

PLEASE NOTE:

12:00:59

This uncertified rough draft is an unread, unedited, rough draft copy of the following proceedings. It is NOT a certified transcript and CANNOT be quoted from in a pleading or in any other document. The final, certified transcript to follow can be quoted from.

12:00:59

Please be aware that the unedited, uncertified rough draft transcript may contain untranslated steno, reporters' notes to themselves, misspelled proper names, nonsensical English word combinations, and/or mistranslated English words. These are not mistakes made by the reporter but are caused by the computer interpretation of the steno strokes and by the limitations imposed by writing the English language phonetically. All such entries will be corrected on the final, certified transcript.

12:00:59

12:00:59

The page and line numbers may change slightly in production of the final transcript; however, the time codes will remain the same.

12:00:59

(Court was called to order by the courtroom deputy.)

09:02:01

(Proceedings begin at 9:05.)

THE COURT: Good morning. Everyone. Please be seated.

COURTROOM DEPUTY: This is case 22-677, *Kari Lake v. Katie Hobbs*.

09:06:23

This is the time set for a motion hearing.

Counsel, please announce four the record.

MR. PARKER: Your Honor, Andrew Parker representing the plaintiffs, Kari Lake and Mark Finchem. Good morning, Your Honor.

09:06:34

THE COURT: Good morning. Who is with you at counsel table?

MR. PARKER: At counsel table is my colleague Joe Pull and my colleague, Jessie Kiborg.

09:06:44

THE COURT: All right. Mr. Parker, you'll be handling the argument for plaintiffs this morning?

MR. PARKER: Yes, Your Honor.

THE COURT: All right. Thank you.

MR. GAONA: Good morning, Your Honor. Andy Gaona along with my colleague Kristen Yost from Coppersmith Brockelman on behalf of Arizona Secretary of State Katie Hobbs.

09:06:53

THE COURT: Good morning.

MR. LARUE: Good morning, Your Honor. Joseph LaRue, Deputy County Attorney. And with me is Thomas Liddy, Karen

09:07:17

Hartman-Tellez, and Brian Urban of the Maricopa County Attorneys Office. Also with me is Emily Craiger and Emily Broadner of the Burgess Law Group who are outside counsel. We're all counsel for the Maricopa County defendants.

09:07:20

THE COURT: All right. Thank you and good morning. Everybody, please be seated for a moment.

09:07:37

In the midst of preparing for today's hearing, the Court was in receipt of two motions. One at about 4 o'clock yesterday afternoon, another one much later than that. I'm going to deal with them independent reverse order.

09:07:50

At docket entry number six was motion filed by the secretary to continue this matter briefly citing that their sole expert witness was caught in transit which I understand.

Mr. Parker, do you wish to be heard on that motion?

MR. PARKER: No, Your Honor. At the Court's discretion.

09:08:13

THE COURT: All right. Thank you.

Here's what I'm going to do. This matter is going to be heard today and it will be heard to conclusion today.

Understanding that there is an issue with the expert gettingly here timely I also am accounting for the fact that because the part and parcel of what I'm hearing in addition to the motions to dismiss is obviously the application for temporary injunctive relief and in that order where evidence will be presented, plaintiff is going first and so we're not

09:08:26

09:08:43

going to hear from your expert for a while, Mr. Gaona so we are going to get started at 10 o'clock. I'm going to give a continuance until 10 o'clock. 09:08:46

MR. GAONA: Your Honor, just an update on that. Mr. Ma see yes actually landed I was informed right before you came on the bench. He is in on Uber right now. He literally left his bag at the airport on time to get here as close as possible so I'm expecting him here within the next 10 or 15 minutes, so it may be that we can start at 9:30 to expedite things a little bit more as soon as he arrives 09:08:59 09:09:16

THE COURT: Let's plan at 9:40, counsel, so that we don't lose any time. This will become evident in my addressing the next motion, but I'm going to go ahead and lay in the schedule now.

The plaintiff is afforded two hours for its presentation today. Each of the two defendants that are here, so not including the joining Pima County defendants will have an hour and a half if they need it. 09:09:30

You can present your material in that time and understand that I have read he have a one's declarations and all of the attachments to those declarations and have internalized them thoroughly. So the directs are not as great of an issue in a circumstance like that. Oftentimes, in fact, I do away with the directing entirely and allow people to proffer their witnesses for cross, but we're going to go ahead 09:09:47 09:10:08

and hear from them on direct if that's what you want to do.

09:10:10

With regard to the earlier motion at docket entry number 74 which was a motion to strike the -- both the declarations and the testimony of five witnesses that may be proffered as experts by the plaintiff, that is really a -- that's really five *Daubert* motions or at least requires the court to go through the *Daubert* analysis five.

09:10:28

I will not decide what amounts to five *Daubert* motions without giving the proponent of those witnesses time to file a written response, reasonable time to file a written response.

09:10:47

I'm not quite sure why counsel filed that motion now on the eve of the hearing when all five of those declarations have been on the docket for over a month. Nonetheless, the conspirators deals with things as they come up.

09:11:04

The danger there's were cited in favor of disallowing those witnesses' testimony today are or will be ameliorated as follows:

With regard to the Rule 702 objections, first of all, this is a bench hearing, not a hearing before a jury. Secondly, for better or worse, the parties have drawn a judge in this case who is an engineer and a computer consultant who practiced in both areas before going to law school and the only relevance with that is simply for the parties to know that I will not blindly credit the testimony of any proffered expert

09:11:25

09:11:44

and will not move forward and accept testimony unless it makes sense under the disciplines that are addressed here.

09:11:48

With regard to the 403 objections as to waste of time, I've set the time limits. Parties are free to use them however they want to use them and when they have exhausted their time they are done so that's not really an issue with regard to waste of time.

09:12:08

With regard to danger of confusion, I think I've just addressed that above in the 702 analysis and then finally with regard to an argument that there could be danger from the testimony of one or more of these witnesses to election officials, that will be handled by the Court's policing and management of its own proceedings in the following way:

09:12:22

If testimony starts heading in a direction like that, I will strike it and I will do it *sua sponte* and I will warn the witness if it happens again I will curtail at that again point the testimony. So the counsel for the parties are advised to keep a reign on their witnesses to comport with the ruling and expected rulings that the Court has just laid out.

09:12:41

All right. Counsel, we're back on at 9:40. Until then you are free to move about the well or otherwise.

09:13:04

(Recess at 9:13; resumed at 9:42.)

THE COURT: Thank you, everyone. Please be seated.

All right. Counsel, welcome back. Two matters of housekeeping before we go forward. First of all, our local

09:42:19

Rule 43.1, which I know the attorneys are familiar with but members in the observers in the gallery may not be, prohibits any audio-taping or recording or photographs or any kind of recording of proceedings. And so that is prohibited and we will enforce compliance.

09:42:21

09:42:37

Second, with regard to masks, counsel, your witnesses while testifying may remove their masks if they are comfortable doing so, and the attorney questioning them or presenting to the Court while doing so may also remove his or her mask.

All right, as I've indicated to you, the Court will keep time on this based on the limits that I've given and I'll let you know at the morning break where we are.

09:42:54

If you wish to make any opening statements, you are welcome to do so.

Mr. Parker?

09:43:14

MR. PARKER: Thank you, Your Honor.

MR. GAONA: Your Honor, before Mr. Parker gets started, I just had one other housekeeping item.

We realized, because my phone was turned off in accordance with the Court's rules, that our colleague, Roopali Desai, is listening in on the public line. I just wanted to clarify for the record that she is present telephonically but will not be participating.

09:43:29

I also believe Mr. Jurkowitz from Pima County is on, and I'm not sure that his appearance was noted for the record

09:43:41

before in the prior proceeding.

09:43:45

THE COURT: It was not. Let me go ahead and have both of those attorneys make their presence known for the record since we've already announced for the Secretary and for Maricopa County. Let's go back to Ms. Desai first.

09:44:01

MR. GAONA: Your Honor, she's actually listening in on the public line but wanted to note for the record that she is listening but will not be participating. So she won't be able to speak to you.

THE COURT: Thank you. We have it set up for listening only, that's right.

09:44:12

COURTROOM DEPUTY: And Mr. Jurkowitz is on the AT&T line so he can speak.

THE COURT: Mr. Jurkowitz, are you there?

MR. JURKOWITZ: Good morning, Your Honor. Daniel Jurkowitz on behalf of the Pima County Board of Supervisors.

09:44:23

THE COURT: All right. I apologize for overlooking your announcement of presence earlier this morning.

Thank you, Mr. Gaona. Anything else?

MR. GAONA: Yes. One other housekeeping matter, Your Honor, and it relates to the time as divided between the defendants. The defendants have conferred before trial, based on the Court's initial order setting this hearing, and I believe Maricopa County is willing to cede some or all of its time to the Secretary as is appropriate, who is taking the lead

09:44:44



in defense of this case. So I just wanted to bring that up now and resolve any issues that the Court may have with that division of labor that we had agreed to before the hearing. 09:44:47

THE COURT: All right. Thank you, Mr. Gaona.

MR. PARKER: Couple of items, Your Honor. Is cross-examination part of the time for the defense when crossing our client or is it part of our time? 09:44:59

THE COURT: When you are examining a witness, either on direct, cross, or if I allow it redirect it's your time. When somebody else is, it's their time. 09:45:15

MR. PARKER: Thank you, Your Honor.

And a housekeeping matter, I believe Alan Dershowitz, counsel in this case, is also on the listen-only line.

THE COURT: Very good. Thank you.

MR. PARKER: The plaintiffs would like to reserve a half-hour of their time for rebuttal if that is permitted by the Court. 09:45:30

THE COURT: Mark, Mr. Parker, I'm going to tack your team with keeping track of that. I'm going to keep track of the entire two hours for plaintiffs. Thank you. 09:45:44

MR. PARKER: Thank you.

Your Honor, counsel, the right to vote and have your vote counted and counted correctly is the most fundamental and precious in our democracy, Your Honor. Other rights even the most basic are illusory if election systems are insecure and 09:46:01

undermined and for candidates, the injury is amplified.

09:46:06

What we are talking about 96 is the marriage between this critical as society of democracy and computers and the act to secure computers in order to make sure that this critical asset is not breached or compromised.

09:46:29

What is known regarding computer systems and this Court is likely well aware is that they are susceptible to intrusion, manipulation and compromise and the fact of the matter is, Your Honor, at the highest levels of this country -- and you'll hear testimony about this -- no matter how hardened their security is, they can be hacked. But certainly if the security isn't hardened at all isn't little more than your protection that you might have on your home computer, you do leave wide open that critical asset.

09:46:48

What is known regarding computer systems is not only that they are suss acceptable to these intrusions but also that electronic voting machine systems are no different than other computer systems other than the application that is overlaid upon them. So when we have testimony about the systems -- Electronic Voting Systems and the systems here in Arizona, it is also important to understand computer systems and other applications and how those have been hacked as well.

09:47:14

09:47:37

Here we have the somewhat unique opportunity, Your Honor, to having been able to look under the hood, if you will, of the very system lated for use in 2022. This opportunity

09:48:01

doesn't come along very often for us to really assess and analyze our protections or lack thereof.

09:48:06

What we find after we take a look is a serious problem and you'll hear this in the testimony. You've seen it already in our complaint, allegations. You've seen it in the filings on the preliminary injunction, line and verse as it relates to sworn testimony in the declarations and exhibits submitted previously as well as those submitted today and you'll hear further testimony on it.

09:48:20

So the serious problem is not just a risk but in fact you ask the question, Your Honor, is it more likely or less likely that, in fact, a hack is going to occur when a system is so wide open as the Arizona and the Maricopa County and Pima County systems were in 2020 and they are slated to be done again in 2022.

09:48:39

09:49:06

So that question, after you review and hear all of the evidence as to what is likely and what isn't, the defense claims, oh, it's a fantastical idea. Once you hear the extraordinary lack of security and the open ability too connect as well as supply chain issues and the fact that components of computer systems made in China and other countries have been and are real world affected regularly at some of the highest levels of this Government of the United States Government and, in fact, even when they are protected and watched.

09:49:28

So with all of that, we would like to call our first

09:49:50

BENJAMIN R. COTTON - Direct

witness, Mr. Ben cotton.

09:49:54

THE COURT: Mr. Cotton, if you would please step up to my courtroom deputy, she will swear you in.

COURTROOM DEPUTY: Please your name and spell your last name for the record.

09:50:09

THE WITNESS: Benjamin Richard Cotton. C-O-T-T-O-N.

(BENJAMIN R. COTTON, a witness herein, was duly sworn or affirmed.)

THE COURT: And Mr. Cotton, you may take your mask off and leave it on as you see fit.

09:50:35

And also the same for you, Mr. Parker.

**DIRECT EXAMINATION**

BY MR. PARKER:

Q. Mr. Cotton, state your full name for the record, please?

A. My name is Benjamin Richard cotton. C-O-T-T-O-N.

09:50:52

Q. And describe, please, four the Court your relevant experience in the area of cybersecurity?

A. I have over 25 years of experience performing computer forensics, e-discovery and instant response within both the public and the private sectors. I have also served 13 years as an instructor for guidance soft wares encase and encase enterprise platform.

09:51:16

Q. Describe some of the work that you have done as it relates to cybersecurity in terms of your experience?

A. I am currently Vice President for Incident Response four

09:51:39

United States District Court

E-Centire (phonetic). And I routinely perform incident responses, computer forensics engagements, cybersecurity assessments, for both public and private sector entities.

09:51:43

My most notable experience was I was the one with my software that I developed that discovered the Office of Personnel Management Breach by the nation state actor, China.

09:52:02

Q. And how did that occur?

A. We were actually there on a demo of the software. We were permitted to install inside of the servers and push some agents out and it just so happened they pushed that agent out to a SQL server that was infected with the agent and we discovered it in about an hour.

09:52:21

Q. And what occurred after you discovered it?

A. Well, you know, it's kind of one of those things, did they put this here to test me, okay. So I looked at it. I did a little bit deeper analysis on it, confirmed that it was malware and I interacted with the IT staff there to ask them a couple of questions. The first one was: Do you use McAfee software? Because the malware was disguised as McAfee executables.

09:52:40

They said they did not, that they used Symantec.

09:53:09

And I told them they had a problem, imaged the memory, turned that over to them and went into the incident response mode.

Q. Have you testified as an expert before?

A. I have.

09:53:25

Q. And can you describe how many times and --

09:53:25

A. Approximately text message times. They are fully detailed in my CV. That includes very large-scale testimony such as I was on the Lockheed Martin side of the *Lockheed Martin v.*

*L-3 Communications* for the Atars contract. I was and the Banco Progreso side of the *Banco Progreso v. Pedro Castillo* which at this time you the largest individual bank fraud in history of the IMF.

09:53:44

Q. In those cases, were you doing computer forensic work?

A. Computer forensic work primarily with cybersecurity as an underlying tenet on all cases.

09:54:04

Q. Have you worked for the United States Government in the area of cybersecurity?

A. I have. I am a contractor for the DHS hunting and incident response team as well as I did deep five forensics on high value terrorist targets for the Intel at the three letter Intel agency and I've also performed forensics analysis work for the drug enforcement agency with their national lab to your in nor ton, Virginia.

09:54:22

Q. Do you have a security clearance?

09:54:50

A. I do.

Q. What is that?

A. It's a top secret with special compartmented information in a full lifestyle poly.

Q. Are you familiar with the electronic voting machine

09:55:02

computerized systems that Maricopa County uses?

09:55:04

A. Yes ?,.

Q. And how did you become familiar with that?

A. I was engaged to do the forensics analysis and the forensics preservation of the systems provided by Maricopa County in response to the Arizona State Senate audit.

09:55:18

Q. And do you understand they are going to be using that system again in 2022?

A. That is my understanding from the statements, yes.

Q. You have submitted a declaration in this case; correct?

09:55:39

A. I have.

Q. And do you stand by the accuracy of all of the statements made in that declaration?

A. I do.

Q. Describe in general the components that you would look at or you did look at as it related to the 2020 election in Maricopa County?

09:55:53

A. So we looked at what was provided in response to the subpoena and that included the EMS server, the election management server. That included the EMS clients which are computers that remotely access the server. It also included the ICC systems that controlled the scanners for the Canon devices. We looked at the high pro scanners, there were four of those. We looked also at the adjudication systems and we were provided with the ICPs, the ballot tabulators. However,

09:56:15

09:56:42

we were not provider with the proper authentication keys to get 09:56:49  
into the technician or the administrative functions of the  
ballot tabulators so we were not able to analyze it's  
configuration or perform forensics image of those systems.

We also had access to all of the SD cards that went 09:57:08  
into each tabulator. Now for every device that you produced to  
us we followed the Federal Rules of Evidence handling  
procedures. We created forensics images of those with the  
encase and the forensics tool kit software.

So we did preserve a forensics image of all of those 09:57:29  
systems that we have and those were used as the basis for the  
analysis.

Q. In terms of the components that you were not provided  
authentication in order to get in and analyze, did you ask to  
be provided with that information? Did you indicate that it 09:57:44  
was important to your review?

A. We did and we did that on multiple occasions. What  
ultimately came back both in public and private statements by  
the county was that the county did not actually control those  
authentications, though eye button tones tokens, that would 09:58:03  
permit to us get access to the technician of the administrative  
functions of the system. The only people who had access and  
control of those were the Dominion employees who were on site  
at the county.

Furthermore, the count indicated that they could not 09:58:27



compel the Dominion employees to produce throws eye buttons on tokens so, therefore, we were not allowed or we did not get accession to confirm the configuration of the wireless modems, the lanes and those such devices as they were configured on the tabulators. 09:58:29  
09:58:46

Q. But you made it clear that you wanted access?

A. Yes.

Q. Now, the vendor is Dominion voting systems in Maricopa.

A. Correct.

Q. And you say they had control of providing the access? 09:59:01

A. Yes. And the concern on that, obviously is, that inherently the validation of the certification of the systems and the validation of those tabulators should be an in interpret governmental function by Maricopa County personnel and if they don't have access to to do that that then that means that they are relying on the goodness and kindness and accurate reporting of the Dominion employees. 09:59:22

Q. In terms of what you were able to get and look at in the -- under the hood, if you will, of the electronic voting system used in maybe copy, what did you find when you looked in terms of any security vulnerability? 09:59:45

MR. GAONA: Objection, Your Honor. I just want to note for the record, given the pending motion, that we do have an objection to Mr. Cotton providing expert testimony on this issue under Rule 702, a *Daubert* decision as well as maintaining 10:00:05

our relevance and 403 objections. I just want to note a standing objection for the record on that issue with respect to his opinions.

10:00:12

THE COURT: You may.

MR. GAONA: Thank you.

10:00:19

THE COURT: All right. You may proceed.

MR. PARKER: No need for me to respond to that at this point, Your Honor.

THE COURT: No. You are going to respond in writing and I know you're in the middle of your examination now so we will establish a timeline for the response before we leave here today.

10:00:29

Go ahead, sir.

MR. PARKER: Thank you.

THE WITNESS: Quite frankly, I was shocked at the lack of cybersecurity elements wherein the voting system and I'll give you a couple of examples of that.

10:00:42

So if I was to summarize this I would say that the average home computer is better protected than the EMS and the client systems that were in the Maricopa County environment.

10:01:02

BY MR. PARKER:

Q. And why do you say that?

A. Well, let me back that up. So when you -- when you look at a computer, you have a layered line of defenses because cybersecurity is an ongoing continual effort and there's no one

10:01:23

security mechanism that is going to be completely bulletproof. 10:01:27  
In the case of Maricopa County, they primarily relied on an air  
gap system and that air-gap system, given the configuration of  
those other components of the enterprise, could be bypassed in  
about 30 seconds. 10:01:48

We'll probably go into that a little bit further. So  
once you get passed that air gap, then you have to rely on  
on-pram type of devices like antivirus. Now, the EAC does  
require the antivirus and on the system. But in the case of  
Maricopa County, the definitions of that antivirus had not been 10:02:08  
updated since August 6 of 2019. I examined the systems in  
April and May of 2021.

So the business importance on that is that from my  
experience as a cybersecurity expert, there are over one  
million pieces of malware that are either generated, modified 10:02:36  
or newly equipped with signatures changed every day and so when  
you look at this, there were, you know, just off the top of my  
head roughly 700 million pieces of malware out there that the  
Maricopa County systems would not detect by their antivirus.

Furthermore -- 10:03:00

Q. What about patches, updates?

A. System patches are an essential element of cybersecurity.

As we know, Microsoft is one of the largest producers  
of system software in the world. In its systems with the  
exception of the tabulators, for all of the computer devices 10:03:18

that were turned over to me, they were running they went by version of Windows software. They had the Dominion software as an application on that device but underlying this was Windows.

10:03:23

Every week Microsoft will release a vulnerability patch update. That's because even Microsoft doesn't know all of the vulnerabilities that exist in their own operating system and people find these vulnerabilities that can allow them to get remote access and exploit the systems and Microsoft will patch those and they do that on a weekly basis depending on where you are, that's typically Wednesday or Thursday.

10:03:40

10:04:00

They also provide an off line service for these patches so that you don't have to connect to the Internet to download them and put them on your systems.

Q. When was the last time those patches were updated or added at all?

10:04:16

A. The same date that they installed the software which was August 6, 2019.

Q. No patches since then and you looked at it in 2021?

A. Correct. There were well over a thousand known vulnerabilities that could have been exploited by a kiddie scriptor with a program called Metasploit or some other exploit tool. It wouldn't have taken any skill.

10:04:32

Q. What about passwords, were those protected?

A. So they did have a password and the reason I use a password was they used the same password for every single

10:04:51

account on the domain on the system.

10:04:54

Q. And you saw this yourself.

A. I did.

Q. With respect to the antivirus, the patches, and the passwords, you saw all of that yourself?

10:05:04

A. Yes, I did. And I used -- I examined the forensics images. I used forensically court approved tools to perform that analysis and those images are available for other experts to look at if they should request.

Q. So if the passwords are the same for all people getting access is, that a proper protection mechanism?

10:05:23

A. No. And furthermore, it wasn't just it was the same password, it's that the password was established at the time of the installation of the software and it had not been changed since it was installed.

10:05:45

So that same password had been used for all accounts from August 2019 until the time that I examined the system.

Q. So if you had that password, could you get into the EMS system?

A. You could. Either locally or if you had remote access, you could log in remoting to the system.

10:06:01

Q. What about log management activity in the system? Did you assess that?

A. I did and, quite frankly, they had left the default sizes for all of the logs.

10:06:26

So the way that works is that I'm going to use the Windows security log, for example. On the server version of Microsoft, that is set at 20 megabytes and when a new log entry comes ins the oldest log entry is deleted and thrown away.

10:06:30

When I examined -- from that forensics image I took of the EMS server, the latest -- or the furthest back that that log went was 5 February, 2021.

10:06:48

Q. Post election?

A. Post election the county had turned over some logs but missing was the Windows security log. There were approximately 79 different entries or different log types on the Windows operatingly system side and they turned over three Windows specific logs to the Senate. But they did not turn over the application log or the security log.

10:07:16

The issue with that is that that is the log that actually records the remote accesses to the system, the IP addresses from which that remote access occurs and the user that performs that remote access.

10:07:39

Q. And so were logs overwritten post election or did you have the election time period logs?

10:08:03

A. Well, the logs were -- the term that I would use were rolling the logs so the logs were rolled in the case of the Windows security log.

On three separate occasions, the first occasion being on on the -- I believe it was the fifth of February. There

10:08:21

were about 462 instances of a script being ran that ran to check for a blank password. Now, there are only about 15 accounts on the stem.

10:08:31

So they ran that 462 times. The next occasion was on the third of March and they ran that same script over 34,000 times and then on the 12th of April, which was right before they were turning the devices over to the Senate, they ran that approximately three hundred and some times. The net result of that activity was that the Windows security log only wept back to the fifth of February.

10:08:51

10:09:19

Q. And were you ever provided with some sort of a secure data set from when the election occurred that might have been saved or backed up or mirror imaged?

A. I was not. That was actually an issue between the Senate and the county as to the full compliance on the subpoena.

10:09:39

Q. Any other maladies or issues you found in terms of the security in the system when you looked at the Maricopa County electronic voting machine system?

A. Yes so there is a -- I have personally viewed a line in the Arizona code that remote access to those systems shall not be enabled. There shall be no program on those systems that would allow remote access.

10:10:10

On all of the systems that I examined, the Microsoft remote desktop application was still on the systems and that was used to remotely log in to the server on multiple times.

10:10:28

Q. So you saw actual evidence of remote intervention. 10:10:36

A. I saw actual evidence of remote log-ins into the EMS server.

Q. And do you think whether those were permissible or security breach or . . . 10:10:51

A. The attributable log-ins, because I did see some anonymous log-ins that I could not trace back to an event. The ones that I did saw came from the local EMS subnet if you will, the IP address that for the voting system.

Q. Since we're talking about intrusion into the system 10:11:13  
through remote access, air gap is a term that you used a little bit earlier. Is that a process to prevent or limit remote access?

A. It is an attempt to limit a remote access. I would say that it's a good step but it's not bulletproof. It's easily 10:11:37  
bypassed.

Everyone in here probably owns a cell phone and whether it's IOS or whether it's Android based that cell phone would have a function called personal hot spot where you can use your cell phone as a wifi connector to the outside. 10:12:00

The issue with that becomes, is that each of the Dell computer that is were within to system did have wifi cards and that oh those wifi cards had been registered as a network on the computing devices.

So what that means is that at the time they installed 10:12:23



the software, those wifi cards were not disabled in Bios. Otherwise, they would not have been recognized by the operating system.

10:12:25

But the other interesting fact is if you set up a wifi without a password, then it is -- the default configuration for Windows to automatically connect to an unprotected wifi system.

10:12:38

Q. Is that a description of a hot spot? If somebody gained access they could utilize the hot spot to gain access?

A. Sure, yeah. That would give access to the Internet. You know, there multiple examples of breaches through air gap systems. If you remember the snow den breach of the NSA, that was an air-gap system.

10:13:04

Q. That the NSA had set up?

A. That the NSA had set up.

10:13:26

Q. And snow den breached it.

A. Correct.

Q. You would assume it was a hardened system?

A. Yes.

Q. It was breached, nonetheless?

10:13:33

A. Yes.

Q. Other examples?

A. Stux. STUX. Net is an example and that was a piece of mail mayor that was designed ton delivered via USB. It would iterate a network promulgate itself until it reached a

10:14:00

centrifuge and then control the speed of the centrifuge in order to destroy the centrifuge.

10:14:04

Q. Have you heard the phrase or statement made by cybersecurity experts that given enough time and access, any computer system can be hacked?

10:14:22

A. Yes.

Q. Do you agree with it?

A. I certainly do. Especially if you have physical access to those systems.

Q. Did you find that the Maricopa County system that you reviewed and is going to be used in 2022 had security to prevent access?

10:14:42

A. Know. The only prevention they had from an access perspective would be their passwords and those passwords were shared. The user accounts were not attributable to an individual. The -- it was the same password for every single account.

10:14:59

Q. Do you remember what the password was?

A. I do.

Q. What was the password?

10:15:11

MR. LARUE: Objection, Your Honor, we're in open court and letting that password out to the public is not in any anyone's interest and it serves no probative purpose to their argument.

THE COURT: Mr. Parker?

10:15:30

MR. PARKER: Your Honor, the testimony is and I don't think it will be disputed, that that password is shared by people who don't work for Maricopa any more. They have had the password. It hasn't changed. It's already out. 10:15:31

MR. LARUE: Your Honor, we do dispute that -- 10:15:44

THE REPORTER: Can you pull the microphone a little closer to you, please.

THE COURT: The objection is sustained. There is no value to going further on this point.

You can make your argument, Mr. Parker. 10:15:55

MR. PARKER: Thank you, Your Honor.

BY MR. PARKER:

Q. What about protective measure that is the defendants point to to say even if we didn't have this or that security measure in place and with the most hardened system in the country, you know, we've got the EAC having certified our machines and we have logic and accuracy testing before and after and of course we have the two percent audit of paper balance. Will those things protect the vote? 10:16:13

MR. GAONA: Objection, Your Honor. Foundation. 10:16:37

THE COURT: Do you wish to be heard, Mr. Parker.

MR. PARKER: I think he has identified his background and credentials as it relates to cybersecurity and he's in a unique position to be able to testify about this because he has been in looking at the Maricopa County system. 10:16:53

BENJAMIN R. COTTON - Direct

THE COURT: The argument here is that you want to ask this witness about essentially among other things the statistical relevancy of two a two percent sampling then is beyond any expertise which you put him up for. The objection is sustained.

I would also point out that this leads into another sort of common theme which is that information in the form of a declaration has already been submitted to the Court so I've looked at it. I'm going to rule on whether or not it is appropriate to consider in the end or needs to be stricken. But, again, we don't need to repeat things that the Court has already -- has in its ambit and as I said to you has internalized.

Mr. Gaona? You're still standing.

MR. GAONA: I'm sorry, Your Honor. I'm just waiting for you to finish talking, Your Honor.

THE COURT: Please go ahead, Mr. Parker.

MR. PARKER: Thank you, Your Honor.

BY MR. PARKER:

Q. Do you have any background -- do you know what the USEAC is?

A. I do.

Q. And do you have any background with working with certifications related to the EAC?

A. I have reviewed the certifications they have produced and

United States District Court

BENJAMIN R. COTTON - Cross

I've reviewed the policies and ultimately I've reviewed the product that was delivered in the field as a result of those certifications.

10:18:04

Q. One of the sticks that you produced was regarding Williamson county correct.

10:18:16

A. Correct.

Q. And that was an EAC certified system?

A. It was.

Q. And it had a number of errors identified.

A. That is correct.

10:18:27

MR. PARKER: Nothing further, Your Honor.

THE COURT: All right. Thank you, motorcycle.

Mr. Gaona, will you be conducting the questioning of the witness?

MR. GAONA: Yes, Your Honor.

10:18:36

THE COURT: All right. Whenever you're ready. And I'm fine if you want to go from -- and this is true for all counsel, from your counsel table position or from the lectern.

MR. LARUE: Your Honor, before Mr. Gaona begins, just to alert the Court, Mr. Liddy will have just a few questions after Mr. Gaona is done.

10:18:50

THE COURT: I understand.

**CROSS - EXAMINATION**

BY MR. GAONA:

Q. Good morning, Mr. Cotton. Thank you for being here this

10:19:01

morning. Appreciate it. I just have a couple of questions for you. 10:19:03

Are you being paid for your work on this case?

A. Yes, I am.

Q. Who is paying you? 10:19:12

A. The law firm of Parker Daniels.

Q. How much have you been paid to date?

A. I haven't been paid anything yet to date but we have billed.

Q. How much have you billed so far? 10:19:24

A. I don't have that information with me. That is generally handled out of the Accounting Department.

Q. Are you billing Mr. Parker's firm on an hourly basis?

A. I am.

Q. What's your hourly rate? 10:19:35

A. My hourly rate for nondeposition testimony is \$350 an hour. For deposition and testimony, it's \$450 an hour.

Q. Do you have an estimate as to how many hours you've devoted so far to this particular case?

A. We have probably performed at least 40 hours of work. 10:19:48

Q. Okay. You are not an expert on elections, are you, Mr. Cotton?

A. Not elections, no.

Q. You're not an expert on voting systems, are you, Mr. Cotton? 10:20:04

A. I am an expert on the underlying operating system that controls and provides access to those systems, yes.

10:20:05

Q. But you would not call yourself an expert on voting systems themselves; correct?

A. I would -- no.

10:20:16

Q. You also wouldn't call yourself an expert on voting systems security; correct?

A. I would call myself an expert on voting systems security as it applies to the underlying computers that prior the computing power, the access for those systems.

10:20:32

Q. But again not as to voting system security specifically; correct?

A. Well, are you trying to draw a line of distinction that says that the operating system is irrelevant because the operating system provides full access to all aspects of the Dominion system.

10:20:51

Q. Prior to the 2020 general recollection, Mr. Cotton, isn't it true that you had not performed a forensic examination into a single voting system?

A. That's incorrect.

10:21:09

Q. Which voting systems had you analyzed prayer to that?

A. Antrim County, Michigan, a Dominion 5.5-B system.

Q. Okay. And was your retention there part of an election fraud lawsuit?

A. It was part of the *Bailey v. Antrim County* lawsuit, yes.

10:21:22

Q. What year did you perform that forensic examination?

10:21:27

A. That would have been in 2021, immediately prior to the examination of the systems down here.

Q. And perhaps you misunderstood my question because my question was, prior to the 2020 general election, had you performed an examination and you just told me that examination was performed in 2021?

10:21:40

A. Correct. So I performed the examination of those systems prior to performing the examination on the Maricopa County systems.

10:21:57

Q. Okay. I think we're two trains passing in the night here. Before the 2020 general election occurred in November of 2020 you had never performed a forensic examination of a voting system?

A. That would be correct.

10:22:10

Q. That's correct. Okay. Thank you.

And were you -- in the Antrim County case that you mentioned were you retained by parties who were disputing the accuracy of the results?

A. I was retained by the parties to investigate why there was a vote-flipping situation that had occurred in an Antrim County.

10:22:21

Q. But who actual hired you, which party?

A. It was the plaintiff on that case. So it was the attorneys representing Bailey.

10:22:35



Q. The plaintiff who alleged that there was a vote-flipping problems you called it; correct? 10:22:37

A. Well, the county clerks admitted that there was discrepancy in the vote. The question was how did it happen. And so that was the investigation that I was hired to analyze. 10:22:50

Q. And the plaintiff in that case, rather the plaintiff in that case was convinced that this vote flipping issue had actually caused there could be errors in how the -- how results were report the; is that correct?

A. Well, there were errors in how the -- how the vote results were initially reported and they caught those and they corrected that with a hand count of the ballot. So then the question was, how did that happen on a certified Dominion voting system? 10:23:09

And so that's why I was retained, is to look at that system. The other sid retained an individual by the name of Halderman who also look at that system. 10:23:29

Q. Okay. Now, your declaration you note that you also performed a forensic examination of a voting system in Mesa County, Colorado; is that correct? 10:23:45

A. I believe I said that I had looked at Antrim, the Coffee County Voting System, and some auxiliary information on the Colorado case, yes.

Q. But you didn't actually perform a forensic examination of the Mesa county Colorado voting system; correct? 10:24:05

A. On the Mesa county Colorado system, I did some additional analysis but not a full evaluation. 10:24:08

Q. Okay. Let's talk about could have tee county, georgia. You mentioned that. Isn't it true that you were recently subpoenaed in a case that is pending in federal court due the to your examination of that voting system? 10:24:21

A. That's true.

Q. And the nature of that subpoena arises out of the fact that the examination wasn't officially authorized by any county authorities; is that correct? 10:24:34

A. That is incorrect. The subpoena asks for my information on my knowledge of unauthorized access to the -- to those voting systems which I have none. My access was authorized by the coffee county election official in that case and I was retained by her attorney to examine those systems. 10:24:54

Q. And isn't it true that that particular official was under investigation for having provided you access to the voting system in coffee county?

A. I don't know the full extent of the charges.

Q. But you're aware that there are charges. 10:25:07

A. I am aware that there's an investigation. I don't know what the full nature of that investigation is.

Q. Okay.

Now, you mentioned that you were involved in the forensic examination of the voting system here in Maricopa 10:25:16

County; correct?

10:25:18

A. Correct.

Q. And your company, cipher was retained alongside Cyber Ninjas ink to perform what was labeled an an audit of the 2020 general election here in Maricopa County correct?

10:25:30

A. I was a subcontractor to cybernine gentleman's.

Q. Correct.

Q. Did you understand when you were retained that the audit was a product of the members of Arizona legislature who were questioning the results of the 2020 general election?

10:25:44

A. What I understood was is they were attempting to to validate what happened, if anything happened, and to and look at the integrity of the vote. You know, I did not enter into this as a partisan type effort. I'm not a partisan individual. You know, this is a -- it's not a Democrat issue. It's not a Republican issue. This is an American issue and when you look at 2016 we had half of the voters disenfranchised when President Trump wouldn't and when you look at 2020 we had half of the voters disenfranchised because they thought something was going on when President Biden won.

10:26:12

10:26:39

So, you know, this was really an effort to kind of reenfranchise everyone and say, look, this is an open audit and there's either something here or there's nothing here. If there's something here then we address that and we direct it. You know, it was not a partisan type issue.

10:27:04

BENJAMIN R. COTTON - Cross

MR. GAONA: Your Honor, I want oh move to strike everything the witness said about 50 percent of the voters in 2016 and 2020 being disenfranchised for lack of foundation.

10:27:09

THE COURT: Mr. Parker.

MR. PARKER: Your Honor, I think further inquiry as to what he meant by that would be appropriate.

10:27:20

MR. GAONA: The motion is denied for now. The parties can explore it.

MR. GAONA: Thank you, Your Honor.

BY MR. GAONA:

10:27:42

BY MR. GAONA:

Q. Mr. Cotton, are you a registered voter?

A. I am.

Q. Which state are you registered in?

A. Montana.

10:27:49

Q. Do you know whether Montana -- well, let me back up. How long have you been voting?

A. I object voting since I was 18 years old.

Q. Do you know whether Montana uses an electronic voting system to tabulate votes?

10:28:00

A. They do.

Q. Now, you mentioned as part of your testimony that I think what you said was there were 700 million pieces of malware that you claim Maricopa County's Dominion systems would not have detected because there hadn't been updates performed. Is that

10:28:19

an accurate summary of your testimony there?

10:28:22

A. There's more than that, but yes.

Q. Okay. And to be clear, you found no evidence that any malware had actually infected any of the voting systems in Maricopa County that you examined; correct?

10:28:32

A. I did not find malware present.

Q. You found no evidence that any viruses of I kind had infected the Maricopa County voting systems; correct?

A. I did not find any viruses. I will caveat this with the systems were delivered to me in a turned-off position so, therefore, any memory resident only artifacts I didn't have access to.

10:28:47

Q. Okay. But based on your detailed forensic examination that you did perform you found no evidence either malware or viruses that had infected those systems; correct?

10:29:05

A. Correct.

Q. As you sit here now, Mr. Cotton, you are not aware of any actual malicious third party intrusion into any voting stem in Arizona, are you?

A. Incorrect.

10:29:22

Q. Incorrect?

A. Yes. In the 2020 election there was a breach of the registration server.

Q. He I'm going to stop you there, Mr. Cotton. My question was about the voting system not a voter registration database.

10:29:33

Those are two distinct things. Talking about the voting is there anything else over which you performed a forensics examination, those systems that tabulate and count voters' ballots you are not aware of any malicious third party intrusion into those systems, are you?

A. Okay. I'm going to caveat this with you said --

Q. Mr. Cotton, it's a yes-or-no question.

A. Actually it's not.

Q. It is, Mr. Cotton. You examined the specific set of systems.

MR. PARKER: Your Honor, argumentative.

THE COURT: The objection is overruled.

Mr. Gaona is the master of his question. He can formulate or reformulate the question. He has not gotten an answer yet.

Ask the question again.

Answer the question, yes, no, or it cannot be answered with yes and no.

THE WITNESS: Yes, Your Honor.

BY MR. GAONA:

Q. Let's try this. Let's back up, Mr. Cotton so I can be as clear as possible. You performed a forensic examination on the voting systems utilized by Maricopa County; is that correct?

A. I cannot answer that yes or no.

Q. Why can you not answer that yes or no, Mr. Cotton?

A. Because I examined a subcomponent of the voting system. 10:30:43

Q. So what did you actually -- how would you describe what you actually examined then?

A. Exactly what I defined. I look at the EMS server. I look at the ICCs. I looked at the adjudication systems and I was not allowed to examine the ICPs. I was not allowed to examine because they didn't turn over the poll looks. Any laptops associated with the system because they said that wasn't covered in the scope but there were laptops that were involved in that system. I did not examine the switch or the routing device that you used on that system. I did not examine multiple IP devices that had. I found the IPs inside of the EMS but those were not produced as part of the subpoena. 10:30:54  
10:31:19

Q. And Mr. Cotton, so just to be clear, you've already listed off everything you did examine; correct. Now are you listing off things that you claim you were not provided; correct? 10:31:45

A. But which are part of the stem?

Q. Okay. So let me ask this again. Of the voting system components that you examined, you found no evidence of any malicious, third party intrusion into those systems; is that correct? 10:32:00

A. That is incorrect.

Q. Why is that incorrect?

A. As I testified before the Senate, there is evidence of atypical anonymous log-ins that due to the lack of information 10:32:17

provided, I was not able to resolve. So, therefore, I cannot determine that there was no breach, nor could I determine that there was a breach.

10:32:21

Q. But again as you sit here now, you have no evidence that shows or proves that those anonymous log-ins that you are mentioning were the product of a malicious third-party intrusion into the voting system; correct?

10:32:34

A. I have seen this very same type of activity --

Q. Mr. Cotton, that's not what I asked. The question is a yes-or-no question now. We've gone down this road --

10:32:52

A. Please repeat the question.

Q. I'm trying to elicit a response from you.

Based on the systems that you actually reviewed and despite the fact that there maybe some log-ins that you can't explain, you found no evidence of any actual third party malicious intrusion into Maricopa County's voting systems?

10:33:05

A. I cannot say yes on that question.

Q. Okay.

Your forensic examination of the voting systems used in Arizona was specific only to the Dominion system that is used by Maricopa County; correct?

10:33:24

A. Within the scope of the Senate engagement, yes.

Q. Right. And are you aware that -- do you know whether any other county other Maricopa County uses a similar system to Maricopa?

10:33:43



A. I believe most of the other counties use ESand Ssystems. 10:33:44

Q. So you did not perform any forensic examination into the ESand Ssystems in any other county other than Maricopa correct?

A. Not in Arizona.

Q. As part of your report to the Senate, you originally concluded there was evidence that Maricopa County's voting system had been connected to the Internet; is that correct? 10:34:00

A. That's correct.

Q. And are you aware that the Senate and the county collectively hired former Congressman Shadegg to gather a group of IT experts to examine that claim among others? 10:34:12

A. I'm what irthat he hired a panel of experts, yes.

Q. And are you aware that those experts concluded that you were wrong about your conclusions about those systems having been connected to the Internet? 10:34:29

A. I am aware of that, yes.

Q. Okay: Are you familiar with Congressman Shadegg's party affiliation?

A. I am not.

Q. So you don't know that he was a elected Republican from Arizona, do you? 10:34:38

A. No.

Q. Now, us also originally claimed in providing information to the Arizona Senate that there was evidence that Maricopa County had deleted election files from its system; is that 10:34:50

correct?

10:34:53

A. That's correct.

Q. Didn't you later recant that claim?

A. I did not.

Q. Did you have to clarify what your position on that claim?

10:34:58

A. I provided additional testimony on that, yes.

Q. But the original scope of your claim was incorrect, wasn't it?

A. No.

Q. Why not?

10:35:09

A. Because there were files deleted on the EMS server. There were files deleted off the high pro systems.

Q. What was your clarification that you provided?

A. I provided screen shots of those deleted files and those were part of my testimony before the Arizona Senate.

10:35:26

Q. And I provided dates and times. I also provided a clarification that on the high pro system they had not turned on or enabled the hashing function for the ballot images.

Q. Are you familiar with a group called the truth and liberty coalition?

10:35:56

A. I am not.

MR. GAONA: I don't have any further questions, Your Honor. Thank you.

THE COURT: All right. Thank you, Mr. Gaona.

Mr. Parker, any redirect.

10:36:06

BENJAMIN R. COTTON - Cross

MR. GAONA: I believe Mr. Liddy Dee had.

10:36:07

THE COURT: I'm sorry. Mr. Liddy please.

MR. LIDDY: Thank you, Your Honor.

**CROSS - EXAMINATION**

BY MR. LIDDY:

10:36:16

Q. Mr. Cotton, Tom Liddy from Maricopa County Attorney's Office on behalf of Maricopa County. You had testified here that you had previously testified before the Arizona Senate?

A. That's correct.

Q. Were you placed under oath when you made your presentation to the Arizona Senate?

10:36:28

A. I was not.

Q. So you didn't actually testify to the Senate, did you?

A. I presented.

Q. You presented. Now, did you present to the full body of the Senate?

10:36:36

A. I presented to a committee. That was televised publicly. I don't know who all was watching.

Q. Do you know the name of the committee?

A. I do not.

10:36:50

Q. Do you know how many senators were -- participated in that presentation?

A. On the dais there were two senators is.

Q. Were any of them from the minority of the Arizona State Senate?

10:37:02

A. I do not know.

10:37:02

Q. Did any of the senators question you?

A. Yes.

Q. And were any of the members of the minority question you?

A. I don't recall.

10:37:12

Q. You previously testified today that you had the opportunity, as a subcontractor with Cyber Ninjas, to look at the EMS system that Maricopa County used in the general election of 2020; is that correct?

A. That's correct.

10:37:25

Q. Did you make a duplicate of that EMS -- of the data in that EMS system?

A. I made a forensics image.

Q. A forensic image. And on what system did you place that forensic image?

10:37:36

A. I placed the forensics image on a storage device. That storage device was retained by the U.S. Senate or not Senate. The Arizona State Senate as part of the retention program.

Q. Are there any other copies made of the data that you put on that storage device?

10:37:57

A. Yes.

Q. How many?

A. Under contract I was allowed to produce one copy of that data and I have retained that in a U.S. Government approved GSA safe.

10:38:10

BENJAMIN R. COTTON - Cross

Q. And you -- who gave you permission to retain that copy? 10:38:13

A. The Senate.

Q. The Arizona Senate?

A. Yes.

Q. The full body of the Senate? Did the Senate vote on it? 10:38:20

A. I know that the president of the Senate under the contract that was initiated authorized us to make that copy.

Q. When you say us, did you make the copy or did you correct to made the copy?

A. I made the copy. 10:38:39

Q. You made the copy. And where is that copy today?

A. That copy is stored and my security facility in Montana.

Q. Do you own property in Montana?

A. I do.

Q. There are improvements upon that property? 10:38:48

A. There are.

Q. Is one of the structures on that property something you from time to time refer to as a lab?

A. Yes.

Q. Is that the structure you are referring to when you say it's in there secure? 10:38:56

A. Yes.

Q. And how did you get it from Arizona outside our borders up to Montana?

A. Any received permission from the U.S. Senate -- or the 10:39:05

state Senate to transport that and I personally transported that in my vehicle.

10:39:08

Q. Is your vehicle a pickup truck?

A. It is.

Q. Is it black?

10:39:16

A. No.

MR. PARKER: Objection, Your Honor. Relevance on this line of questioning?

THE COURT: Mr. Liddy, what is the relevance of the details of the transport?

10:39:24

MR. LIDDY: Your Honor, this witness has testified in this proceeding ad nauseam as to his expertise in security protocols. I would like to examine him about the security protocols that he used moving our election data after he duplicated it out of our state into a log cabin in Montana.

10:39:41

THE COURT: The objection is overrule. You may proceed.

BY MR. LIDDY:

Q. So did you drive that pickup truck yourself?

A. I did.

10:39:53

Q. Was there anybody else in there with you?

A. My wife.

Q. Did you make any stops along the way?

A. I did.

Q. Did you leave the vehicle during those stops?

10:39:57

A. I did but the vehicle, if the data was still in the vehicle, there was one person at all times with the vehicle. 10:39:59

Q. At all times?

A. Yes.

Q. Now, you mentioned that you've done some Sentencing Reform Act work for a Lee letter agency that shall not be named; is that correct? 10:40:06

A. That's correct.

Q. And is that somewhere south of the leach unmemorial chain and north of the chain bridge in northern Virginia off the toast of positive to me mat regularly referred to as great false? 10:40:20

A. It would be in the northern Virginia area.

Q. And would the experts with whom you've done deep dives approve of the security protocol that you use in moving that data from your pickup truck from our state up to Montana? 10:40:32

A. Yes.

Q. What are the names of those experts in security up there in languagely that would approve of you moving that with your wife in the pickup truck? 10:40:46

A. Languagely had no involvement with this, period, and I'm not going to bring in something that is irrelevant to this because they had no authorities, node no approvals on this. What I can say is that if you wants to look at the handling of classified information that that is available on the Internet 10:41:07

and and it's known as a hand carry, and, y they would have approved with my security procedures had this been classified information.

10:41:10

Q. You've answered my question. You said they would have approved. Can you give me the names of those federal government experts who would have approved?

10:41:21

A. I am currently working, so I have no point of contact to give you for that.

Q. So when you say they would have approved, you have no one in particular in mind; is that correct?

10:41:35

A. What I am saying is it would have been in accordance with the published procedures?

Q. Has anybody else had access to the data that you copied that is up there in Montana?

A. Only with the approval of the Senate.

10:41:44

Q. May I have the names of the people that have access to it?

A. I would have to produce that. I don't have that with me.

Q. Will you do that for us for all parties?

A. Yes.

Q. Thank you.

10:41:56

MR. LIDDY: Your Honor, I have no further questions.

THE COURT: All right. Thank you, Mr. Liddy.

Now, Mr. Parker, did you have any redirect?

**REDIRECT EXAMINATION**

\\



BY MR. PARKER:

10:42:12

Q. Mr. Cotton, you were asked about Congressman Shadegg's review of the work that you did in his panel. Do you recall that?

A. I do.

10:42:19

Q. Did Congressman Shadegg find that there was anything you did that was wrong or inappropriate?

A. No. Their findings were incorrect; but other than that, he found no objection to the procedures or my examination techniques.

10:42:46

Q. How were there findings incorrect?

A. Well, first and foremost, I don't know what they examined from an EMS perspective to determine that there was no Internet access. I know that under the contract that was signed by Maricopa County, there were actually two EMS servers. I don't know which server they looked at. That's not itemized in the report. I don't know what the basis for his findings were.

10:43:03

What I do know is that when the report came out I reran my findings and I'm confident in my findings of the instances where there was Internet access.

10:43:23

Q. So you are here to testify and swear to the fact that your findings are not changing and that you have rechecked and that they are accurate as it relates to connectivity?

A. That is correct, and also there was a previous mention of that they couldn't find the log-rolling activity and rechecked

10:43:42

all of that as well.

10:43:48

And on the images that I preserved and are still forensically preserved, that data is still there.

THE COURT: I'm sorry, Mr. Parker. You're going to have to clarify that for me, the phrase log-rolling activity. I'm not familiar with that.

10:43:57

THE WITNESS: So rolling the logs, Your Honor, is the act of an individual whether authorized or unauthorized of performing an action that essentially clears the logs out. Then is called rolling the logs in hacker vernacular.

10:44:13

THE COURT: Thank you.

BY MR. PARKER:

Q. So logs remain in the system for a period of time and they could be overwritten if activity overwrites -- reaches a certain point that overwrites previous logs?

10:44:26

A. Correct.

Q. All right.

Turning your attention now to the questioning that that you just shared from the defense regarding trying to differentiate between your expertise on computer systems and your expertise on electronic voting computer systems. Is there something unique about electronic voting computer systems that makes your expertise about cybersecurity and computer systems inapplicable?

10:44:41

A. No. Quite the opposite. In the case of the Dominion

10:45:03

voting system, for any authentication into the SQL server which was used to store all the voting data, all of the results, all of those things, they were using what is known as a user mode access. So they were using the Windows user account to grant access into the very heart of the voting system. 10:45:06  
10:45:27

So if you have one of those shared passwords and one of those user names, you could get literally right into where the votes were recorded, tabulated and you could edit those votes.

Q. It appears the defense is taking the position that because the Arizona voting system has not been entirely hacked and decimated to your knowledge that it must not have happened. Can hacks or malware occur undetected in computer voting computer systems? 10:45:49

A. They can especially if you don't have a good monitoring function in that network. And Maricopa County had a zero monitoring function on the network and on the end points. 10:46:09

Q. They had a zero monitoring function. What does that mean?

A. It means they had none. So any -- you know, it's recommended by CISA that you have end-point monitoring and baseline monitoring so you can alert if any program is executed that is not part of your approved baseline. They also recommend that you have a network monitoring protocol so that you can determine whether additional devices are add to do that network. Even an air gap network can be easily bypassed. 10:46:27  
10:46:48

In this particular case there was no monitoring.  
There was zero collection of network traffic. There was just no way they would have ever detected that if it had been a memory resident piece of malware.

10:46:53

Q. In terms of undetectability of malicious intrusion, are you familiar that see is a itself had an undetected malicious intrusion that they didn't know about for ten months just in the last short while?

10:47:08

A. I'm not aware of that and I'm not apprized.

MR. GAONA: Objection as to foundation and relevance.

10:47:29

MR. PARKER: Your Honor, the undetect ability issue is of central importance to this case. This is just an example at the highest levels of the U.S. Government where undetectable malware has been discovered and existed for ten months before it was discovered.

10:47:50

THE COURT: In a system having nothing to do with Arizona's EMS. The objection is sustained. That's a point for argument, Mr. Parker.

BY MR. PARKER:

Q. Can computers be invaded by malicious attack without the users' owners knowing about it?

10:48:03

A. I would redefine invaded. I would say infected but yes.

Q. Now, you made the reference to 50 percent being disenfranchised in one election and 50 percent being disenfranchised in the other election. Are you telling that 50

10:48:47

percent of Americans were disenfranchised during either of these elections or are you referring to how they may feel?

10:48:49

A. I'm referring to how they may feel.

Q. So you're not asserting that they were disenfranchised?

A. No.

10:49:01

MR. PARKER: Nothing further, Your Honor.

THE COURT: All right. Mr. Parker, thank you.

May the witness be excused.

Mr. Parker, may the witness be used?

MR. PARKER: Yes, Your Honor.

10:49:19

THE COURT: Mr. Gaona.

MR. GAONA: Yes, Your Honor.

THE COURT: And Mr. Liddy, may the witness be excused?

MR. LIDDY: Yes, sir.

10:49:25

THE COURT: All right. You may step down, sir.

And please call your next witness, Mr. Parker, for purposes of planning, I'm going to go at least another ten maybe 15 minutes and then we'll take a brief morning break.

MR. PARKER: Thank you, Your Honor.

10:49:37

Plaintiffs call Doug Logan.

THE COURT: All right. Mr. Logan if you'll step up to my courtroom deputy's station, she'll swear you in.

COURTROOM DEPUTY: Can you please state your name and spell your last name for the record?

10:50:01

DOUGLAS J. LOGAN - Direct

THE WITNESS: Douglas J. Logan. L-O-G-A-N.

10:50:03

COURTROOM DEPUTY: Raise your right hand.

(DOUGLAS J. LOGAN, a witness herein, was duly sworn or affirmed.)

THE COURT: All right, sir. Mr. Logan, you may remove your maks or not as you a comfortable.

10:50:24

THE WITNESS: Thank you.

**DIRECT EXAMINATION**

BY MR. PARKER:

Q. Please state your name for the record.

10:50:33

A. Douglas J. Logan, L-O-G-A-N.

Q. Describe for the Court your experience with cybersecurity.

A. So I have over 20 years of experience in general IT and ten years of experience specifically in the area of cybersecurity. My specialty is in the area of application security.

10:50:49

Q. Have you worked with any private sector organizations and their cybersecurity area?

A. Yes, sir. I've worked with fortune 100 companies including Bank of America and JPMorgan Chase as well as the federal government.

10:51:00

Q. What did you do four them?

A. Which one?

Q. Start at the beginning.

A. So with Fortune 100 company, we -- we've done penetration

10:51:10

United States District Court

testing. We've done malicious code detection. We've done threat modeling.

10:51:15

Q. And when you say "we," are you talking about you or someone else?

A. Me personally. I've done that work, correct, in my company, Cyber Ninjas.

10:51:30

Q. Go ahead. Why don't you start with JPMorgan? What did you do for them? Were you a contract or what was the work?

A. So at the time I worked for a company called Sigital and we had -- I was the technical lead that set up the Sigital assessment center that did all of the vulnerability assessments for all JPMorgan Chase's application and I established and built that program, trained staff, originally we were -- had about ten assessments a month. Quickly moved up to 100 and were eventually doing over 200 assessments a month for JPMorgan chase and similar clients.

10:51:49

10:52:08

Q. And what about your work with the other private sector companies you referred to. What was your title and what work did you do?

A. So I was a CO of Cyber Ninjas at the time and we did malicious code detection for Fortune 100 company and that is when we go take a look at source code to see if there's any intentionally malicious code add to do it for the -- for various reactions.

10:52:23

Q. And you said that you worked for the Government?

10:52:41

A. Yes, sir.

10:52:44

Q. Describe federal Government or state.

A. Federal Government. So a federal agency brought me in to do an evaluation of the security posture of the federal agency. It was rich fully designed to be a 90-day engagement in the first two weeks of that worked. The CSO actually stepped down and left. So for the course of roughly the next two years, I was the lead security advisor for the CIO and helped put together the cybersecurity plan for monitoring and moving everything to the Cloud.

10:52:55

10:53:13

Q. And have you looked at -- well, how would you describe the relationship between cybersecurity analysis of computer systems and cybersecurity analysis of voting election machine computer systems?

A. It's absolutely exactly the same. The only difference -- I mean, it's just like any other computer system with a complex application on it. And I have tested thousands of applications either with oversight or directly and we have worked with a number of complicated systems.

10:53:33

Q. You say you've done thousands of software applications vulnerability assessments?

10:53:50

A. Yes, sir. I have overseen or performed over 2000 application assessments that includes both Web applications, mobile publics, embedded systems.

Q. And in your work have you received security clearances.

10:54:06



A. Yes, sir.

10:54:16

Q. I want to turn your attention to knowledge regarding the Arizona system. Now, you have provided a declaration in this case along with supportment do you stand by that declaration and the statements you made in there?

10:54:32

A. Yes, sir.

Q. All of them are accurate?

A. Yes, sir.

Q. Describe what you found in the Arizona computer system when you analyzed it, in terms of security vulnerabilities?

10:54:43

A. So a lot of these were already cuffed by Mr. Cotton.

MR. GAONA: Excuse me, Your Honor. I just wanted to note, again, a standing objection to any purported expert testimony by Mr. Logan on these issues consistent with our *Daubert* motion that son file and pending. Thank you.

10:55:00

THE COURT: Based on the possession as well as a footnote in your response to the pending motion, the Court notes that the standing objection applies to all of the experts that plaintiff would call and you don't need to interpose it again.

10:55:18

MR. GAONA: Thank you, Your Honor.

THE COURT: Thank you.

Please proceed. I'm sorry.

MR. PARKER: Thank you, Your Honor.

\\

BY MR. PARKER:

10:55:25

Q. So turn to go Arizona, you said that the vulnerabilities that Mr. Cotton found, do you confirm those findings that he made?

A. Yes, sir. And I do want to further illustrate I believe this point was brought up before. But the password was something that was weak that could easily brute force within a short period of time. Would it take less than an hour, most likely within the first five to ten minutes would find it.

10:55:37

Q. You would find what?

10:55:55

A. Would discover what the password is if are you brute force and it was just a way to I'll truss straight how poor the password was that was used across the board.

Q. What are the various ways that someone who had malicious intent might be able to get access, remote access to the Arizona voting system based upon your review?

10:56:15

A. So probably one of the weakest points is it would be via USB that could inject malware into the system and there's a number of different ways that could happen. We've seen in other supply chains where China has actually intercepted hardware on it's way into say shipping into a logistics company and replaced it with malware. For example, if you had a USB keyboard that was being shipped and brought in and utilized within the air-gapped network, it would immediately be penetrated.

10:56:36

10:56:54

Really, to look at the all of the places that could be changed, you would have to follow the entire flow. The entire flow of the election system.

10:56:55

Q. Now, are you aware that it's system was EAC certified?

A. Yes, sir.

10:57:08

Q. Are you familiar with the EAC?

A. I am familiar with some of it, yes.

Q. And what is your background and knowledge regarding certification of electronic voting systems?

A. Based on what I've seen of the systems that are gone through EAC certification, they would not meet any cybersecurity standard that is established in any other domain or any other industry of our country.

10:57:18

Q. And when you say domain or industry, are you talking about HIPAA or other such?

10:57:33

A. Yes. PCI, HIPAA, FISMA, they don't meet the standards of CIS benchmarks, which are a standard way of hardening systems. They don't fit -- they don't meet STIGS, S-T-I-G-S. It's DOD standard for hardening systems. In fact, there was no indication of hardening in on the systems.

10:57:56

Q. In terms of EAC certification, if a system, an electronic voting system gets EAC certification, are they -- does that mean that they have all necessary security in place?

A. Oh, absolutely not.

Q. So standards that EAC applies certification to may not

10:58:15

mean that hardened security has occurred?

10:58:22

A. I would actually say the opposite. I would say some of the standards that EAC applies actually requires obsolescence of various different formats and there's ways around it. They can submit *di minimis* changes in order to, say, do virus scan updates, so there's ways around it. But by design, the EAC basically forces obsolescence.

10:58:35

Q. What do you mean by forcing obsolescence. When you put restrictions on when and how you can apply things like patches and virus scans that would impact a system I think as Mr. Cotton testified, that none of those were updated since 2019. And the argument from the county and others is that that is because of EAC requirements. But that in itself creates a vulnerable system.

10:59:00

Q. Have you ever in your experience in working with in the private sector or the public sector seen any supply chain issues or problems arise with components?

10:59:20

A. Yes. It's well -- it's well reported in the media and well documented the number of supply chain attacks have continued to happen. Specifically, China is well-known for those type of engagements.

10:59:42

Q. Did you receive all of the information that you needed in order to analyze the Maricopa system?

A. We did not receive everything that had been requested that would have been useful to come with conclusive results but I

11:00:10

will defer to Mr. Cotton's expertise more along that line.

11:00:14

Q. In terms of your review of the protective measures that Maricopa County had when you reviewed their voting system, setting aside EAC for a minute, are you familiar with the logic and accuracy testing that they did?

11:00:37

A. Yes, sir.

Q. And do you know what that is?

A. Yes, sir.

Q. And did you review what it was that they did and determine whether or not that provides any safeguard?

11:00:47

A. I think one of the most significant problems with logic and accuracy testing is the test deck is usually less than 100 ballots and just in Maricopa County as an example, there are thousands of different ballot types so there's no way for you to even test one of each ballot type that is utilized in an election. From my experience with working application security and specifically with development teams, there's no way to ensure there aren't problems or bugs without testing every single case. Then would normally require every iteration of a ballot, not just -- you know every single iteration of what choice would be chosen, not just every single ballot.

11:01:05

11:01:22

So it's woefully insufficient to test a few ballots in logic and accuracy testing, and that is further proven by Williamson County, Tennessee, went through logic and actually testing and they found a large number of ballots that had been

11:01:40

completely skipped the end. And the only reason it was actually identified was because there was a pool pork worker that was keeping track of how many people went to a given voting machine and when they got to the end of night totals he said it didn't match up.

11:01:43

11:01:58

Q. What electronic voting systems have you reviewed or analyzed?

A. So I've reviewed the system in Antrim Michigan. I've also reviewed a system in a county in Georgia in addition to the Maricopa County systems.

11:02:13

Q. Thank you, Mr. Logan.

THE COURT: All right. Thank you, Mr. Parker.

Let's go ahead and take our break now for -- we'll break until 11:15 and then we'll go another hour before the lunch break. All right.

11:02:32

Mr. Logan, if you are able to return to the stand just a minute before 11:15, it gives us a minute for setting?

THE WITNESS: Yes, sir.

THE COURT: Thank you. And I am going to stay.

(Recess at 11:03; resumed at 11:11.)

11:03:14

THE COURT: Thank you, everyone. Please be seated.

Mr. Logan, thank you for returning.

Mr. Gaona, whenever you're ready, sir.

MR. GAONA: Thank you, Your Honor.

**CROSS - EXAMINATION**

11:18:33

BY MR. GAONA:

Q. Good morning, Mr. Logan. Thank you for being here today.

Are you being paid for your work on this case?

A. Yes.

11:18:39

Q. How much?

A. It's not done yet.

Q. All right. Well, let's get there. Have you been paid anything to date?

A. No, sir.

11:18:45

Q. Have you billed anything so far?

A. No, sir.

Q. What's your hourly rate for your work on this case, Mr. Logan?

A. \$225 for prep work and \$325 for work in court.

11:18:52

Q. And what's your best estimate of how many hours you spent working on this case.

A. Somewhere around 80 hours.

Q. Who is paying your bill?

A. The law firm.

11:19:05

Q. Your declaration that you submit in this case caulked about how you evaluated as you put it Dominion voting machine deployments in Antrim, Michigan; Maricopa County, Arizona; and Georgia; is that right?

A. Yes, sir.

11:19:22

Q. And all of those evaluations you've completed occurred after the 2020 general election; is that correct? 11:19:28

A. Yes, sir.

Q. So prior to the results of the 2020 general election, you had never examined a voting system deployment of any kind before. Is that accurate? 11:19:39

A. I have examined things of similar complexity but no I have not examined a voting stem.

Q. Okay.

You used to have a Twitter account; is that right, Mr. Logan? 11:19:55

A. Yes, sir.

Q. You've since deleted it; is that right?

A. Yes, sir.

Q. Now, before you were retained to perform these evaluations of voting systems in the jurisdictions I just mentioned, you tweeted out your only personal belief that the 2020 presidential election was rigged against former President Trump; is that correct? 11:20:01

A. I'm not sure if those are exactly the words I used. Can you be more specific on what tweet you're reference. 11:20:18

Q. Okay. Sure. Do you remember tweeting using the hashtag stop the steal?

A. No, sir, I don't recall it.

Q. Would you be surprised to learn that you did tweet out 11:20:30



using the hashtag stop the steal?

11:20:32

A. It's not impossible.

Q. Okay. Do you recall ever retweeting a claim that, quote, Trump got 200K more votes than previously reported in Arizona?

A. I do not recall that.

11:20:45

Q. Does that sound familiar to you at all?

A. Honestly, not really.

Q. Do you recall ever making a claim like that in any way?

A. No, sir.

Q. Do you believe that -- I'm sorry. Let me rephrase that. You believe that President Trump actually won the 2020 general election, don't you? Yes or no, Mr. Logan?

11:20:55

A. It's not a yes-or-no question.

Q. I'm confused about how it can't be a yes-or-no question.

Do you believe that president Joe Biden is the duly elected president of the United States of America. Let's try it that way?

11:21:12

A. Yes, sir. I do. But I also think that there are some questions that need to be answered about what happened and potential as we go forward on things.

11:21:25

So there's -- I don't think it's clear exactly what happened. It's clear what the process is. It's clear where we are.

Q. Sir, are you now claiming you don't have a personal belief about whether or not President Trump actually won the 2020

11:21:37

general election?

11:21:41

A. I think the most compelling evidence that it's possible came from "2000 Mules" but up until the point where I saw that, no, I didn't have belief.

Q. You mentioned "2000 Mules." That's a movie that was produced by Dinesh D'Souza; is that correct?

11:21:53

A. Yes, sir.

Q. Mr. D'Souza was convicted of a felony just a couple years ago; isn't that correct?

MR. PARKER: Objection, Your Honor, as to the relevance of this line of questioning. This not because --

11:22:05

THE COURT: I'm going to sustain the objection. Mr. D'Souza's status while known to the Court is not relevant to the questioning of this witness and whether or not you're sussing out potential bias says or otherwise.

11:22:17

MR. GAONA: Fair enough, thank you, Your Honor.

BY MR. GAONA:

Q. Mr. Logan, you authored a document that was posted on the website of attorney Sidney Powell that was titled election fraud facts and details; is that right?

11:22:28

A. Yes, sir.

Q. And you intended that that document be used by United States senators who planned to object to the certification of electoral 11 votes on January 6, 2021; is that correct?

A. Every angle item in that document references primary

11:22:45

source information such as SEC--

11:22:48

Q. That wasn't my question. My question was, did you intend for that document to be used by United States senators in their objections to the certification of electoral votes on January 6, 2021? Yes or no?

11:23:01

A. I intended to get the evidence into the record, yes.

Q. Now, I want to talk a little bit about the audit as it was called of Maricopa County's 2020 general election results. Your company Cyber Ninjas was contracted by Arizona -- by the president of the Arizona Senate to perform that review; is that correct?

11:23:22

A. Yes, sir.

Q. And that audit, the audit, the review, one of the components of that was to include a hand count of all of the ballots that had been cast in Maricopa County in 2020; is that correct?

11:23:36

A. Yes, sir.

Q. Prior to being contracted to perform that hand count, had you ever performed an election audit of any kind before?

A. I had performed audit work in Antrim, Michigan supporting that case. I had done an expert witness analysis as part of that case. But a full audit, no, I nod. However, members of mirror team had done audits and hand recounts in two different locations.

11:23:51

Q. But you personally had never been involved in a full hand

11:24:07

count of an election; is that correct?

11:24:09

A. Me personally?

Q. You personally.

A. No.

Q. To be clear, you were the head contractor for the Arizona Senate; is that correct?

11:24:17

A. Yes, sir.

Q. And you then subcontracted by other vendors; correct?

A. Yes, sir.

Q. Now, when you team performed a hand count of all of the ballots cast in Maricopa County, how many races did you actually look at?

11:24:26

A. We looked at the presidential and the Senate race.

Q. Do you have any sense of how many other races were on all of the various ballot styles in Maricopa County in 2020?

11:24:40

A. There was quite a few of them. I would say, what, more than 30.

Q. But you didn't count any of those other ones; correct?

A. Yes, sir. We did not hand count any others.

Q. Before you began the hand count of all of the ballots that were cast in Maricopa County, did you provide an estimate of about how long you thought that was going to take?

11:24:54

A. Yes, sir.

Q. What was your estimate originally?

A. I don't recall exactly offhand but it was somewhere around

11:25:06

a month.

11:25:08

Q. Okay. And your team performed the hand count. How many people were involved in the hand count process?

A. Roughly 2000.

Q. Do you have any estimate as to the number of hours of work that those two,000 individuals performed in order to perform the hand count on just those two races? 11:25:24

A. Just be clear, our work and our scope was wider than just a hand count. There was a lot of other things that we did those people were involved in so we're not just talking about hand count here. There was a lot of paper examination and other actions like that. 11:25:39

Q. Is there any way you can estimate the number of hours that those 2000 people spent on just the hasn't count?

A. I do not have that number in front of me but we -- I believe we've had that information public in the past before. 11:25:50

Q. Would you say it was tens of thousands collectively of man-hours that were spent on the hand count alower end of the range? Would that be accurate?

A. I really wouldn't want to just guess on the spot. 11:26:03

Q. Okay. So to cut to the chase, your hand count of those two races couldn't filled that President Biden in fact received more votes than former President Trump in Maricopa County; is that correct?

A. There were some minor differences in it. We I think 11:26:19

actually technically found that the Biden had a little bit more votes based on our hand count. 11:26:22

Q. So your review revealed that President Trump actually lost by more votes in Maricopa County than the county had originally reported; correct? 11:26:33

A. Based on the hand count data.

Q. Now, how long did the hand count process end up actually taking after you had originally estimated that it would take one month approximately?

A. It depends how you actually quantify that. The actual hand count the majority of it was all done in about two and a half oh or three months but there was a lot of quality control work we did make sure those numbers were accurate that went on for a longer period of time. 11:26:52

Q. So it took two or three times the original estimate that you had made in order to actually finish the -- just the hand count itself, 91 of the other ancillary tasks you just mentioned; right? 11:27:06

A. Yes, sir.

Q. Okay. Now, you in your declaration and here today you've talked a lot about security and I want to talk about that just for a minute. Isn't it true that before the hand count in Maricopa County got under way, a reporter was able to enter the audit site without permission and was able to approach voted ballots and voting equipment without anyone stopping him? 11:27:16 11:27:32

A. No, sir, that is not correct.

11:27:36

Q. A reporter did not get in there and it wasn't on the news here in town.

A. The individuals that had access to the audit was before the ballots and the equipment arrived. Once the ballots and equipment arrived, we had stationed guards physically in front of the equipment at all times.

11:27:43

So there was no way for anyone to get anywhere close to the actual materials?

Q. Okay. Mr. Logan, Cyber Ninjas is a party to public records litigation arising out of the audit that's currently pending here in Maricopa County Superior Court; is that right?

11:27:58

A. Yes, sir.

Q. And Cyber Ninjas has been ordered to turn over various records to the plaintiffs in those cases; is that correct?

11:28:15

A. Yes, sir.

Q. Now, earlier this year, a Maricopa County Superior Court judge held Cyber Ninjas in contempt for its failure to abide by its orders to turn over those records; is that correct?

MR. PARKER: Objection, Your Honor, as to the relevance of this to this case?

11:28:30

THE COURT: One moment, please, I want to reread the question.

Mr. Gaona, relevance?

MR. GAONA: Your Honor, this goes to bias and

11:28:49

credibility. The fact of the matter is, Cyber Ninjas is the subject of a contempt order under which it's being fined \$50,000 a day by a judicial officer right down the street here. I think that goes directly to Mr. Logan's credibility, the correct of his company and the reliability and accuracy of the report that his company ultimately produced.

11:28:51

11:29:02

THE COURT: Depending on his answers to the questions so I will allow you to finish out the -- that line. The objection is overruled.

Do you need the question read back Mr. Logan?

11:29:17

THE WITNESS: Yes. Please.

BY MR. GAONA:

Q. Sure. Mr. Logan, my question was.

THE COURT: Excuse me, Mr. Gaona. When we do that, we go back to the original source, as formulated.

11:29:25

MR. GAONA: Gotcha. Thank you, Your Honor.

(Question was read.)

THE WITNESS: Yes, that is correct but we file the motion to recuse that judge based on bias.

BY MR. GAONA:

11:29:55

Q. But, Mr. Logan, it was a yes-or-no question. We didn't need further elaboration about your beliefs about the propriety of the order. The fact is that Cyber Ninjas is current the subject of a contempt order in Maricopa County Superior Court; is that correct?

11:30:05



A. Yes, sir. 11:30:06

Q. And, again, that's arising out of the Cyber Ninjas failure to comply with the court's orders correct?

A. We did not have the capability to execute what the Court was asking us to do. 11:30:14

Q. Under that contempt order, Mr. Logan, Cyber Ninjas is currently subject to a fine of \$have 50,000 per day; is that correct?

A. No, sir.

Q. It's 0 correct? 11:30:23

A. It's only correct up to the point where I didn't comply and I object complying.

Q. Has the court said that you are in compliance with its order yet?

A. I don't know there's been official ruling. There's been no further motions otherwise. 11:30:33

Q. You're still actively producing public records, aren't you?

A. We're still actively producing records.

Q. Okay. Do you have any sense of what the accrued contempt fine is at this point in time? 11:30:42

A. No, sir.

MR. PARKER: Your Honor, I renew my relevance objection.

MR. GAONA: I'll withdraw it, Your Honor. 11:30:53

BY MR. GAONA:

11:30:56

Q. Mr. Logan, your audit of Maricopa County's general election results and its -- and voting equipment, threw that process, you didn't find any evidence of actual malicious third-party intrusion into Maricopa County's voting systems, did you?

11:31:11

A. Can you please repeat the question?

Q. Sure. Through your audit of Maricopa County's general election results and the voting systems, you uncovered no evidence of any actual third party malicious intrusion into Maricopa County's voting system, did you?

11:31:27

A. I don't believe I can answer this yes or no.

Q. Why not?

A. I think you are misusing the word evidence. If you walk down the street and you see a casing for a gun that has been fired, is evidence but a crime may or may not have occurred. So there are things that we've gone over in our test here and before that could be indicated as evidence. We did not find proof but that's a different thing than evidence.

11:31:44

Q. Sure. I understand that that dysfunction, Mr. Logan and let me just rephrase it and maybe we can get there.

11:32:02

You found no direct evidence that there was any actual malicious third-party intrusion into Maricopa County's voting systems?

A. We found no direct proof.

11:32:14

Q. Okay.

11:32:16

Is Cyber Ninjas a vendor that has been certified by the EAC?

A. No, sir.

MR. GAONA: No further questions, Your Honor. I believe Mr. LaRue may have a couple.

11:32:39

**CROSS - EXAMINATION**

BY MR. LARUE:

Q. Good morning, Mr. Logan.

A. Good morning.

11:32:52

Q. Thank you for being here today. We appreciate your attendance.

I want to be sure that you testified to this. I am not certain if Mr. Gaona already asked you. But can you state for the record how long it actually took Cyber Ninjas to perform the hand count of the two races on Maricopa County's ballots?

11:33:06

A. So as stated beforehand, there was more than just hand counting but we started handled counting in middle of April and we finished with the delivery of the report that was, what, September 22.

11:33:24

Q. Okay. Thank you.

Now, you testified earlier that you did not receive everything that was requested in order to allow you to do your review of Maricopa County's materials. I assume by that was

11:33:38

requested you meant that was requested in the subpoena; is that correct? 11:33:43

A. Yes, sir.

Q. Okay. Do you know who issued that subpoena?

A. It was the judicial committee of the Arizona Senate. 11:33:52

Q. Do you know whether a Senate President Fann also signed that subpoena?

A. I believe so. That makes logical sense to me.

Q. And Senate President Fann is the one who retains Cyber Ninjas to perform the review; is that correct? 11:34:06

A. Yes, sir.

Q. Okay. Are you aware that Senate pretty Fann actually sent a letter to Maricopa County saying that the county was in full compliance with the subpoena?

A. As part of the settlement agreement, yes. 11:34:19

Q. Okay. Did Cyber Ninjas or any of your subcontractors use shared passwords during the review?

A. Yes, sir.

Q. Were you -- there was testimony earlier by Mr. Cotton and perhaps by you that you were not provided the administrative passwords that Dominion uses for the ICPTwos; is that correct? 11:34:40

A. That is correct.

Q. Okay. Were you able to bypass those passwords and look at the ICP2s?

A. That would be a question to your Mr. Cotton. 11:34:58

Q. Okay. Do you know how many ballots are tested in Maricopa County -- hem radio rephrase. I'm sorry. 11:35:00

Do you know how many ballots were tested in Maricopa County during the full logic and accuracy tests that were performed prior to the 2020 election? 11:35:17

A. I do not know the precise number but I do know what is normal.

Q. What is normal?

A. It's usually less than 100.

Q. Usually less than 100. And when you say that, what do you mean normal. Do you mean normal for Maricopa County or do you mean that's an *v. standard*? 11:35:30

A. That is what is typically done with logic and action testing based on me talking with election officials in multiple different jurisdictions. 11:35:45

Q. Okay. Thank you.

Do you have an understanding as to who is better at counting and adding massive amounts of things? Is it humans or computers?

A. If everything works properly, computers are better at it but I think there's an adage that says it's human to error. It's takes a computer to really mess things up. 11:36:00

Q. Okay. Thank you, Mr. Logan.

When you performed the hand count of Maricopa County's ballots, is it true that that the people performing 11:36:17

that hand count kept tally sheets of the count as they went.

11:36:21

Yes, sir.

Q. Okay. Do you still have those tally sheets?

A. Yes, sir, we do.

Q. Could the parties to this case all get copies of those tally sheets?

11:36:32

THE WITNESS: The Senate already has them. You are welcome to request them. They have digital copies but do you want the physical ones.

MR. LARUE: I just would like digital copies and if possible I would like them from you the actual source but not just for me but for all the parties.

11:36:44

MR. PARKER: Your Honor, I don't think this is appropriate for an preliminary injunction hearing to be requesting discovery.

11:36:55

THE COURT: Yeah. Mr. LaRue, I'm going to ask you to take disup with counsel when we're not on the clock for the evincing of evidence today.

MR. LARUE: Yes, sir. Your Honor. The only thing I would say, Your Honor, the tally sheets reveal the actual hand count that they performed, not the final aggregate but how they got there and that is relevant as to whether a hand count of ballots, what's involved in that, how many errors are made, when hand counts are performed by humans and whether it's reliable if the Court were to order the relief that the

11:37:09

11:37:29

plaintiffs request.

11:37:34

THE COURT: Right. I understand the potential usefulness in proving a point or fashioning a way forward.

My point is, you're not going to get them right now and that's what we're here for is for the aduesing of evidence.

11:37:44

MR. LARUE: Thank you, Your Honor.

And that's all the questions I have. Mr. Logan. Again, thank you.

THE COURT: Thank you, Mr. LaRue.

Mr. Parker, any redirect?

11:37:58

**REDIRECT EXAMINATION**

BY MR. PARKER:

Q. Mr. Logan, you were asked about the hand counts that you did. And how many how many ballots did you count?

A. About 2.1 million.

11:38:22

Q. All at once kind of in central location?

A. Yes. And the complexity increases quite a bit. I would say exponentially the more ballots that you count.

Q. If you counted the ballots, say, per precinct with people in that precinct and let's say there were three, 4,000 votes or ballots, do you think it could go faster than a month or two months or three months?

11:38:42

MR. GAONA: Objection, Your Honor. Foundation.

THE COURT: Hang on just a second, please.

No, the objection is overrecall. The witness can

11:39:04

answer based on this knowledge.

11:39:07

THE WITNESS: Yes, sir, absolutely. We found on average that one counting table could handle roughly 1,500 per a four-hour shift. We had peaks there were as high as almost 4,000 and, I mean, that was -- yeah.

11:39:22

BY MR. PARKER:

Q. So if you had an election and you had people from both parties at a table, if you did it by precinct, without taking one, two, or three months?

A. Oh, absolutely.

11:39:44

Q. Now, I want to ask you the same question I asked Mr. Cotton. You were asked about the fact that you didn't find direct evidence of malicious intrusion following your analysis that you did that Mr. Cotton was a part of. Can there be malicious intrusion into Electronic Voting Systems or into a computer system generally that occur without detection?

11:40:11

A. Yes, absolutely of the average time to notice a breach is somewhere around ten months and even once its found it takes 90 days or I should say it's somewhere between 60 and 90 days to actually contain it.

11:40:30

And it's possible for it to go undetected altogether that we only know what we found.

Q. And what do you base that information on? What experience do you have to be able to testify to this court about that undetectability?

11:40:44



A. Those are well-known stats that in my field you know? 11:40:46

Q. And when you say in your filed is that based on the work did you in the private sector and for the Government?

A. Yes, sir.

Q. Now, you were asked the question whether you were doing your work in Maricopa County whether you shared passwords amongst your team when you were doing your work and I think you said you did? 11:41:12

A. Correct. We had a couple supervisors that had access to a password list that allowed them to log in to certain machines. 11:41:29

Q. Why is that okay but you're asserting that it's not okay that Maricopa County have shared single passwords for years without changing them?

A. Well, there's a very big difference between the two. We were conducting an audit. We were not doing a recount that had any binding impact. We were helping serve a legislative function for the Arizona Senate to determine about possible legislative reform. If we had come and said the results were different, it would not have been binding. It wouldn't have done anything besides trigger other investigations. The point was to see what was working to help with legislative reform. 11:41:51 11:42:08

Q. Yeah, but what about the protocol of shared passwords. I mean whatever it was that you were doing, why is it okay for you to share passwords, not okay for Maricopa County to share passwords and have a single password for years? 11:42:29

A. Well, any cybersecurity standards need to be applied appropriately to the sensitivity of the systems being utilized. In the case of something that is the official tally and official vote, a very high standard needs to be applied to it. And in the case of a machine that's used to scan images for the course of audit work it's not as big a concern. You don't just go by buy the very expensive tool and apply to it protect nothing. You use the expensive tools and the heightened things for heightened sensitive systems. 11:42:32 11:42:44

Speaking of the heightened sensitive systems, the EMS server is the brains of the whole system, isn't it? 11:43:02

A. Yes, sir.

Q. And are you familiar with Microsoft SQL, SGL?

A. Yes, sir, I am.

Q. Is that part of this brains EMS systems? 11:43:20

A. Microsoft SQL is the database Burt also specifically Microsoft SQL management tools was installed on the EMS server and that allows you to directly go in and edit the database and just to reiterate something that Mr. Cotton referenced, the Microsoft SQL server was configured with Windows authentication. That means that if you have the administrative password and anyone that had a password had administrative password because it was the same thing, then you had the capability to log into the database and to change everything in that database. And had includes voting results. 11:43:40 11:43:56

Q. And that's going to be the same system that Maricopa County uses in 2022 with that same configuration? 11:44:01

A. Yes, sir.

MR. PARKER: Nothing further.

THE COURT: All right. Thank you. As I will do from now on, I'll ask each of the examining attorneys whether the witness may be excused. 11:44:16

Mr. Parker.

MR. PARKER: Yes, Your Honor, thank you.

THE COURT: Mr. Gaona. 11:44:25

MR. GAONA: Yes, Your Honor.

THE COURT: Mr. LaRue.

MR. LARUE: Yes, Your Honor.

THE COURT: All right. Thank you. Mr., you may step down. 11:44:32

THE WITNESS: Thank you.

(Witness excused.)

THE COURT: Mr. Parker, you may call your next witness.

MR. PARKER: Thank you, Your Honor. The plaintiffs call John Mills. 11:44:37

THE COURT: Mr. Mills, if you would step forward to my courtroom deputy, she'll swear you in.

COURTROOM DEPUTY: If you can please state your name and spell your last name for the record. 11:44:53

THE WITNESS: John R Mills. M-I-L-L-S.

11:44:54

(JOHN R. MILLS, a witness herein, was duly sworn or affirmed.)

COURTROOM DEPUTY: Thank you. You can have a seat right up there.

11:45:17

**DIRECT EXAMINATION**

BY MR. PARKER:

Q. Thank you. Please state your name for the record. John Robert Mills.

Q. And Mr. Mills, describe your experience in cybersecurity police for the Court.

11:45:28

A. Okay. From 2004 until 2018 I was in the office of the Secretary of defense, culminating as being the director of cybersecurity policy strategy and international affairs for the entire Department of Defense.

11:45:49

Q. And so do you have background in I don't remember work for the Department of Defense then related to cybersecurity? You obviously do but can you describe what it is?

A. I'll break that up into three major components. First of all, over that time I had to review many perhaps even hundreds of breaches of a variety of systems and would have to review detailed technical reports to come up with findings and actual recommendations for remediation so I did that numerous times and really all the time that always routinely wept into five buckets. Either supply chain, password, the spear phishing,

11:46:07

11:46:34

elevating privileges of an in side error lack of independent third party audit so there's that. Also was the DOD lead for the cybersecurity initiative call the CNCI created by the *Bush* administration and reviewed. I was at the white house reviewed by the owe palm ma administration and not only endorsed but embraced and accelerated and our findings were given to the John Brennan who recommended them to the presidents who approved it.

11:46:44

11:47:04

And then also --

Q. Was that a presidential directive then?

11:47:17

A. Correct. That was an NH-- NSHSPD four 5023 and so I helped write that and then implement that.

Q. And that related to cybersecurity control in this country?

A. Yes. It was a very significant increase in programmatics and spending across the U.S. Government to increase the level and it was -- this is very important. It was across the entire U.S. Government, not just one department or agency.

11:47:38

Q. As it relates to that, was that back in the time when cybersecurity first became nomenclature?

A. Right. Right. I think you kind of have to sayes stone illegal alien in the cyberright and the summer of 2007 was kind of the BC. AD. That's when we really learned that some of our most sensitive systems were breached, were being breached. And even after a number of years of significant spend and focus, continued to be breached.

11:47:58

11:48:16

Q. Do you have any work as in teaching? 11:48:22

A. Correct. I'm an adjunct professor at a major university.  
I teach the cybersecurity Capstone course.

Q. And where is that?

A. University of Maryland, global campus. 11:48:33

Q. And do you have security clearance?

A. Yes, I do.

Q. And what level?

A. TSSCIso top secret compartment information.

Q. You provided a declaration for this litigation. are you 11:48:52  
aware of that?

A. Yes, I did.

Q. And you have reviewed that and can -- can you confirm that  
everything in it is truthful and accurate?

A. Yes, I can. 11:49:05

Q. You stand by that declaration?

A. Yes, I do.

Q. I want to focus your attention on providing the Court with  
some examples that you have experienced directly, personally of  
undetected intrusions into computer systems, some of the most 11:49:24  
serious computer systems in the country. Can you describe any  
examples of that?

A. I mean, the two that I can probably talk about are really  
the office of personnel management breach and the F35. As a  
subcomponent of my work I was part of the cyberresponse group 11:49:48

which really worked the hardest of the hardest problem sets but really starting in about 200 nine the operating imperative was presume breach. Always presume breach and then with that starting an imperative it's all about speed of are he mediation, speed of removal.

Q. Why would you presume breach?

A. Because otherwise primarily on the defense side I had to work very closely with the offense side and the there was just so many tactics, techniques, and procedures many of which we can't talk about that the opponent will get in one way or the other.

Q. And you're talking about highly sensitive systems like military weapon systems.

A. That is correct.

Q. And are you aware that voting systems in the United States have been identified by CISA as critical infrastructure?

A. That is correct. They are identified as critical infrastructure.

Q. You talked about the breach of OPM. Was the OPM system prior to breach a hardened security system in place?

MR. GAONA: Objection, Your Honor, to foundation and relevance. This has nothing to do with voting systems in Arizona. There's nothing in this witness's declaration and he said nothing to the contrary today indicating he has any experience whatsoever with voting systems or the State of

Arizona for that matter.

11:51:33

THE COURT: Mr. Parker?

MR. PARKER: Your Honor, central theme of this case is not just -- yes, it is about the electronic voting system in Arizona but our testimony can go to any computer system was the Court needs to understand and have evidence to show that computer systems can be hacked even when they are screamly hardened. And in this case when you compare it to a computer system which all in electronic voting machine system is, that is not hardened at all and that we have evidence that it's wide open, that gives the Court that sort of reference point.

11:51:47

11:52:09

THE COURT: I'm the not sure how this translates in terms of sustaining or overruling the objection. The Court accepts the point that a system can be hacked in any event given enough time, enough resources, and enough access. And so I'm not really sure what the point of this examination is on this issue. It's just taking up time. But it's your time, Mr. Parker, and so I'm going to overrule the objection.

11:52:31

There is some baseline relevance to the point but I'm telling you I understand that?

11:52:57

MR. PARKER: Thank you, Your Honor. And I appreciate -- I know it's note a stipulation certainly from the Court but I appreciate if that point is accepted by the Court, that is a primary point of our assertions.

MR. GAONA: And upper on that point if I may have a

11:53:13



standing objection to this entire line of questioning along those lines so as to avoid interruptions. I think this entire line of testimony is irrelevant and lacks foundation.

11:53:15

THE COURT: You may.

MR. GAONA: Thank you, Your Honor.

11:53:25

THE COURT: You may and proceed Mr. Parker, however you wish.

MR. PARKER: Thank you.

BY MR. PARKER:

Q. Describe how remote access operations might infiltrate a computer system like an electronic voting system?

11:53:35

MR. GAONA: Again objection, Your Honor. Foundation. This is a separate issue now?

THE COURT: And, again, my ruling is going to be the same. You have a standing objection on this.

11:53:54

Go ahead.

BY MR. PARKER:

Q. Go ahead, Mr. Mills.

A. Could you please restate the question?

Q. Describe how remote access intrusion can occur in computer systems like an electronic voting machine system?

11:54:06

A. Well, so I give some examples of successful remote access operations. There's many more but they always center around five regardless of the type of system, they always are around five things: Supply chain knowing and understanding not the

11:54:32

system but the subsystems and the components so I see no evidence that counties have that ability so there's that.

11:54:37

Q. What are you saying about the components?

A. That they have any ability to actually break down and under subcomponents such as a modem, such as a thumb drive. I see no evidence that, though, the ability to ascertain one way or the other that the heritage or pedigree of those critical subcomponents of a voting machine.

11:54:55

Q. Do you know whether they have even looked at the subcomponents to determine whether or not there is a -- an intrusion?

11:55:11

A. I've seen no evidence. I reviewed the Mesa County case, Halderman and also discussion with the other experts on Mesa. I see no evidence of that. We would call that bench testing of subcomponents and I see no evidence of that.

11:55:30

MR. GAONA: Your Honor, at this point I need to move to strike everything this witness has said about subcomponents in his review of counties, again for the same reason. I understand there is a standing objection here. This is now getting highly prejudicial with a witness who has no experience with any of the counties that at issue in this specific case talking about his alleged knowledge of what they do or don't do.

11:55:44

MR. LARUE: Your Honor, Maricopa County joins that objection.

11:55:55

THE COURT: All right. Give me a moment, please, counsel.

11:55:57

THE COURT: I'm going to ask for your patience one more minute, counsel. I'm not sure the transcription is quite right on a couple of the words.

11:57:34

All right. Mr. Parker, can you respond to the objection or would you like to hear it again.

MR. PARKER: I would like to hear it again.

THE COURT: Can you read it back please eye line.

MR. PARKER: You were, maybe I can lay some foundation.

11:59:41

THE COURT: You may attempt to lay foundation. Mr. Gaona, I'll hear you again after that foundation had been laid.  
BY MR. PARKER:

Q. Mr. Mills, setting aside whether Arizona has done any bench testing I think is what you said. By the way, what is bench testing of components?

11:59:55

A. Well, that's when you have technical experts would actually break down the machine and into the subcomponents because there are some very creative ways in which malware intrusion sets can be introduced and you can't just say with confidence a machine is good unless you know with great degree of specificity about the subcomponents. You just can't take the word of the subcomponent provider to the manufacturer who assembles the machine. You ever to know each component.

12:00:18

12:00:39

Q. So is it a best practice to do this bench testing? 12:00:41

A. Absolutely. Absolutely. This is on our sensitive systems we have to know this on critical infrastructure we have to know this.

Q. And do you know one way or the other whether Arizona has done bench testing? 12:00:53

A. I have not seen any evidence of that.

THE COURT: Mr. Gaona.

MR. GAONA: Your Honor again the witness just proved the point with his answer right there. He has no idea about what Arizona does or doesn't do. This entire line of questioning should be stricken and this witness should the no be able to testify any further about a topic about which he has no direct knowledge or information. It is not relevant to this case in any way. 12:01:04

THE COURT: I'm going to overrule the objection because the ultimate answer was he has no knowledge, therefore, I'm not considering any judgment that he would lay forth as an opinion on this. It's a nonissue with regard to the examination, the evidence that the Court will consider. 12:01:17

Please move on, Mr. Parker.

MR. PARKER: Thank you, Your Honor.

BY MR. PARKER:

Q. So bench testing is something you would expect a stated to but you don't know whether Arizona does it; correct? 12:01:34

A. That is a correct statement.

12:01:50

Q. I assume that they will bring in evidence if they do.

The --

THE COURT: Mr. Parker, let's keep the editorialization out of this.

12:01:58

MR. PARKER: All right. I will Your Honor, certainly.

BY MR. PARKER:

Q. My point, Mr. Mills, is that when the U.S. Government has a sensitive system that it is intending to protect, do they take the word or do they take the equipment off the itself for what it is supposedly on its face to be or do they look deeper than that?

12:02:09

A. They would look deeper --

MR. GAONA: Objection, Your Honor. Foundation. This witness cannot speak on behalf of the entire U.S. Government as far as anything as far as I can tell.

12:02:32

THE COURT: Mr. Parker.

MR. PARKER: His expertise in the area of remote access and at the Department of Defense will indicate, as I asked, about highly sensitive systems.

12:02:47

THE COURT: The objection is sustained. You are using an issue that I have allowed in general in terms of remote expertise as the camel's nose under the at the present time. This is going too far and it is now under 403 a danger

12:03:04

of a waste of time and it's not helping the finder of fact.

12:03:08

Please move on.

MR. PARKER: Thank you, Your Honor.

BY MR. PARKER:

Q. What are some of the ways there rogue actors, foreign actors, might infiltrate computer systems in the United States?

12:03:21

A. Keeping to things that have been talked about in the public or acknowledged by the U.S. Government, one of your immediate ones is any kind of portable media such as USB. It's a very common. It has been identified in agent BT."

12:03:48

Potentially something in Stux net but absolutely -- and those are privilege length in voting machines is the thumb drive but there are other ways that are not traditional ways that are not well understood and they are the public media such as through the copper power lines.

12:04:07

Q. What about in your experience at the Department of Defense, things that you can talk about?

A. Well, there's other unique things such as a keyboard. When a keyboard is looked up, that has firm ware, resident firm ware which is potentially tainted or contains malware. That is another -- so anything that is hooked into the environment so -- and that's one nontraditional way which is often overlooked is simple things like keyboards.

12:04:26

Q. In yes, Your Honor experience at the Department of Defense, have you had systems that were certified as both

12:04:45

compliant and security, in fact, then be hacked?

12:04:49

A. Yes. That's an interesting question because there's a difference -- you can be certified and still be vulnerable so when you ever standards and certification that kind of starts to delve into the policy world. Those can take months and years to determine those. So you can actually meet a standard or a certification and still be vulnerable because by the time that is established, the attack vector has moved way beyond that. So you can still be -- you can still be certified, meet a standard, and still be vulnerable.

12:05:05

12:05:25

MR. PARKER: Nothing further, Your Honor.

THE COURT: All right. Mr. Parker, thank you.

Mr. Gaona?

**CROSS - EXAMINATION**

BY MR. GAONA:

12:05:43

Q. Good -- I believe it's afternoon now, Mr. Mills. How are you?

A. Hey. Just fine.

THE COURT: I'm sorry. Mr. Gaona. Give me just a sense how long you think you might need.

12:05:56

MR. GAONA: I think I've got about five minutes.

THE COURT: And then will it be Mr. Liddy?

MR. LIDDY: Yes, Your Honor.

THE COURT: Okay. Then we'll go ahead and finish with this witness before we start our lunch break.

12:06:06

MR. GAONA: Thank you, Your Honor. And I realize I forgot my glasses. 12:06:09

BY MR. GAONA:

Q. Mr. Mills, are you being paid for your work on this case?

A. Yes. Yes, I am. 12:06:17

Q. Mr. Parker's firm is paying you?

A. For this portion, yes. That's what my understanding is.

Q. Okay. --

A. I have not received.

Q. Somebody else has paid for another portion of your work. 12:06:27

A. Well, there was a statement that I made that -- I can't remember exactly who it was -- it might have been the Lundell group or ship. I can't remember the exact name.

Q. So you think there's a possibility that former CEO of My Pillow, Mike Lundell, may be covering your costs associated with this case? 12:06:44

A. I would have to check and verify the name of the organization. It might have his name. I don't know if that means that's him personally.

Q. Okay. What is your hourly rate for your work on this case? 12:06:53

A. \$350 is what I charge for consulting on court matters like this and complex issues.

Q. Do you have a sense of the number of hours you've spent up through your testimony today working on this case? 12:07:07



A. I would say maybe about 15.

12:07:12

Q. Have you been paid anything to date?

A. For the statement approximately that was \$4,000. It was less than that. I can't remember the exact.

Q. And when are you referring to your statement, are you referring to the statement of the declaration submitted by the plaintiffs or are you referring to something?

12:07:32

A. I apologize. Call that the declaration, yes.

Q. Okay. Thank you. In the declaration you submitted 96 at paragraph 17, you said, quote, I have served as a sworn election official and understand the U.S. election process at the county level, close quotement.

12:07:43

Do you recall writing those words. Correct and I have done that numerous times in my county.

Q. You've never served as a counter tee elections director, have you?

12:08:00

A. A sworn election officer, not the director, correct.

Q. You've never served as a county recorder correct.

A. I don't think that would be -- I don't think that would be my title no. Sworn election officer is what I remember.

12:08:13

Q. So when you say sworn election official, does that mean you were a poll worker?

A. Behind the counter actually either operating the poll book. Normally operating the poll book.

Q. Okay.

12:08:29

Q. So you were working on administrative tasks as a temporary poll worker behind the count as you put it? 12:08:30

A. Well, sworn election official we would call that in Virginia. You are essentialal deputized sworn eye official for the temporary period of the election. 12:08:42

Q. Right. And I understand that but you weren't making policy decisions in any way related to the administration of an election. Is that accurate to say?

A. There was numerous times feedback and advice was actually requested or given? 12:08:57

Q. You've never testified as an expert in any court of law on any issue, have you?

A. This goes back a lot of yearsment I object involved in a lot of legal proceedings, some of them classified. I don't think -- I don't remember sitting like where I am right now talking to somebody like you. 12:09:18

Q. This is the first case in which you ever have been asked to provide what you are calling an expert opinion. Would that be accurate?

A. I think back, years back I have provided statements before so, again, I have not sat in a booth looking at somebody like you. 12:09:30

Q. But just to be clear you've never testified in any court of law based on the opinions you expressed in your declaration and here earlier today about what you perceived to be 12:09:48

vulnerabilities in voting systems in the United States?

12:09:51

A. Okay. You are correct, yes.

Q. Are you a registered voter?

A. Yes, I am.

Q. What state are you registered in currently?

12:10:01

A. Virginia.

Q. How long have you been voting, sir?

A. I would say as long as I have been in Virginia, so about 1992.

Q. Do you know whether Virginia uses an electronic voting system to tabulate ballots?

12:10:11

A. Yes. Yes. We do. There are concerns with them. I actually was asked -- the Attorney General asked me to come in earlier this year and talk to them about this.

Q. Okay. Isn't it true, Mr. Mills, that you never raised any alarms about the alleged vulnerabilities in voting -- electronic voting systems in the United States until after the 2020 general election?

12:10:26

A. I have to parse that a little bit, sir. after the 2021 election 2019 election in Virginia I was concerned -- I think it would be more toward -- I was concerned about the jury duty roles are drawn from the -- drawn from the voting records and there was very significant concerns over the number -- several categories of what would be considered unlawful voters in a federal election in 18 U.S. code so that started my interest

12:10:48

12:11:11

and my study and my research into this.

12:11:15

Q. Do you believe that former President Trump actually won the 2020 general election?

MR. PARKER: Objection, Your Honor. As to the relevance of this.

12:11:23

THE WITNESS: I think it's unclear.

MR. PARKER: Objection, Your Honor.

THE COURT: Hold on for just a second, Mr. Mills. I need to rule on the objection first.

THE WITNESS: Oh.

12:11:31

THE COURT: Relevance you say.

MR. PARKER: Yes. What's the relevance of who won the election or didn't.

THE COURT: I'm going to overrule the objection. If the point is you're attempt to go show some bias, I'm not sure just -- hang on -- yeah. I will overrule the objection.

12:11:50

And you may answer that question, Mr. Mills?

THE WITNESS: We have a sworn president. His name is Joe die Biden and the process has run its course. I do think we have questions with our election process and I believe it's reasonable to look into them.

12:12:11

BY MR. GAONA:

Q. Okay. You are not an election expert; is that correct?

A. Well, I think it's interesting how you would define an election expert. I'm a concerned citizen that has spent a lot

12:12:24

of time looking into this on my own time and so I've began to develop an understanding of the process.

12:12:27

Q. Sure if I were to look to your résumé or CV, you wouldn't represent yourself to the public as an expert on elections in the United States, would you?

12:12:42

A. I would say I'm very knowledgeable. And I think anybody who would assert assert that they are an expert I would want to know how they define being an expert.

Q. Fair enough. You're not a computer expert, are you, Mr. Mills?

12:12:52

A. I am not, I would call it I am not a line of code expert. I understand highway computers operate. I've spent a lot of years reviewing vulnerabilities and, again, I've had to do hundreds of assessments and write-ups on breach after breach of some of the most sensitive systems that we spend immense resources to protect and it still happens.

12:13:09

Q. You're not an expert on voting systems; correct?

A. There's shared componentry of the voting system which leads to the commonality of those five common themes that I mentioned earlier.

12:13:26

Q. Now, in formulating the opinions you've expressed in this case both in your declaration and here in open court today, you didn't actually examine the voting systems that are used by either Maricopa County or Pima County, did you?

A. That is correct.

12:13:41

Q. You mentioned earlier some potential ways that a bad actor could gain access to a computer system generally. I think I heard you say a USBthumb drive, keyboard and copper power lines. Am I summarizing some of the things you said earlier accurately?

A. Yes. Our side and the other side are extremely creative and it goes far beyond that.

Q. Okay. As you sit here right now under oath you have no evidence that any of those methods have been used by anybody to gain access to any voting system in Arizona, do you?

A. I object in meetings where concerns have been raised about both Russia and China involved in election systems.

Q. I understand concerns have been raised but that was not my question, Mr. Mills. My question is whether you have any direct evidence that there's been any malicious third-party intrusion into any voting system in the State of Arizona.

A. Well, because of some of the things that we start to do talk about --

Q. Mr. Mills, it's yes or no. Do you have direct evidence of that or no?

A. Well, there's been an absence of review of several key things from my seat that I would have to say I'm sorry we have not looked at these so it's hard to say.

Q. You have no direct evidence, do you, Mr. Mills?

A. We have not looked at several topics.

Q. All right.

12:15:03

MR. GAONA: I don't think I have any further questions, Your Honor. Thank you.

THE COURT: All right. Mr. Gaona. Thank you.  
And Mr. Liddy?

12:15:08

MR. LIDDY: Thank you, Your Honor.

**CROSS - EXAMINATION**

BY MR. LIDDY:

Q. Serve I see in your declaration that you served our country in the United States Air Force; is that correct?

12:15:25

A. Uh.

Q. Army. I'm sorry.

A. Yes, that was -- I was Army, to the best of my knowledge.

Q. So USAR, United States Army Reserve; is that correct?

A. Yes. 33 years as both active guard and reserve.

12:15:36

Q. So you have been serving our country since 1983; is that correct?

A. That is correct.

Q. Thank you for your service.

On direct examination, you were asked questions and you responded about potential harm of rogue actors and foreign actors. Do you recall that?

12:15:45

A. I think we talked about that, yes.

Q. And you were asked if you an expert on election systems and you -- do you recall that?

12:16:03

A. I believe -- I believe the expression was elections. 12:16:05  
Elections.

Q. And do you recall your response?

A. I would say I'm very knowledgeable but I would also like 12:16:15  
to know the definition of who is an expert on elections.

Q. Have you been trained on elections?

A. Yeah, I actually have gone through formal training on  
numerous times in my county, so in Virginia.

Q. But not at the University of Maryland and Prince Georges 12:16:29  
County, Maryland, College Park?

A. Correct.

Q. And not at the United States Army War College or  
otherwise?

A. Well, actually that's -- we actually -- I participated in 12:16:40  
oversight of very simplistic elections both in Bosnia in Iraq.  
So we trained as best as we could with simplistic situations.

Q. Thank you. Are you familiar with the term psy ops?

A. That is correct. Psychological -- I don't think that is  
the correct -- I think I used that termly. Frankly, I don't  
know what the U.S. army calls in contemporary times. It has 12:16:59  
gone back and forth.

MR. LIDDY: Your Honor, for the benefit of the court  
reporter, that's capital P-S-Y, capital O-P, Psy Op, with an S,  
plural.

Q. Psychological operations; is that correct? 12:17:11



- A. Yes. 12:17:12
- Q. Have you been trained in psychological operations?
- A. Yes, that is correct.
- Q. Could a rogue actor or foreign actor utilize the arts as  
likelological operations in order to undermine the confidence of  
a foreign power? 12:17:21
- A. Yes. I would -- I would differentiate the way doctrinally  
and lawfully United States looks at it from foreign power such  
as Russia or China. There's inherently different viewpoints on  
that so it's not quite an apples-to-apples comparison. 12:17:41
- Q. I understand but I'm not asking you about the Article II  
lawful authority as a natural authority to participate in  
psychological operations of a foreign power. I'm just asking  
you if the arts taught in psychological operations would be  
effective in a foreign power? 12:18:02
- A. I apologize. I have to clarify. From us to them or from  
them to us?
- Q. Either.
- A. Again, we look at it doctrinally different. In American  
psychological operations, it's very simple simple. It's not  
that complicated. There's a lot of specter of secrecy perhaps  
or -- but you tell the truth. In American psychological  
operations, you tell the truth. It's as simple as that. 12:18:18
- Q. So under your experience and your training, the United  
States never mixes some aspects of factual betrayal with 12:18:34

unfactual material or misleading material or vague material in order to create an environment to undermine the national command authority of a foreign power? 12:18:39

A. Yeah. That starts to delve into a different U.S. Code and Title 50 so I would differentiate -- 12:18:53

Q. Again, I'm not asking you about the Code. I'm asking you about whether the training you've received in psychological operations could be effective in achieving such an end.

A. I will -- I apologize to parse U.S. codes but it is important. I was trained in Title 10, psychological operations where telling misleading things is really starts to deviate are both the law and the training. 12:19:11

Now, with a -- with a clandestine covert finding that's a different world.

Q. I understand that but I'm not asking you about title ten. I'm asking you whether psychological operations can be effective in undermining a public's confidence in the change of command of the national authority? 12:19:28

A. But you are prohibiting me from parsing between different doctrines or U.S. codes. I mean, you're blur ago huge picture together. 12:19:48

Q. I'm just asking you the question sir, colonel. Just asking you a question.

A. From my perspective, it's title ten, yes, we could emphasize the truth and absolutely. That's the whole point is 12:20:01

to influence the population.

12:20:05

Q. And by influencing population, is it possible to undermine the population's confidence in the country's line of success?

MR. PARKER: Objection, Your Honor, to relevance to this line of questioning to this case.

12:20:14

THE COURT: The objection is overruled.

Please finish your question.

BY MR. LIDDY:

Q. Under your training and your experience, is it possible that psychological operations, psy ops if you will, could be effective in undermining the population's confidence in the country's line of succession at the national command authority level?

12:20:23

A. If we were broadcasting toward a foreign audience which by law that is the only one we can talk to. We can't talk to the U.S. population, yes.

12:20:39

Q. When you say we you're referring to the Government?

A. I'm talking about the U.S. army and our doctrine.

Q. Well, let's go outside the constraints of the United States army or the Department of Defense or the United States Government. Is it possible that psy ops could be effective in undermining a nation's authority in the transfer of power at the national command authority whether it's lawful or unlawful, whether it's Title 10 or not Title 10. Let's say it's a rogue actor. Is it possible?

12:20:51

12:21:12

A. That an extremely broad question. Somebody could use something to undermine something. Yes. 12:21:15

Q. Thank you, Your Honor?

MR. LIDDY: No further questions.

THE COURT: All right. Mr. Liddy. Thank you. 12:21:26

And Mr. Parker, if you have any redirect.

MR. PARKER: No, Your Honor. Thank you.

THE COURT: All right. Thank you.

So same question for all three counsel. May Mr. Mills be excused? 12:21:34

MR. PARKER: He may, Your Honor.

MR. GAONA: Yes, Your Honor.

MR. LARUE: Yes, Your Honor.

MR. LIDDY: Yes, Your Honor.

THE COURT: Thank you all. 12:21:42

Mr. Mills, you may step down and I can excuse you sir.

(Witness excused.)

THE COURT: Counsel, let's take the lunch break. I'm going to give you an hour. We'll start again at 1:20 and finish up then. 12:21:50

THE COURT: Let's go back on for a second. I'm going to give you times just so you all know for planning purposesment give me a second.

All right. Counsel, plaintiffs have 33 minutes of 12:22:26

their allotted two hours remaining. The defendants have indicated to me that they were combining so I looked at three hours together. You have exactly two hours remaining.

12:22:29

Thank you, counsel.

(Recess at 12:22

12:22:42