed this ourselves. This is Michigan Net or Wisconsin Votes or whatever. All of them are not using true in-house development. Not that that would be better because they don't have the skill set or capacity, unless you have a couple noble laureate kind of level capability, people working on it, they're not up to the task. You, the States and counties, just are not going to have the resources or this highly skilled people necessary to even have a chance at building a secure system. They don't have the funds to maintain them. They don't have the people to defend them. It's smokescreen. It's 100% smokescreen. But even with that, you have states that claim to have done organic development really like we found in Michigan. What they've done is they've contracted out. So when you look at the resources they've allocated to development and maintenance, it's all contract and they have a few government

people on top pretending to be captaining the ship, right? But it's like, if you've ever seen the grocery carts where the parent is pushing the grocery cart, but in front of it there's like a little toy car, a make-believe car and the toddler can sit in there with the steering wheel. They're not operating the cart, they're not choosing the direction it goes and that's how it is for the technology in our election offices.

So let me get back to the bottom-up idea. All of the voting registration systems in the United States are theoretically either top down, hybrid, or bottom up. If they are connected, the centralized system is the single access point to modify the data. So in some cases, we're told, the clerks are the only ones who have the authority to modify the voter registration information, but if it's held in a centralized database? That centralized database can be modified by the lowest level administrator of that database and anybody who gets either authorized or unauthorized access. So when you take a company like Runbeck or another company, a vendor that's providing an automatic signature verification machine, if they have an application programming interface, a machine-to-machine interface to the voter registration system, they have access to the database, they can populate it, they can modify it, they can read it, and the suggestion that they can't do that. This is, you know, is sort of putative. It's a technical suggestion that has not been borne out by independent auditing and review and, you know, verifiable sort of forensic work and the fact that the citizens in none of our states have access to do that and we aren't being given the reports.

Like I know in Colorado, for example, there was a 2015 report from the auditor about vulnerabilities in our voter registration system never revealed to the public. There was a 2020 audit done by a private company that is, you know, now tight with the election officials, a company called Synak. They've gotten very big, very fast by paying National Association of Secretaries of State and state election directors to be their partner. Now Synak is doing these reviews. Synak was bragging on the NASS site about the vulnerabilities they found in Colorado's election related systems. Colorado's election offices and Secretary of State never told the public or public officials about any vulnerabilities that were found. So this is true everywhere. The systems aren't secure. We can't get to them to verify them. Nobody else is verifying them. It's smokescreen and you connect an ePollbook to that and that poll book is compromised. The poll book may be the channel of compromise if it has any wireless or network connections.

ASG: Shawn, I have a question that came in from Edie actually through e-mail after the last one and I it seems like it's relevant here. If not, we have Jeff coming on next time to talk about, you know, how to look at voter rolls. But I think this is more for you. OK, here's what she says: I've been thinking about the whole concept of phantom voters, those for whom votes are cast, but they didn't actually vote. And how inflated voter rolls fits into the picture. I have questions on how to identify those votes and actions other states have taken once they're identified. I also would like to better understand how voter rolls are inflated and whether inflated rolls have a purpose other than becoming a repository of phantom voters. I think it would be helpful to have a discussion about them.

SS: Yeah, Jeff, I'm sure, is going to discuss that. And I'm excited because Jeff is the master of the data. In fact, we just had another call about a week and 1/2 ago with somebody who's also thinking hard about this. But there are multiple states that have taken, in some cases, overlapping or similar approaches. And then there are multiple states where new approaches to vetting and reviewing voter roll data have kind of been developed. And so Jeff and the data team are working on sort of cataloging all those techniques and building easy access for grassroots teams in different states to do their own states data. So there's several challenges with the data, right? There's obtaining it, which a lot of states, secretary, states or public officials have made difficult and expensive. Then there's kind of normalizing the data because they don't keep the same data elements in the same way in every state. You know, one database may have 100 different elements per voter, one may have 6. Trying to compare those, if you're looking for duplicate voters or dead voters or reuse of the same or permutations of voters names, you have to be able to compare as much of that data as possible. So there's this whole interface problem of matching up one state's database approach to another state's database approach and then seeing what you can learn from it and then applying other tools like national change of address database and those kind of things as well as looking at motor vehicle databases and taxpayer databases. And so all of the data that's possible with information pertaining to specific individuals is potentially useful. And the data team is working through all that. Jeff will explain what they're doing there.

So as far as the purposes of having inflated voter rolls, multiple purposes. So one is actually fake voters, to actually cast fake votes. Another is so you can normalize abnormal turnout. So let's say your state has 100,000 people. In theory, about 80,000 of those should be voting eligible population. About 80% of a given population should be voter eligible voting age not disqualified for some reason. If you have turnout, our US turnout was like depending on age range, 60 percent, 50% depending on midterms or the general elections, presidential elections, etc., you had this normal range of turnout. If you want to cast more votes, especially if you want to cast more votes than are really exist, you have to increase the amount of voters in the database so your turnout doesn't look like this. So your turnout doesn't go from you know, 50% of the registered voters or 60% of the registered voters to 90% of registered voters. So when you see the turnout stays, you know high or relatively normal, but really the registered voting population as a percentage of the population has skyrocketed. What you're really seeing is an abnormal turnout that's being masked.

Then one thing that's for another purpose for it is when you have redistricting. For example, in Colorado you have a redistricting Commission, and the redistricting Commission is allocated on the basis of roughly the percentage of affiliations or proportions of voter affiliations in the voter registration system. So let's say you're real, no kidding, non fraudulent voting population is actually like 40% Democrat, 40% Republican, 20% independent. But you inflate that with a lot of independents or unaffiliated. So now when you go to the voter redistricting boards you are picking 1/3. You know you instead of having the real values you have 1/3 of each and so you have a 1/3 of the redistricting Commissioners are going to be Republican, 1/3 Democrat and 1/3 unaffiliated or independent. Well are those 1/3 of independent, unaffiliated, truly unaffiliated, independent? Are they people who were basically set up to be able to state that

they're unaffiliated when they're actually not unaffiliated, or they're independent when they're actually not? So there's a third purpose. One is votes, two is to mask extraordinary voter turnout, and three is to effect proportional allocation based redistricting commissions and boards. Those are off the top of my head.

ASG: Awesome. Alright. And Edie, I made a note to bring up that question again for next time when we have DataJeff here too. Linda?

LINDA: Yeah, I wanted to tell Edie that because I went to our house, the Missouri House yesterday and actually testified on this against one of the bills and it was the initiative petition process, which of course is citizens filing petitions. And when you have inflated voter rolls and they're basing it on voter registration numbers.

EDIE: Yep. Thank you.

LINDA: You could grab it from there.

SS: That's perfect. So there's a fourth and a very important one. When you have a larger number of voters, you increase the threshold and therefore the barrier to voter-initiated ballot petition. So if it's based on a proportion or percentage of votes cast for a given office, like if you want to recall your governor or your Secretary of State or something, if it was, you know, an accurate number, it might be much lower. And you see this in California, where they tried to recall George Gascon, I think. When they tried to recall him and not only did they have, you know, an extraordinary, unprecedented, historically unbelievable number of petition signatures rejected, I want to say it was close to 30%. Not only that, but the barrier or a threshold was so high because they had this inflated cast vote turnout. That's exactly right.

ASG: Thank you, Linda. That's perfect. That's such a good point. Shawn, George is saying the key to phantom voters is the ePollbooks, as the ePollbooks knows who has voted in real time. All ballots cast number has to match the ballots approved to be cast. Voter’s info is in the Epoll books.

SS: All right. Yeah, they have access to it, right? ePollbooks are an extraordinarily bad idea. I view them as a collection mechanism for bad actors. So there may be a beneficial and legitimate purpose for them, but the architecture of them, the fact of them is creates a vulnerability that just can't be tolerated. And it all goes back to, why do we have to have people vote anywhere, right? What's the real argument for that? Is it convenience? You can't sleep anywhere, right? You can't have your home anywhere. People have either no home because they're homeless, in which case they can identify a government office and receive official mail there. Or they can go to the post office and say, you know, a homeless person can go to a post office and say, I live here in this postal district. Here's where I will receive my official mail. I will come and pick it up. But having the ability to vote anywhere is what requires every single vote center or precinct or location to have access to the entire voter registration system. It is a bad trade. It's like Tonto good trade, bad trade. It's a bad trade. We're trading convenience and

argument of convenience for integrity and security and a good reason to trust our elections. There is no reason to do it. We should vote at our own personal precincts, and we should make an event of it. If you have to go vote somewhere else, you should request an absentee ballot. Provide evidence or a certification that you're going to be absent from your polling location. Not do this vote anywhere, drop your ballot anywhere thing that is a recipe for loss of custody and that's exactly what we've got.

ASG: So Shawn, can you talk about a solution? As a kid I remember going with my parents to vote. There were these printouts, like the dot matrix printers that had the holes on the side. I'm probably dating myself saying that but I remember that green and white striped paper, and we'd stand in line and then when you got to the front, you'd say your name, give your ID, they'd look it up on that paper and then they check off your name and send you to a booth. But if we, and I know you've talked before about how it's harder for the criminals if all the data is decentralized, if they have to break into multiple little counties. But even still, wouldn't those counties be storing, even if the counties were storing it locally, aren't they still storing it on machines that are connected to the Internet? And so can you talk a little bit about now that we've come so far with technology, how do we fix that as far as the poll books?

SS: OK, so this is what I would do and what I would recommend. Counties or parishes or in some cases townships, some states have townships more than counties that are their voting centers and they are responsible for their roles. This plan requires modification of HAVA because HAVA requires a centralized, single authoritative, statewide voter registration system. You can still have an authoritative list, but you have to eliminate access from anywhere outside the county. That means the machines cannot be connected. So what I would do is have a single county network with backups that is not connected to anything. That is an isolated system. It's not that difficult to do that. You don't introduce anything to the system. You lock down the configuration. It's used for one purpose. It's not that expensive to do this. And then for elections, I would have them print off precinct rosters. So as of the day before election, they print off the precinct roster, they hand carry that precinct roster to whatever the voting education is, and you do exactly as you described. You show up with your government issued photo ID. You vote in person. If you requested an absentee ballot and it shouldn't be no excuse, then you receive that and you return that however it's prescribed. Presumably you would have a security envelope inside that. You would have the signature, you would actually have qualified certified questioned document examiners, because that should be the standard that examine any absentee ballot signature to verify that it in fact matches the locally held county-controlled signature for that voter that was given in person. You have a paper roster at your precinct, they check your name, they verify your ID, and if you're not on that precinct list, but you assert that you're an authorized voter and this would be a statutory thing within the state. Then you would show your government issued ID, they may take a photo of your government issued photo ID and they would hold your ballot until they had verified that you were an authorized voter within that precinct and had not voted anywhere else. And then they could count your ballot and that might delay release of results for precincts that were affected if the number was significant enough to effect any of the races or issues. So that's how I would do it.

And then as far as reconciling the rosters between counties or townships or parishes and each other in the state and between states you can do one-way extracts. So in other words you can write a database, you know how cheap a compact disc or a DVD is? Super cheap. Especially if the government buys tens of thousands of them.

ASG: Well, when the government buys them they won't be cheap.

SS: Yeah, that's right. If you go to OfficeMax or whatever and you buy these or, don't use Amazon, but if you go to one of the vendors. So imagine now you're Harris County, Pennsylvania so and you need to send your database every day to the state you have an optical DVD or CD writer on the machine. But you keep that database on and you write that database, the current version of the database. You put a time stamp on it or a label on it or whatever. And then you take it over to machine and transmit it to the state on whatever their VPN connection is. And the state can get that from every Township and every day they can get that update. And so every day they can have that list that they can reconcile between counties to make available to all the rest of the counties so they can verify the voter ID number or Social Security number, address, name, date of birth, etc. It should be very few criteria. And verify that they don't have duplicates. And then if they have duplicates between Counties, Townships, parishes, or between states, then there needs to be an office with the procedure for reconciling those, like a notification. But nobody outside of County, Township, or parish should have access to directly manipulate or even read anything on that locally held voter roll. It should be read-only to anything outside that local office. And they should have secure backups which are not hard to do so that's what I'd recommend doing.

ASG: OK, thank you. So from the chat Pierre posted a link which he prefaced by saying: Shawn, after nearly six years in data networking, I fully agree with your clear vulnerability descriptions. For anyone who is not aware of scientifically exotic voter roll manipulation, have a look at this link. It's unknown how the algorithms initially got into their roles, but networking was surely involved. In North Carolina, we're seeing similar oddities, but we haven't analyzed them to the level New York has. So there's a link there. And then Marlene and John: our town clerk just went through the registered voters list and verified with our cards, as well as verified against the CVR. She told me she wanted to make sure ours were correct. She said it all checked out. We do not have epollbook signatures. We have a vote on the town warrant to get rid of the tabulator we use, hoping we can have enough people to sign and vote in our favor. They also said in Maine, all towns are voting centers and results are sent by computer results to Secretary of State. This is not safe either. I will petition to have the state or a couple of towns to do it. And then George said Illinois requires hard copies of poll books at each precinct in case of voter system failure. No, what could go wrong? It's safe and secure, right? And then, Edie said, in Massachusetts, our central database is fed by our RMV, Department of Health and other organizations. They then send lists of voters to each of the 351 separate cities or towns for verification. Beginning in July, illegals will be able to obtain a driver's license. Yeah, that's already happening in Colorado.

SS: And the RMV doesn't allow the driver to indicate that the driver is illegal. You can see it coming, right? It's a recipe for fraud and, and I suspect it's actually intended for fraud, right?

ASG: All right, Linda, go ahead.

LINDA: OK. Maybe similar but slightly off, but I wanted to ask you, Shawn, so our counties are being requested by our Secretary of State. We have a new provision for cyber security reviews, which I'll send you a document at some point, which is really we have a cyber security guy who's like, this is a joke, but I'm finding out that there's a company and I thought he said it was called Cyber Defense, but it was sold to a company in Texas called Apollo. So they're providing cyber services to the counties. They're also doing their own cyber check on their own services. But I didn't know if you know anything about Apollo because I'm being told there's some, there might be something where there we should be looking at.

SS: I'm not familiar with them. I could probably look them up. So what I would say is that your public officials don't know the difference. So next time you go to an airport, imagine that you just pick one of the passengers getting on the plane who has a child that's gonna board early. You get the child and you ask them to go out and do a safety inspection on the airplane before everybody flies. That's where we're at. And again, that sounds terrible, but it's just true. So you look at our voting systems and the voter registration systems, the people responsible for them do not have the slightest idea what they are talking about or how to secure them. Like in Colorado, for example, we saw this guidance, Secretary of State is now giving guidance. The Secretary of State's office is giving guidance to county clerks who are the chief election officials or designated election officials for their counties in Colorado to make sure as part of their logic and accuracy test and during the election, conduct to make sure that the wireless devices and their voting systems are turned off. They don't know how to do that. Even if they knew how to do it, they don't have the ability to do it. They don't even have BIOS passwords. Even if you add BIOS passwords, that hardware can be controlled on those voting systems at the hardware level, by scripts, by triggered scripts, by complex like binary and tertiary type triggers. It's ludicrous.

So the idea that you're going to have public officials doing this now, now you're going to have some low bidder, private contractor, I'll look them up. I can look them up. I can tell you right now they're not going to be good enough because the government can't afford people who are good enough. The people who are good enough are working for national security and defense firms and the big tech companies and they're not good enough. The Joint Staff Knowledge Management at that time, I think it was only about 7 1/2 or $8 billion a year spent on cyber offense and defense in the Department of Defense, let's say charitably only for four and a half billion was spent on defense and the Department of Defense could not protect the joint Staff's knowledge management network. It's an unsecured network because it was connected to the Internet. You cannot protect anything connected to the Internet. It cannot be done right. The systems are too complex. You'd have to lock down so much like the users of the system would not be able to navigate to Google. You would never let a user on the system you were trying to secure navigate to a public search network. You would have to lock down so much in order to

even have a hope of defending them. Then have intrusion detection and intrusion protection. I don't care who they get, they're not securing their networks. It's not happening. They're pretending to secure their networks, and they're going through the motions so that they can say that they did a good job, and so that NASA and NSA and EAC can give them Cleary Awards and pats on the back and publicly praise them for following the protocol and the narrative. But they are not secure. I promise you, give a carte blanche, give a blank check to a red team being used in the Department of Defense and give them five minutes and they will own any election network in the country.

LINDA: I put a link in the chat. I'm calling it our Fab Four, these four, so they put this event on that's coming up to show. I think they're getting nervous with the stuff that we're getting out there. So it's how our elections are secure and how we can make them more secure. But these four counties, these four counties represent, we have 4.3 million registered voters. These four represent about 1,000,000 of the voters. And the one in the woman in the picture, she's actually, she's a lawyer, county clerk-lawyer, and she actually sits on the board of some of those subsidiaries of CISA like the IIS AC and things like that. So this is a pretty dangerous group out there, but they're putting their event together. I kind of laugh. I tell people because those who believe it's secure, why do they have to go to a seminar and I tell everybody else, don't waste your time.

SS: So the IISACs, first of all they're basically run by CIS. Second, the people from DHS and CISA, for the most part, have no technical knowledge or expertise whatsoever. I don't claim to be a cybersecurity expert. I know far more than most of these individuals about cybersecurity and the threats. I'm not a defender. I'm not a coder, I haven't done penetration testing for computer systems other than some very basic work and I haven't done any coding in a long time. These people are wildly ignorant but being praised and told they're the experts and then they get to go out like Chris Krebbs and say. Hi, I'm a cybersecurity expert that literally the person running sizzle right now, the director of CISA (Cybersecurity and Infrastructure Security Agency) that is responsible for protecting US critical cyber infrastructure, national security infrastructure including election infrastructure. Literally. She is a former professor, assistant professor of sociology, that is her background and she did a bunch of policy stuff in cyber related offices and those people coming out and saying they're cyber experts.

Kurt, our good friend and one of the attorneys in the Arizona case and many others, such a good man, former Navy SEAL, he used to tell me not to say anymore that I'm not a cyber expert. I am not a cyber expert. There are people like Clay Parikh who are cyber experts. Clay will tell you he's kind of mid-level with all of his experience and expertise and certifications. He's not an autist. The autists are like magic. You watch them and they are like Neo in the matrix. They almost think in machine language. They're more like in sync with machines than they are with people. And it becomes evident when they start doing penetration testing or hacks, they flow through security architectures like a hot knife through butter. And so that is the threat. The people who are claiming to be cybersecurity experts for the most part of the government are posers, if not imbeciles. And so a lot of these people, these election officials,

they go to these meetings and they get these briefings and then they consider themselves informed. “They told us about the threat.” OK, well, what do you do about the threat?

A perfect example is that information or the industrial control system advisory on the Dominion voting systems Democracy Suite ICX or Imagecast X tablets nine critical vulnerabilities, including some which could affect other components of the voting system. Because you can hop through them, they can transport vulnerabilities and hacks into other components because you're carrying portable media back and forth, or because they have an actual connection? And no election administrator in the country who is using the Dominion systems, including that version and the other versions which were not tested for the vulnerability, none of them have taken all the mitigating measures. They don't even understand what the mitigating measures mean.

LINDA: Is it Brianna Lennon that you're talking about?

SS: Yeah, I mean, I don't know what her background is if it isn't cyber. She's a babe in the woods. She is a toddler walking across a superhighway. But being praised, I'm sure, and being told now she's an expert so she can talk to public and say, Oh yeah, we're super secure, I'm in IISAC. We share threat information and then you do what with that? Nothing. What would they do with that? It'd be like me telling you that you are about to be bombed by B52. Where you’re going to run out with your umbrella up. They have no ability to defend the systems. They don't know what they're talking about. And the continued perpetration of the narrative about the systems being secure is a lie. They are violating their oaths by perpetuating these lies.

So we found out that in the elections bill that passed last August, the Secretary of State here has the authority to require penetration testing of any machine or they can't sell their machines in our state anymore. And he brought that up when Mike Lindell was here. We're sitting there and I had told Mike about it ahead of time. We were going to kind of kind of strategize on it, but he brought it up and we said, well, then do it. Because he said penetration testing just means they're going to look at whatever. I can't remember if he said it was the software or not the software, whatever. I'm like I think penetration testing is what we want and we're trying to get him to do it. So I don't know if it would that, I mean is penetration testing really truly what you mentioned with Clay going in and actually finding out what's in those machines? So typically penetration testing is it can be either. So there's different types.

Let's say a Department of Defense, a weapon system, you will go through like multiple phases starts at development where you have the concepts or requirements, it's bench level testing of components, it's verification and configuration. Then you get to developmental testing for cyber where you'll have typically cooperative or blue team testing. So this is where I'm a cyber threat tester and I sit down and I've got my arm around the developer of the system or the program manager and I say OK let's look and see if you're using user authentication. Let's see if you're locking down your communications protocols and your ports. Let's see if you're actually logging everything you should be. Let's see if you're using the built in security configurations that were supposedly programmed to begin with. That's all cooperative.

Then there's non cooperative, where you take that system, you put the intended user in front of it. They're going either doing it real world, whatever they use it for like they're operating satellites with it or whatever. And then you give red teams boundaries and say look don't command the satellite, whatever you do, don't do that. So stop short of that or don't make the servers or the uninterruptible power supplies light on fire again like we don't have to tell you, don't light the server room on fire again because that's been done and then you turn them loose. And they then have to gain physical access if you're still doing that or if you just accept that they always gain physical access, they always gain physical access to some connection or aspect of the system. And then are they just putting in a thumb drive or are they pulling a power plug and putting something in there that does phase modulation of commanding through the hardware, through the power system into that system? Or in fact are they connecting in a different room to a socket on the same circuit and doing that modulation? To get commands into the system, we've seen that too. But they're getting to the system, and then they're looking for vulnerabilities and configuration or hardware. Maybe it's something that could have been patched but wasn't, or maybe it's a vulnerability in hardware or software for which no patch exists. There is no way to protect it. If it's on your system, it's vulnerable, right?

This is the state of the ICX tablets in the Dominion Democracy Suite system. For that version, we know for sure, their vulnerabilities in that system that have not been and cannot be mitigated. It's about the way the system is built and the software on it. You know, like if you're using the old Citrix front end appliances in your voter registration system, it's no longer being supported, it's past end of life from Citrix and it's not being patched. That security vulnerability is there for the rest of the time. The only way to prevent it being exploited is to prevent access to the system en todo, and they cannot do that because they've exposed it to the public Internet. So anyway, back to penetration testing, it's like a seat belt, right? If you don't use it, it's not a safety device, it's just a hand waving. So if they don't do the penetration testing then it's of no use. If they do the penetration testing with qualified you know experts, cyber penetration testers, they're going to get access to the system. That doesn't mean you'll be able to find every possible vulnerability and compromise of that system because they can be very complex and all hidden, as CISA knows very well, because they had the Solar Wind supply chain compromise on their networks, as well as almost every other major federal agency and department for ten months without them being able to even detect it. And they were running intrusion detection and prevention systems along with actual cyber defenders whose job was to defend those networks 24 hours a day. So they didn't have a signature or a heuristic profile that revealed that vulnerability or compromise, and it happened anyway. The voting systems and the election management systems and the voter registration systems and their administrators do not have a chance. They have no chance.

ASG: Yes. And when you were talking about in Colorado what the Secretary of State is doing and having all the county clerks make sure their devices have the Wi-Fi turned off.

SS: But it won't even get that far, right? Because what will happen is Matt Crane who runs the Association of County Clerks in Colorado, will just talk. They'll say how do we do that, Matt? and he'll say, oh, don't worry, put your ear real close and you listen to hear. If you hear the Wi-Fi

right, they don't like and he'll say, you don't have to worry about that. And they'll just all breathe a sigh of relief, right. Like, OK, good. I don't have to worry about that, right.

ASG: Yeah, don't worry, these are tested by Jack Cobb at Pro V&V, who said he has no cybersecurity expertise. And Shawn, you were talking about when Linda was talking about the penetration testing and you were talking about that. I thought, yeah, but how this is likely to play out if history is any indicator? Is it that they will bring in either someone who's already in the network of these vendors or there'll be a brand new LLC filed, right? That's cyber security penetration testing by some guy who landed the deal. But the other thing that I thought was really striking too, Linda, when you said these four individuals that are doing the conference, which by the way Marlene and John, I see your comment because since I know that you guys are having trouble accessing the chat, yes, I will include the link that Linda shared and the link that Pierre shared. I will include those in the follow up e-mail so that you have access to those. But Linda, when you were saying that these four individuals represent over 1,000,000 voters, and given, probably at least 800,000 of those are real people, right?

LINDA: Yep.

ASG: No wonder your state is wanting to shift towards weighted representation, right, for your party elections, which then is just a stepping stone to ranked choice voting. So very, very interesting. OK. So I realize we could definitely keep Shawn forever here talking about stuff. This has been such good information and but I did promise you guys that I could give you a sneak peek of something that we've been working on. And Shawn, by the way, thank you always for the most descriptive yet horrifying analogies, like a toddler crossing a superhighway. I just love it. It's like horror but it makes an impression, it sticks.

SS: Well, while you're pulling that video up, Linda, I just looked up a couple of those people. Brianna Lennon has a Masters in public policy and a law degree. If her life depended on it, on her cyber knowledge, she's dead. Kurt Barr, director of Elections, Air Force Guy. So, so that's great. He was a finance officer and a deputy flight commander who honed his leadership and managerial skills. I know exactly what all this means. He has no idea what's happening on the computers and never will, right? If you're, if you're in your 30s or 40s, the chances that you're going to develop any kind of significant expertise in cyber is somewhere between zero and the asymptote of 0. So the idea that these people you know as well-intentioned and honorable as they may be—and I presume they are—the idea that they can really advise the public or protect the public's for election security with cyber based systems? ZERO chance. They will get happy talk from the federal state government and the elections offices and the nonprofits and the institutions, and they will repeat that happy talk. And it is nonsense.

ASG: So this is just a one minute and 15 second example, but what Shawn and I have been working on for the last couple of weeks is a section of the Cause of America website called Elections 101. Essentially what this will be is an educational section that you won't have to log in or have a registered account to be able to access any of these videos. So you'll be able to share these videos with anybody you want, whether it's elected officials or just the general

public, or you could share them on social media or whatever. But if you're familiar at all with the platform, Lynda.com, I love the format of Lynda. It's basically an instructional platform where you can go in and learn about all different kinds of things and they're grouped by topic. You could take a whole course on how to master Photoshop or the videos are so short, just a few minutes long each one. So if you already know how to use Photoshop, but want to know how to remove the glare off Shawn's glasses in a video, then you can drill down just to that video, watch that three minute video, get what you need and go back to what you were doing. So we're going to be using a similar type of format, where you can either watch one- to five-minute videos of Shawn explaining different, very specific, really drilled down topics, or if you want, you can watch, say, a whole 1-hour video where it's all of those little videos together. So Shawn is providing all the expertise and I'm just doing the technical stuff to make it look good. So here is just a little example of 1 minute video on what is a voter roll.

ASG PLAYED A ONE-MINUTE VIDEO FROM NEW COA EDUCATIONAL SERIES: ELECTIONS 101
You can watch the video here:
https://rumble.com/v27eh02-coa-elections-101-what-is-a-voter-roll.html

SS: I just wanted to say this as a segue or a tangent if I could real quick. Amy, I meant to do this before when I was talking about Paris Script. I originally looked at Paris Script because I was looking for people who could help me with signature verification, and then I found out they were being used by the voting industry already, and I looked at their personnel. So this is from LinkedIn, and Paris script again is in Longmont, Colorado. They're the company responsible for the signature verification technology being used in Runbeck's automated signature verification machines, which is verifying massive numbers of signatures for massive numbers of mail-in votes. You can see in LinkedIn where their 55 personnel studied. The number one location where they studied for Paris Script company personnel, Lomonosov Moscow State University. That's in Moscow. Number two: University of Colorado Boulder. So when I see a company, and I'm not saying Russians are bad ethnically. But when I see people who studied at Russian or Iranian universities that come into US technology firms, I'm automatically suspect of that firm. Like when we found out that the company that performed the only security auditing done on Democracy Works risk limiting audit software used now in increasing numbers of states, including Colorado. The only security audit done on that software was by a Canadian company called Security Compass with a bunch of Iranian engineers that graduated out of universities in Tehran, just like North Korea. Just like People's Republic of China. They do not let capable technology people go overseas unless they have a hook in them and a reason for them going overseas, right? This is not like Elon Musk escaping South Africa. If you see people from Russia or Iran or North Korea or the People's Republic of China that originated there, like the chief security software security guy for the company VOTUM, which bought out Everyone Counts, which is really the contractor behind Michigan's voter registration and roll system, that guy is a Chinese national who lives in Australia. So when you see those people in these companies, you know that there is foreign influence or very likely foreign influence in them. So when I look at Paris Script, what I see is a bunch of Russian engineers, that's what I see. And the fact that we're using that in our voting system with no external validation, in our election system with no

external validation, certification, accreditation or auditing should tell you everything that you need to know about the system.

ASG: Wow, OK. So I know we're overtime so we're going to go ahead and wrap. Shawn, I want to thank you again for being with us today to share your expertise and thank everybody for watching our first little video. We will have a whole lot more of those to come as soon as next week you should start seeing those. So thanks everybody for being here and remember our next meeting is going to be Wednesday, February 8th and DataJeff will be here to talk to us more about voter rolls and what you can do and what you can look for in your own counties and states. All right everybody have a great week.

SS: Talk to you soon. Bye. And thanks everybody.

(VARIOUS): Thank you. Thank you, Shawn. Thank you.