

1	UNITED STATES PATENT AND TRADEMARK OFFICE
2	BEFORE THE PATENT AND APPEAL BOARD
3	KEYSIGHT TECHNOLOGIES,) CASE IPR2023-00445
4	INC.,) U.S. PATENT NO. 10,785,266
5	PETITIONER,)
6	v.) MOBILE VIDEOCONFERENCE
7	CENTRIPETAL NETWORKS,) DEPOSITION OF
8	INC.,) DOUGLAS W. JACOBSON, Ph.D.
9	PATENT OWNER.)
10	
11	
12	
13	MOBILE VIDEOCONFERENCE DEPOSITION OF DOUGLAS W.
14	JACOBSON, Ph.D., taken remotely before Cheryl A.
15	Rooney, RPR, CRR, Online General Notary Public within
16	and for the State of Nebraska, beginning at 9:02 AM, on
17	March 27, 2024.
18	
19	
20	
21	
22	
23	
24	
25	

1	APPEARANCES
2	(Appearing Remotely)
3	THE WITNESS:
4	DOUGLAS W. JACOBSON, Ph.D.
5	(Appearing Remotely)
6	FOR THE PETITIONER:
7	JONATHAN I. DETRIXHE
8	REED SMITH LLP
9	101 Second Street, Suite 1800
10	San Francisco, CA, 94105
11	(415) 543-8700
12	jdetrixhe@reedsmith.com
13	(Appearing Remotely)
14	FOR THE PATENT OWNER:
15	JENNA FULLER
16	JEHRA JAFRI
17	KRAMER LEVIN NAFTALIS & FRANKEL LLP
18	1177 Avenue of the Americas
19	New York, NY 10036
20	(212) 715-9100
21	jfuller@kramerlevin.com
22	ajafri@kramerlevin.com
23	
24	
25	

1	I N D E X		
2	CASE CAPTION.....	Page	1
3	APPEARANCES.....	Page	2
4	INDEX.....	Page	3
5	TESTIMONY.....	Page	4
6	REPORTER CERTIFICATE.....	Page	56
7	DIRECT EXAMINATION:		
8	BY MS. FULLER.....	Page	4
9	EXHIBITS		
10	EXHIBITS PREVIOUSLY MARKED:	IDENTIFIED	
11	Exhibit 1001 '266 Patent		4
12	Exhibit 1001 '474 Patent		4
13	Exhibit 1003 '266 Patent - Jacobson Declaration		4
14	Exhibit 1003 '474 Patent - Jacobson Declaration		4
15	Exhibit 1005 Law Patent		4
16	Exhibit 1014 '266 Patent - Reply Declaration of Jacobson		4
17	Exhibit 1017 '474 Patent - Reply Declaration of Jacobson		4
18			
19			
20			
21			
22			
23			
24			
25			

Page 4 1 (Whereupon, the following proceedings 2 were had, to-wit:) 3 (Exhibits 1001-'266, 1001-'474, 4 1003-'266, 1003-'474, 1005, 1014, and 1017 5 marked in a previous proceeding.) 6 DOUGLAS W. JACOBSON, Ph.D., 7 having been first duly sworn, 8 was examined and testified as follows: 9 DIRECT EXAMINATION 10 BY MS. FULLER: 11 Q. Good morning, Dr. Jacobson. 12 A. Good morning. 13 Q. Do you understand why you're here 14 today? 15 A. Yeah, I'm here to give a deposition in 16 the IPR case involving the '274 patent and the 17 '266 patents. 18 Q. And the '274 patent, you mean the '474 19 patent, is that -- 20 A. Oh, I'm sorry, yes, '474, thanks. 21 Q. Is there any reason that you cannot 22 give your truthful testimony today? 23 A. No. 24 Q. Dr. Jacobson, you have in front of you 25 Exhibit 1014 in the '266 IPR proceeding, and	Page 6 1 A. Yeah. Counsel provided an initial 2 draft. We then iterated through multiple 3 iterations of the draft, you know, back and 4 forth with email, and I think we had at least 5 one or two calls discussing the drafts. 6 Q. How many hours would you say you spent 7 preparing these declarations? 8 A. Without having my billing in front of 9 me, probably in the order of 10 to 15 hours, I 10 would say, somewhere in that neighborhood. 11 Q. Did you review any of the exhibits or 12 papers when preparing these declarations? 13 A. Sorry, you cut out in the middle of 14 that. 15 Q. Did you review any exhibits or papers 16 when preparing these reply declarations? 17 A. Yeah. And they're listed in the reply 18 declaration, the exhibits and the materials that 19 I reviewed, so I mean, I can re-read them. 20 Q. That's fine. You don't need to 21 re-read them. 22 Did you review any other documents 23 outside of the materials listed, documents in 24 your declarations? 25 A. No, not that I recall.
Page 5 1 1017 in the '474 IPR proceeding; is that 2 correct? 3 A. That's correct. 4 Q. Do your declarations include all of 5 the opinions you have formed in this case? 6 A. They're reply declarations, so they 7 have all the opinions I have relative to the 8 reply declaration. 9 Q. Are there any corrections to those 10 reply declarations that you would like to make 11 at this time? 12 A. No. 13 Q. Pardon me? No? That was a no, 14 Dr. Jacobson? 15 A. Yeah, that was a no. You're cutting 16 in and out. 17 Q. Okay. Well, let me know if you can't 18 hear anything or understand what I said and I'll 19 try to repeat myself. I am in an echoey room, 20 so I apologize for that. 21 Dr. Jacobson, how did you prepare your 22 reply declarations? Did you write them 23 yourself, did you work with counsel? 24 A. I worked with counsel. 25 Q. Can you describe your process?	Page 7 1 Q. Did you prepare for this deposition 2 today? 3 A. Yeah. 4 Q. Did you meet with counsel in 5 preparation? 6 A. Yeah, I had a video call with counsel 7 and, of course, read through the materials. 8 Q. How many hours would you say that you 9 put in to preparing for this deposition? 10 A. Oh, probably five, six hours. 11 Q. Can I have you look at Exhibit 1001, 12 which is the '266 patent. 13 A. Yes, I've got it. 14 Q. Can I have you turn to Column 21, 15 Line 3, going to Line 8. Let me know when you 16 get there. 17 A. Column 21, you said, Line 3. Yeah. 18 Yep, I'm there. 19 Q. So in your reading of this claim 20 language, a dynamic security policy comprising a 21 first set of packet filtering rules to be 22 applied to all network traffic traversing the 23 boundary, do you understand that language, 24 Dr. Jacobson, to mean that the first set of 25 rules is included in the dynamic security

1 policy? 2 MR. DETRIXHE: Objection -- 3 THE WITNESS: Boy, I don't know 4 if it's on my end. You cut out again on that. 5 MS. FULLER: Is it really echoey? 6 THE WITNESS: Yeah, it's kind of 7 echoey. It kind of cancels out. Let me get a 8 set of headphones and see if that might make it 9 clearer. Just one second. 10 (Discussion was had off the record.) 11 BY MS. FULLER: 12 Q. Dr. Jacobson, in your reading of a 13 dynamic security policy comprising a first set 14 of packet filtering rules to be applied to all 15 network traffic traversing boundary, do you 16 understand that to mean that the first set of 17 rules is included in the dynamic security 18 policy? 19 MR. DETRIXHE: Objection, form. 20 THE WITNESS: Sorry, I'm trying 21 to play through my mind what you said, because 22 it was a little slow, and I'm having to repeat 23 what you said over and over. 24 MS. FULLER: Let's go off the 25 record for a second.	Page 8 1 (At 9:18 a.m., with parties present as 2 before, the following proceedings were had, 3 to-wit:) 4 BY MS. FULLER: 5 Q. So, Dr. Jacobson, where we left off, 6 in your reading of a dynamic security policy 7 comprising a first set of packet filtering 8 rules, do you understand that plainly which to 9 mean that the first set of rules is included in 10 the dynamic security policy? 11 A. Yeah, it says that the policy needs -- 12 yeah, needs to have a set of rules. 13 Q. And that dynamic security policy with 14 the first set of rules is transmitted from 15 security policy management server to the packet 16 security gateway; is that correct? 17 MR. DETRIXHE: Objection, form. 18 THE WITNESS: Yeah, it states 19 that the security policy manager will -- that's 20 received by the gateway from the policy manager, 21 that's correct. 22 BY MS. FULLER: 23 Q. So the dynamic security policy in the 24 first set of rules, included in the dynamic 25 security policy, originate from the dynamic Page 10
1 (Discussion was had off the record.) 2 (9:12 a.m. - Recess taken.) 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	Page 9 1 security policy; that's correct? 2 MR. DETRIXHE: Objection, form. 3 THE WITNESS: Yeah -- you kind of 4 cut out a little bit, but -- yeah, in the middle 5 you dropped out on my end. 6 MS. FULLER: Let's go off the 7 record again. 8 (9:20 a.m. - Recess taken.) 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 Page 11

Page 12 1 (At 9:23 a.m., with parties present as 2 before, the following proceedings were had, 3 to-wit:) 4 BY MS. FULLER: 5 Q. Dr. Jacobson, the dynamic security 6 policy includes a first set of packet filtering 7 rules that originate from the security policy 8 management server; is that correct? 9 A. Yeah, it receives a first set of 10 filtering rules; correct. 11 Q. And when you say it receives a first 12 set of filtering rules, it's a packet security 13 gateway that receives the first set included in 14 the dynamic security policy; is that correct? 15 A. Correct, the packet security gateway 16 receives a first set of rules inside the -- 17 yeah, is part of the packet security policy, 18 dynamic security policy. 19 Q. Dr. Jacobson, do you see in the claim 20 language -- I'll direct you to the column, 21 Column 35 -- Column 21, Line 35 through 39, do 22 you see where it says, receiving, by the packet 23 security gateway and after performing packet 24 filtering on the first portion of the packets, 25 an updated second set of packet filtering rules?	Page 14 1 are optionally joined together to form a single 2 network protected by the firewalls. Is your 3 basis that the LANs are joined together to form 4 based on Figure 3 of Law? 5 A. Figure 3, to me, indicates that the 6 150a and b are indeed joined together in one 7 network. 8 Q. And what is your basis for that 9 conclusion? 10 A. You have, again, the figure, the 11 diagram showing that, and you have Law referring 12 to 150 within his -- sorry, within his patent, 13 as I mentioned further down in Paragraph 9. 14 Q. So as I understand, your basis is 15 based on Figure 3 of Law and Law's reference to 16 network 150; is that correct? 17 A. Yes. 18 Q. Do you see in Figure 3 of Law where it 19 shows the network access device with ruleset 20 151? 21 A. Yeah, I see he has three network 22 access devices shown in Figure 3, yes. 23 Q. So specifically the network access 24 device 149c with ruleset 151c; do you see that? 25 A. Yes, I do.
Page 13 1 A. Yes. 2 Q. Do you understand that language to 3 mean that the updated second set of rules is for 4 updating the first set of packet filtering rules 5 in the dynamic security policy? 6 MR. DETRIXHE: Objection, form. 7 THE WITNESS: Yeah, that's what 8 it states, the updated set of packet filtering 9 rules for the security policy from the server. 10 BY MS. FULLER: 11 Q. So that updated second set of packet 12 filtering rules is sent from the server to the 13 packet security gateway to update the first set 14 of packet filtering rules; is that correct? 15 MR. DETRIXHE: Objection, form. 16 THE WITNESS: Yeah, that's 17 correct. 18 BY MS. FULLER: 19 Q. Dr. Jacobson, can we turn to your '266 20 reply declaration, and specifically Paragraph 9. 21 A. 9, you said? 22 Q. Yes. 23 A. All right, I'm there. 24 Q. In Paragraph 9 you explain that Figure 25 3 of Law shows an embodiment in which the LANs	Page 15 1 Q. Does ruleset -- is ruleset -- 2 COURT REPORTER: (Requests 3 clarification.) 4 BY MS. FULLER: 5 Q. Is ruleset 151 used by network access 6 device to monitor and control communications? 7 MR. DETRIXHE: Objection, form. 8 THE WITNESS: As I have in my 9 declaration, Law describes several different 10 embodiments, and he talks about that ruleset -- 11 device 149c may or may not include a ruleset 12 such as 151c. So 149c does not have to have a 13 ruleset, but can. 14 BY MS. FULLER: 15 Q. And in this embodiment where it shows 16 ruleset 151c in the network access device 149c, 17 what is that ruleset's purpose? 18 MR. DETRIXHE: Objection, form. 19 THE WITNESS: I'd have to re-read 20 through Law to see if he actually specified a 21 specific purpose for 151c. Again, he said it 22 does or does not have to have the ruleset 151c. 23 BY MS. FULLER: 24 Q. Why do network access devices use 25 rulesets?

Page 16 1 MR. DETRIXHE: Objection, form. 2 THE WITNESS: Did you ask why 3 would they or -- you cut out at the beginning. 4 BY MS. FULLER: 5 Q. Yes, yes. Why do network access 6 devices use rulesets? 7 A. I'll answer the question why could 8 they or would they. They don't have to. If 9 you -- again, this is my opinion based off of my 10 experience. Network access devices can be a lot 11 of different things. Can be as simple as a 12 network switch, and most switches will have 13 various types of simple rulesets that may stop 14 certain protocols. Basic simple rules that a 15 switch itself does not create -- you know, it's 16 all part of the same network. 17 So these network access devices -- 18 most network devices with electronics on them 19 with intelligence have the ability to program 20 certain -- usually they're restrictions or 21 exceptions, and those vendors often talk about 22 them as being rules. So it could be as simple 23 as a, you know, set of hardware address 24 identifiers that are not allowed to cross or -- 25 so he doesn't, again, specify the nature of	Page 18 1 MR. DETRIXHE: Objection, form. 2 THE WITNESS: That would be a 3 rule that could be implemented in a device that 4 can see the traffic. 5 BY MS. FULLER: 6 Q. So in this way this ruleset looking at 7 UDP protocols would be monitoring and 8 controlling communication? 9 MR. DETRIXHE: Objection, form. 10 THE WITNESS: Yeah, those 11 aren't -- yeah, it looks at the traffic and 12 makes a decision, so I guess you could call that 13 monitoring and control. 14 BY MS. FULLER: 15 Q. Can we turn to Paragraph 102 of Law, 16 which is Exhibit 1005. 17 A. Where am I headed? I'm sorry, we're 18 in Law? 19 Q. Yes. Paragraph 102. 20 A. Okay, I'm there. 21 Q. Do you see in that paragraph where it 22 says that UTMS-configured devices 146, 149 may 23 include any number of additional rule tables to 24 monitor and/or protect a control system from 25 unwanted action and/or malicious attack?
Page 17 1 those particular rules. 2 BY MS. FULLER: 3 Q. So do these rulesets then monitor and 4 control communication; is that a correct 5 understanding? 6 MR. DETRIXHE: Objection, form. 7 THE WITNESS: Well, a rule that 8 is on a network device, a policy, a criteria 9 rule, would, in order to be invoked, have to 10 look at the packets, and then based on the rule, 11 take that particular action. 12 BY MS. FULLER: 13 Q. So in your previous testimony you said 14 that rulesets can be invoked to stop protocols; 15 is that correct? 16 A. Yeah, I mean, these -- yeah, these 17 devices can -- you know, based on their 18 complexity, can look at packet information. It 19 doesn't create separate networks, it's just 20 these devices, if you have rules in them, can 21 look at packets. 22 Q. So for instance, a ruleset could look 23 at a packet for UDP protocols, and if that 24 packet has a UDP protocol, invoke an action to 25 block that packet?	Page 19 1 A. How far down in the paragraph are you? 2 Q. Right at the beginning of the 3 paragraph. 4 A. 102? 5 Q. Yes. 6 A. Read what you're reading again. I'm 7 sorry. 8 Q. It's Paragraph 102, right at the 9 beginning of Paragraph 102, it says, 10 UTMS-configured devices 146, 149, internal UTMS 11 configured devices 134, 152. Do you see that? 12 A. Yes, yes. 13 Q. So continuing on with that sentence, 14 it says, may include any number of additional 15 rule tables to monitor and/or protect a control 16 system from unwanted access and/or malicious 17 attack. 18 Do you see that? 19 A. Yes. 20 Q. So do these rule tables include 21 protocols, addresses to and from an action, 22 that, if a particular packet meets certain 23 requirements, would trigger an action such as 24 block the packet? 25 A. Yeah, I mean, if you had rulesets on

Page 20 1 them, then yes, those rules would -- yeah, based 2 on what the rule describes as the packet, 3 whatever the packet should look like, and then 4 the action of the rule based on that match of 5 what the packet looks like. 6 Q. So would network access devices 7 include these rule tables for monitoring traffic 8 that is traversing the perimeter of the 9 networks? 10 MR. DETRIXHE: Objection, form. 11 THE WITNESS: They may contain 12 rules. So yes, 146 and 149 may contain rules. 13 BY MS. FULLER: 14 Q. And may contain rules that monitor 15 traffic that are traversing the boundaries of 16 the networks; correct? 17 A. Yes, yeah, the traffic that traverses 18 through those devices, the rules will be applied 19 to that traffic. 20 Q. Can we go back to either Figure 3 in 21 your declaration in Paragraph 9, or we can go to 22 Figure 3 in Law itself, whatever is easier for 23 you. 24 A. Yeah, I'm there. I've got Law up. 25 It's a bigger picture.	Page 22 1 perimeter device cut out. Sorry. 2 BY MS. FULLER: 3 Q. In reading law, what was your 4 understanding of law's description of the 5 perimeter device? 6 MR. DETRIXHE: Objection, form. 7 THE WITNESS: My understanding of 8 the perimeter device are those devices that, 9 again, are between the Internet or the outside 10 of the organization, those devices that separate 11 the organization from, for lack of a better 12 word, the outside world. 13 BY MS. FULLER: 14 Q. And then what is the purpose of the 15 perimeter device sitting outside of the network? 16 MR. DETRIXHE: Objection, form. 17 THE WITNESS: Sitting outside the 18 network. You're referring to a particular 19 device in the figure? 20 BY MS. FULLER: 21 Q. The perimeter devices. 22 A. So the perimeter devices are those 23 that separate the organization from the 24 Internet, from -- yeah, I guess from the 25 Internet is the best way to call it.
Page 21 1 Q. So looking at the network access 2 device 149c in Figure 3 of Law, this is 3 positioned outside the subsystems of 105a and 4 105b; correct? 5 A. Yeah, it's drawn in between the two 6 boxes, 105a and 105b; correct. 7 Q. So it sits outside of both subsystems; 8 correct? 9 A. Yeah. 10 Q. So, Dr. Jacobson, you've reviewed Law 11 before this deposition today, and in the process 12 of preparing your declarations; that's correct? 13 A. Correct. 14 Q. And in reviewing Law, I would assume 15 that you read it in its entirety, looked at its 16 figures, so you understand Law's disclosure; 17 correct? 18 A. Yes, yeah. I can't tell you verbatim 19 everything that's in there, but yes, I've read 20 Law. 21 Q. So when reading Law, what was your -- 22 did you come to an understanding of Law's 23 description of a perimeter device? 24 MR. DETRIXHE: Objection, form. 25 THE WITNESS: The word before	Page 23 1 Q. So perimeter device 146 sitting -- 2 separating the Internet from subsystem 105a, for 3 example, what is that perimeter device's 4 purpose? 5 A. To allow controlled access, you know, 6 to and from the Internet. 7 Q. Can you elaborate more on control 8 access? How does it allow control access? 9 A. Well, it would implement how it is 10 actually configured. It would likely implement 11 rulesets to determine what if anything can come 12 in, potentially rules to indicate what if 13 anything can leave the organization. So you put 14 perimeter security devices in place to control 15 traffic, both inbound and outbound. 16 Q. So continuing with your protocol rules 17 example, a rule that could be put in place would 18 be a UDP protocol rule in which the network 19 access device is monitoring traffic for a UDP 20 packet, and if it intercepts traffic with the 21 UDP packet, would potentially block those 22 packets? 23 A. Yes, you could implement a rule that 24 would stop, block UDP traffic from traversing 25 that particular perimeter device.

Page 24 1 Q. So going back to Figure 3 of Law, do 2 you see the server 122 of subsystem 105a? 3 A. Mm-hmm, yes. 4 Q. Okay. And then the computer 120 of 5 subsystem 105b? 6 A. Yes. 7 Q. So in a hypothetical, server 122 of 8 subsystem 105a wants to communicate with the 9 computer 120 of subsystem 105b, does that 10 communication occur through both networks, 150a 11 and 150b? 12 MR. DETRIXHE: Objection, form. 13 THE WITNESS: So your question is 14 does -- for 120 on side A -- or which was it -- 15 well, it doesn't matter, talking to 122 on side 16 b, the traffic would need to traverse through 17 150a and 150b? 18 BY MS. FULLER: 19 Q. Can you describe that process, how 20 that traffic traverses through both networks? 21 MR. DETRIXHE: Objection, form. 22 THE WITNESS: So for the client 23 side, the computer 120 to talk to a server in 24 the TCP/IP protocol, 120 would send out an 25 initial packet to make that connection with the	Page 26 1 physical things. We often refer to these as a 2 cyber physical system. And so packets, data 3 information shows up in these devices, and then 4 these devices perform certain functions and 5 actions. They may be output devices, so they'll 6 turn on and off valves, close relays in a power 7 station. They may be input devices, so you'll 8 be able to read the temperature of a tank in a 9 nuclear reactor, or in a chemical plant. 10 And so these devices bridge that gap 11 between the digital world and the physical 12 world. These devices are then interconnected to 13 the network. Some of these devices have their 14 own communications protocols that they speak, 15 and some of them may use the classic protocols 16 that we find on the -- traversing the Internet, 17 TCP/IP. So I don't know how much more detail 18 you want me to go in. 19 Q. That's good. Thank you, Dr. Jacobson. 20 When you say some of these devices 21 have their own communication protocols, what are 22 these communication protocols? 23 A. Oh, boy, there's several of them. Law 24 mentions a couple of them. The Hart protocol is 25 one. That he mentions several times. And these
Page 25 1 IP address of the destination 122 that would 2 traverse across the 150a, and that initial 3 packet would traverse through the network access 4 device showing up on 150b, and then the server 5 122 would correspondingly respond, and that 6 would start the -- again, if it was a TCP 7 connection, that would start the TCP connection 8 back and forth between client 120 and server 9 122. 10 Q. Thank you. 11 Do you have an understanding of what 12 factors into device-specific features and 13 requirements within a process control system? 14 A. Can you rephrase that question, 15 please? 16 Q. So you have an understanding of Law's 17 process control system; correct? 18 A. Yeah, as he's described, yes. 19 Q. And can you, for the record, provide 20 your understanding of what the process control 21 system is in Law? 22 A. Yeah. It gives lots of different 23 pieces and parts, but, you know, the process 24 control system, as its name implies, there are a 25 set of computing devices that control, manage	Page 27 1 protocols are -- we often refer to as 2 application protocols. They are very specific 3 to that particular functionality and 4 application. 5 Q. So these devices within a process 6 control system, they are unique to the process 7 control system and what the process control 8 system is managing; is that correct? 9 A. I guess define what you mean by 10 unique. 11 Q. Unique to the process control systems 12 management. For example, for a chemical plant. 13 A. They would be -- okay, there may not 14 be a separate physical device for a chemical 15 plant versus a power plant versus a car 16 manufacturing -- you know, versus a production 17 line. Many of these devices are somewhat 18 generic, and like I said, they'll open and close 19 switches, they'll open and close valves, they'll 20 monitor temperature, monitor all sorts of 21 external real world parameters. And so I could 22 take the same device and use it in the chemical 23 plant, use it in a nuclear power plant, use it 24 in a substation, and use it to make lawn mowers. 25 Q. And using a device in a nuclear power

Page 28 1 plant, though, there would be specific 2 privileges and rules for communications that 3 flow from the Internet to those devices 4 within -- or connected devices within the 5 nuclear power plant, that would be different 6 from a car manufacturer, given the higher 7 security? 8 A. I hope higher security. Yeah, 9 these -- so now you're talking about the 10 software, the server and various clients that 11 manage the interconnection and control of these 12 devices. And so you would configure these 13 devices to work under the control of the nuclear 14 power plant control system. So there would be a 15 control system for the nuclear power plant, and 16 then that would manage these devices in that 17 power plant, and yes, you would not want people 18 on the Internet to be able to get at the control 19 system and/or the control rod valve -- or the 20 control rod switches. 21 Q. So is it correct understanding that 22 these different control systems have different 23 rules and privileges for communication that 24 flows in and out? 25 A. And that's what Law talks about, also,	Page 30 1 coming from the Internet and traversing firewall 2 146a in Figure 3, that would have ruleset 147a 3 applied to it in order to facilitate that 4 protection; is that correct? 5 A. Yeah, in his diagram that's how he 6 shows it. 7 Q. And then traffic that's traversing 8 from the Internet through firewall 146b, that 9 would have ruleset 147b applied to it to protect 10 that system; is that also correct? 11 A. It would have -- it has a ruleset 12 drawn to protect traffic that's going in that 13 direction, yes, going through 146b. 14 Q. So ruleset 147a -- let's continue with 15 ruleset 147a -- that ruleset that's applied to 16 traffic that's going through 146a, is that going 17 to be unique to the specific device requirements 18 and privileges within subsystem 105a? 19 MR. DETRIXHE: Objection, form. 20 THE WITNESS: No, because you can 21 get a through 146b, as we've already talked 22 about, traversing from network 150a and 150b. 23 So you would have the same rule -- you know, the 24 same threat rule or rules that protect you from 25 the Internet you would have on both sides
Page 29 1 is that many of these devices on their own, if 2 you just go buy one off the shelf, have very 3 limited built-in security themselves. So they 4 really rely on devices that protect access to 5 them. And so many of these devices, if you were 6 to put one on the Internet, there would be 7 nothing to protect it. Just straight, you know, 8 unfiltered access to the Internet. So Law is 9 describing and is -- this threat management 10 system that wraps around the organization to 11 protect these devices, like I said, many of 12 which are really unable to protect themselves. 13 Q. How does Law's threat management 14 system wrap around these devices to protect 15 them? 16 MR. DETRIXHE: Objection, form. 17 THE WITNESS: Well, he talks 18 about his 146a and b that provides that 19 isolation from traffic in the Internet. So 20 that's where the rulesets 147a and b are 21 implemented. And so that's where that 22 protection boundary exists between the Internet 23 and the control system. 24 BY MS. FULLER: 25 Q. So, for example, communication that is	Page 31 1 because the traffic is capable of traversing 2 either way. 3 Q. Let me make sure I understand your 4 answer. So because traffic can go from network 5 150a to network 150b, you can have another 6 ruleset besides ruleset 147a applied to the 7 traffic that's going across firewall 146a? 8 MR. DETRIXHE: Objection, form. 9 THE WITNESS: Maybe I 10 misinterpreted the first question. My 11 interpretation was you asked if 147a and b have 12 to be different or are different. And rules 13 147a and b would contain the same rules that 14 protects the 150, the whole thing, from the 15 Internet. 16 BY MS. FULLER: 17 Q. And did I misunderstand you when you 18 said that that was because network traffic is 19 going from network 150a to network 150b? 20 A. Yeah, when you asked the question, the 21 implication of the question was that 105a and b 22 were separate, and as we discussed several 23 questions ago, we talked about how using the 24 network 150a and b, that 105a and b can talk to 25 each other.

Page 32 1 Q. So is the fact that in your 2 understanding that network 150a and network 150b 3 can talk to each other through network access 4 device 149c, the rulesets can be the same? 5 A. Yes, you'd want the same ruleset that 6 has been provided by -- you know, you want the 7 same ruleset that's protecting you from threats 8 on the Internet. 9 Q. Thank you, Dr. Jacobson. 10 Can we turn to Paragraph 83 of Law. 11 A. Okay. Okay, sorry, I'm here. 12 Q. So in Paragraph 83 of Law, that 13 paragraph is referring to the process control 14 system; is that correct? 15 MR. DETRIXHE: Objection, form. 16 THE WITNESS: Yes. 17 BY MS. FULLER: 18 Q. So the process control system can 19 automatically update rulesets in response to 20 detected network conditions; is that correct? 21 A. Yeah, that's what it states. 22 Q. Do you have an understanding of how 23 the process control system can either 24 automatically update or provide manual updates 25 to rulesets?	Page 34 1 had me refer to, it has automatic updates or an 2 alarm to prompt a manual update. So again, I 3 don't see where he describes a protocol or a 4 methodology to actually automatically update the 5 rulesets. He talks about how the operator, 6 through this console, which manages the whole 7 process, he mentions in a couple of places that 8 it may also be triggered -- I forgot where I saw 9 that -- but he talks about the possibility that 10 these alarms may also come from other events 11 that happen, these -- when we had the 12 description of a process control system, the 13 control management software that controls the 14 nuclear power plant, et cetera, is a giant 15 graphical interface that receives lots of data 16 from lots of different sources, not just network 17 sources, and so operators are responding to 18 multiple types of events, most of which tend to 19 not be network events. 20 Q. Thank you, Dr. Jacobson. 21 MS. FULLER: Looks like we've 22 been on the record for a little over an hour 23 now. Let's take a 10-15 minute break. 24 (10:14 a.m. - Recess taken.) 25
Page 33 1 A. I'm trying to remember if Law gives an 2 exact way to perform that function. I don't 3 recall if he defines a specific method to update 4 the rulesets. I'd have to -- 5 Q. Let me know if you want a moment to 6 collect your thoughts or go through Law. 7 A. Yeah, he goes into how -- okay, I lost 8 my place. Let's see, we're on Paragraph 83? 9 I'm sorry, what paragraph are we in? 10 Q. Paragraph 83. 11 A. There you go, I'm sorry, that's why it 12 didn't make sense. I lost my place and then 13 couldn't get back. He spends a lot of time 14 talking about how the operator would do that 15 based on the alarm. I don't offhand see where 16 he says exactly how those rules would be 17 automatically changed. So I don't see where he 18 describes a process to perform that 19 functionality, other than it just says that that 20 could happen. 21 Q. And that it could happen in the 22 process control system because operators allow 23 that functionality? 24 MR. DETRIXHE: Objection, form. 25 THE WITNESS: The paragraph you	Page 35 1 (At 10:28 a.m. - with parties present 2 as before, the following proceedings were had, 3 to-wit:) 4 BY MS. FULLER: 5 Q. Dr. Jacobson, can we go to Law's 6 Paragraph 66? 7 A. 66? 8 Q. Yes. 9 A. Okay. 10 Q. Great. Do you see in that paragraph 11 where it talks about a data store 220b? 12 A. Yes. 13 Q. Is this data store 220b, is this where 14 it stores data such as ruleset data? 15 A. That's what it says, yes. 16 Q. So is it correct understanding that 17 when operators configure and manage rulesets, 18 the ruleset data would be stored in data store 19 220b? 20 MR. DETRIXHE: Objection, form. 21 THE WITNESS: Yes, it says may be 22 stored there. 23 BY MS. FULLER: 24 Q. So then when the UTMS-configured 25 device need to access this ruleset data, it

Page 36 1 would access it through the data store 220b; is 2 that correct? 3 A. He's talking about the management 4 system, so this is data that's associated with 5 the management system. So yes, I guess. 6 Q. So, yes, the UTMS-configured devices 7 would access ruleset data through the data 8 source? 9 A. Configured devices -- this is the -- 10 I'm much more a visual person, so I'm trying to 11 go through the -- 12 Q. Take your time. 13 A. All right. Can you state the question 14 again? 15 Q. So I'll try my best to at least 16 paraphrase what I asked, since I don't have 17 realtime. 18 The UTMS-configured devices, they 19 receive the ruleset data through this data store 20 220b; is that a correct understanding? 21 A. Yeah, it says that they may receive 22 data from -- yeah, from the data store -- I 23 forget which one you're talking about, 204e, 24 220b? Data store 220b. 25 Q. Data store 220b is accessed by	Page 38 1 BY MS. FULLER: 2 Q. Now I'd like you to look at 3 Exhibit 1003 of your declaration in the '266. 4 Let me know when you get there. 5 A. Okay, I'm there. 6 Q. All right, perfect. Can you turn to 7 Paragraph 69 of that -- 8 A. Can you tell me what page that is on. 9 Q. That is on Page 41 of the document. I 10 don't know what PDF page. 11 A. Okay, I happen to match. Okay, which 12 one? 13 Q. 69. So in Paragraph 69 you state: 14 Law's cyber security risk management firm 305 15 corresponds to the claimed security policy 16 management server. Do you see that? 17 A. Yes. 18 Q. When you say corresponds to, what do 19 you mean by that? 20 A. It's -- it carries out the functions 21 as described in the '266. 205 serves as that 22 function. 23 Q. So firm 305 serves as carrying out the 24 functions of automatic generation in 25 distributing rulesets to the packet security
Page 37 1 UTMS-configured devices for ruleset data; is 2 that correct? 3 A. Yes. The data store has, as it 4 describes, a possibility of lots of different 5 information in it, and then it talks about that 6 the -- may receive data from the data store. So 7 these, as he calls them, UTMS-configured devices 8 can receive information from the data store. 9 Q. Would updated ruleset data also be 10 sent to and stored in the data store 220b? 11 A. Yeah, he goes on and talks about how 12 information from, like, 305 is where updated 13 data can come from 305, further on down in that 14 paragraph. So this -- and all this is referring 15 to Figure 2. So Figure 2 lays out basically the 16 system, the graphical system that manages all of 17 this. 18 Q. So is it the correct understanding 19 then that the UTMS-configured devices can 20 receive from the data store either the ruleset 21 data or the updated ruleset data? 22 MR. DETRIXHE: Objection, form. 23 THE WITNESS: Yeah, it talks 24 about rulesets can be updated. So yes, it 25 receives the data from the data store.	Page 39 1 gateway; is that correct? 2 MR. DETRIXHE: Objection, form. 3 THE WITNESS: Yes. 4 MS. FULLER: Thank you, 5 Dr. Jacobson. 6 BY MS. FULLER: 7 Q. Can we go to your '474 reply 8 declaration. 9 A. Oh, okay. Let me close this window. 10 Q. So specifically I want to draw your 11 attention to Paragraph 29, and -- I'll let you 12 get there. 13 A. Yes, 29, yes. 14 Q. Give me one second. My computer is 15 freezing on me. In Figure 13 that you have of 16 Law from -- in that Paragraph 29. 17 A. Okay. 18 Q. Do you see Figure 13? And that's a 19 rule table; correct? 20 A. Yes. 21 Q. So is it your understanding that each 22 row in Figure 13's rule table corresponds to a 23 packet matching criterion of a packet filtering 24 rule? 25 A. Yeah, that's what that figure shows --

Page 40 1 or yeah, parts of the packet. 2 Q. So for instance in -- let's take as an 3 example Row 1326. That is what you say is a 4 packet matching criterion, has conditions such 5 as protocols from threshold to an action; 6 correct? 7 A. Yes. 8 Q. So if traffic is crossing firewall 9 146a, for example, a packet matching criterion 10 would look at the protocol of the packet, and if 11 it meets certain protocol such as the UDP 12 protocol from certain address to a certain 13 address, the action would be accept; is that 14 correct? 15 MR. DETRIXHE: Objection, form. 16 THE WITNESS: Yeah, that's what 17 1326 shows. 18 BY MS. FULLER: 19 Q. And each column is a condition field, 20 right, 1302 through 1310? 21 A. 1310 is the action. So restate what 22 you asked. 23 Q. So the condition -- yes. 24 So the condition fields would be 1302 25 to 1308 then?	Page 42 1 number in a particular field in the packet. So 2 your rule could contain any number that matches 3 a particular type of protocol. Law talks about 4 a couple -- 5 Q. So it could be any -- 6 A. Sorry. 7 Q. No, you continue. I interrupted. 8 A. So Law talks about a couple less 9 common protocols. You know, obviously this 10 figure shows kind of the three most common 11 protocols that we see. 12 Q. And less common protocols, what would 13 those be? 14 A. Oh, he talks about SCPI. There are -- 15 I don't off the top of my head know all of the, 16 you know, particular protocols that are out 17 there that could be -- that are less common, yet 18 still used. 19 Q. And less common but still used, what 20 do you mean by "yet still used"? 21 A. Okay, so I'm so old that I remember 22 protocols that are long since dead. So, I don't 23 know, I'll try to give you an example from 24 ancient history. There was a protocol called 25 LANtastic. That's long since dead because of
Page 41 1 A. Yeah, that's the match side, and then 2 1310 is the what to do. 3 Q. The action. 4 A. Yes. 5 Q. So when a packet is coming through, 6 the conditions of 1302 through 1308 are looked 7 at to see if they're met, and if so, and if they 8 are met, then the action would be accept? 9 A. Yes. 10 Q. So looking at the condition field 1302 11 column, do you see that column in the rules 12 table? 13 A. Yeah. 14 Q. So this column can include any number 15 of protocols such as UDP, TCP, ICMP? 16 A. Yes. 17 Q. What other protocols could this column 18 be looking for? 19 A. Any number of protocols. The protocol 20 field is, if I remember right, is a byte long, 21 two bytes. So anyway, there can be -- in the 22 standard there can be hundreds of protocols, and 23 so that term UDP is the graphical representation 24 of a number -- I don't remember what it is for 25 sure. And so each of those correspond to a	Page 43 1 various security reasons, et cetera. That's why 2 I use that term of still in use versus protocols 3 that have been obsoleted. 4 Q. So the SCPI protocol is still used 5 for -- in a condition field to indicate a 6 specific packet matching criterion; is that 7 correct? 8 A. Yeah, that's -- yeah. 9 Q. And what is the SCPI protocol used 10 for? 11 A. Boy, I'd have to research. That's not 12 one that I'm intimately familiar with. Given 13 that Law referenced it, I would speculate that 14 it is some type of a process protocol. 15 Q. A process protocol for the process 16 control system? 17 A. Yeah. He talks about the Hart 18 protocol, that's the one that he mentions in his 19 documents. And -- 20 Q. But sitting here today, you don't have 21 a recollection of what the SCPI protocol is? 22 A. No, I don't. 23 Q. Can these protocols come from 24 different sources? 25 MR. DETRIXHE: Objection, form.

1 THE WITNESS: I don't know what 2 you mean by come from different sources. 3 BY MS. FULLER: 4 Q. Sources meaning sources that provide 5 threat data. 6 A. Protocols come from them -- the 7 protocols exist. Can you rephrase the question? 8 Q. Yeah. So in the threat data that 9 provides rules which include -- which do these 10 rules include condition fields? 11 A. Condition fields -- you mean like the 12 protocol type, et cetera? 13 Q. Yes. 14 A. Yeah, the rules would contain various 15 fields in the packet headers. 16 Q. So the sources providing these rules 17 could provide the same or duplicate rules in the 18 threat data; is that correct? 19 A. Provide what rules? You cut out. 20 Q. The same or duplicate rules in the 21 threat data. 22 A. I still didn't catch that word. What 23 kind of rules? 24 Q. Duplicate. 25 A. Oh, duplicate, okay.	Page 44 1 using the threat data. And then typically these 2 systems allow you to choose how you use that 3 threat data. 4 Q. So when threat data comes in, the 5 operator then would have to determine the 6 action, or how would this be done? 7 A. Yeah, I didn't mean to imply it that 8 way. Your question asked about whether the 9 action comes with the threat data. And that's 10 typically not the case. Especially if it's 11 threat data, the action typically is, because 12 it's threat data, is blocked, not accept. His 13 Figure 13 is a little -- I won't say misleading, 14 but he basically has everything as an accept 15 rule. But that action, again, if you're looking 16 at threat data, generally would come down as 17 something that you don't want to have happen. 18 But again, the action field may or may not be 19 incorporated in the data that comes from the 20 sources. 21 Q. So the data that does come from the 22 sources, though, would include a protocol field, 23 an address, destination field; is that correct? 24 A. Yeah, it would contain, yeah, 25 information that is part of the packet. So what Page 46
1 Q. My apologies. 2 A. That's okay. Yeah, yes, I mean, 3 different sources can have -- would in all 4 likelihood -- independent sources would in all 5 likelihood have duplicate rules, especially the 6 higher the probability that the -- you know, the 7 more common the threat is, the higher the 8 probability that they're going to have duplicate 9 rules. 10 Q. And then again, just to make sure I 11 have a clear understanding, these duplicate 12 rules include the fields such as prototype, 13 addresses, actions; is that correct? 14 A. Rules -- I'm not sure all rulesets 15 would have the action field. That is -- general 16 practice is the action field -- depends why 17 you've got the rules. Some providers would give 18 you rules of bad things, and so your default 19 action would be not accept. So often, in most 20 implementations of any type of firewall system, 21 is that the action is something that the -- is 22 based on why you're using it. Usually if it's 23 threat data, the action is not accept. 24 So, yeah, it just depends on the 25 nature of the threat data and how you plan on	Page 45 1 typically comes from these threat sources is 2 information needed to identify that that packet 3 is a threat. 4 Q. So these sources, then, can -- there's 5 a high likelihood that these sources provide the 6 same rules as they identify the same threats? 7 A. The probability of duplicates would 8 depend on the uniqueness of the threat, you 9 know, how widespread the threat is. Each of 10 these data sources have different methods of 11 collecting threats, and some data sources are 12 actually -- may be vendor-specific. It's not 13 uncommon to receive threat data from specific 14 manufacturers that -- you know, sort of around 15 their equipment, their systems. So in that case 16 there would be a very low, if not zero 17 probability of duplication. So it really 18 depends on the nature of the threat itself and 19 how that threat was discovered, viewed, you 20 know, who found it, how easy it was to find. 21 Q. Thank you, Dr. Jacobson. 22 Can we turn to Paragraph 20 of your 23 declaration '474. Specifically where -- it's 24 the end of Paragraph 20 where it says, Law's 25 disclosure that the threat data includes Page 47

Page 48 1 firewall ruleset data, the problem of duplicate 2 rules arising from Law's aggregation of threat 3 data follows directly from the text of Law. 4 So based on your opinion, there's 5 threat data that identifies duplicate rules; is 6 that correct? Or is there threat data? 7 MR. DETRIXHE: Objection, form. 8 THE WITNESS: I'm sorry, you two 9 walked over each other. 10 BY MS. FULLER: 11 Q. I was going to say, there is threat 12 data that potentially has identified the same 13 rules. 14 A. Yeah. As I just got done describing, 15 these multiple sources can identify the same 16 threat and have the same rule. So you would end 17 up -- you could have duplicates from multiple 18 entities that create the rules. 19 Q. And then because of this potential for 20 duplicate rules in the threat data, you opine 21 that a POSITA would have correlated the threat 22 data to remove any of the duplicates; is that 23 correct? 24 A. Yeah, you -- yeah. 25 Q. Is there a potential for error in the	Page 50 1 algorithm or some other way to do that. You 2 know, if two of them say yes, then, you know, 3 you, of course, would remove the duplicate, but 4 you have a higher probability believing that's 5 more accurate. But you know, the 305, you know, 6 has a hard time knowing if this particular rule 7 is indeed an actual -- represents a match to an 8 actual threat. 9 Q. But there's processes that they put in 10 place to look at these threats, when 11 constructing the rulesets? 12 A. Well, they have algorithms and 13 processes to do the combining and ordering of 14 the rulesets. How much they can, actually, 15 again -- you know, you get a particular rule 16 that says -- just a hypothetical. You get a 17 particular rule that says this IP address is a 18 known bad -- bad things come from this IP 19 address, so therefore the rule is match source 20 equals this. You know, 305 would basically -- 21 you know, pretty much have to trust that they 22 got that right. And you know, if they didn't 23 get it right, then your rule is stopping traffic 24 that you didn't want to stop from that one 25 particular IP address.
Page 49 1 threat data that's received from the sources. 2 A. Yeah, there's always a probability of 3 error the way these sources -- it's not like the 4 adversary calls up the threat source and says, 5 hey, I just created a new packet that's going to 6 crash the system, here is how it works. And so 7 these threat -- these places that identify 8 threat data are out collecting information and, 9 yeah, there's a chance that they may identify 10 something that is not a threat, yet they call it 11 a threat. 12 Q. When firm 305 receives the threat 13 data, would it then process the threat data to 14 ensure that there's no errors? 15 MR. DETRIXHE: Objection, form. 16 THE WITNESS: I'm trying to think 17 how they could do that, even if they wanted to 18 try to -- obviously, anybody would want to make 19 sure there's no errors. But the sources that 20 provide that data are sources -- they have 21 different levels of trust, so they may look at 22 the nature of the actual provider of that threat 23 data, those rules, looking at that provider with 24 different levels of trust, and therefore, you 25 know, could have a waiting factor, some type of	Page 51 1 So while 305 would like to verify, you 2 know, the data, it's really trusting the 3 providers -- the rule providers to it that they 4 have done that vetting of the ruleset. 5 Q. So firm 305 is trusting the various 6 sources that provide the threat data that they 7 have vetted the threat data for these providers; 8 is that correct? 9 A. They vet the providers that they are 10 in different levels of trust based on different 11 providers, and, you know, I said it is difficult 12 for a 305 -- you know, the data coming to them 13 says this was a threat, and so they tend to 14 accept that as something that's true, this rule 15 represents a -- you know, matches a particular 16 threat, and so they will take that rule. 17 Q. And they take that rule as an 18 accepting that rule because of their -- how they 19 indicate the level of trust for the -- of the 20 provider, as I believe you just testified to? 21 MR. DETRIXHE: Objection, form. 22 THE WITNESS: Yeah, what I said 23 was that, again, we're kind of in the business 24 process, but the 305 is from a business process 25 standpoint is going to enter contractual

Page 52 1 relationships with the threat -- the rule 2 providers, the 315s, that they view trustworthy. 3 And so from a business process standpoint, 4 they're going to accept these particular vendors 5 producing these rulesets, and so -- well, that's 6 a -- 305 is not -- you know, is the one that 7 takes these rules and provides that set of rules 8 down to whoever subscribes to them. 9 Q. Okay. And again, this is based on 10 accepting the trustworthiness of the providers 11 that serve 305 in a contractual relationship 12 with and accepting threats? 13 MR. DETRIXHE: Objection, form. 14 THE WITNESS: Yeah, I mean, 15 everything is built on trust. You know, if 16 you're buying your service from 305, you are 17 assuming that you also have a trust of 305. I 18 mean, that's true of anything in security. If 19 the service comes external to you, there's a 20 certain level of trust and business process that 21 you need to go through. It's like with any 22 supplier. 23 BY MS. FULLER: 24 Q. Dr. Jacobson, can we turn to 25 Exhibit 1001 of the '266 patent. And	Page 54 1 BY MS. FULLER: 2 Q. Yes. So, for instance, they receive 3 information from a third party, and based on 4 that information, can either create or update 5 rules; is that correct? 6 A. Yeah, it can add, remove or alter. 7 Yes. 8 Q. And these are rules of a dynamic 9 security policy? 10 A. I forget what they call them -- yes, 11 yes. 12 Q. And then this dynamic security policy 13 originates from the server, and it's distributed 14 to the packet security gateway; is that correct? 15 A. So the security policy management 16 server pushes the rules out, is that -- 17 Q. Yeah, pushes the rules out to packet 18 security gateways; is that correct? 19 A. Oh, yes, sorry. 20 MS. FULLER: I have no further 21 questions. 22 MR. DETRIXHE: I have no 23 questions, either. 24 COURT REPORTER: (Requests 25 transcript orders for the record.)
Page 53 1 specifically Column 14. 2 A. Okay. All right, so we're in the '266 3 patent, is that what you said? 4 Q. Correct. 5 A. My patent numbers don't have the 6 exhibit number written on the bottom. 7 Q. My apologies. 8 A. That's fine. Which column? 9 Q. The '266 patent, Column 14, lines 13 10 through 20. 11 A. I'm there. 12 Q. So do you understand this passage to 13 be describing the security policy management 14 server as creating or altering packet filtering 15 rules that are included in a dynamic security 16 policy? 17 MR. DETRIXHE: Objection, form. 18 THE WITNESS: It states that in 19 some embodiments, yeah, the security policy 20 management server may be configured to add, 21 remove, or alter one or more of the policies 22 stored in memory, based on information received 23 from devices within the environment. So the 24 management server can configure, add, remove, 25 alter rules. Is that what you asked?	Page 55 1 MS. FULLER: Rough draft and 2 expedited, April 1st. 3 MR. DETRIXHE: I just need final, 4 expedite for April 1st. He will read and sign. 5 THE WITNESS: Email address is 6 dougj@iastate.edu. 7 (11:11 a.m. - Adjournment.) 8 *** ** ** ** 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

1	C E R T I F I C A T E
2	STATE OF NEBRASKA)
3	COUNTY OF DOUGLAS) Ss.
4	I, Cheryl A. Rooney, Registered
5	Professional Reporter, General Notary Public
6	within and for the State of Nebraska, do hereby
7	certify that the foregoing testimony of DOUGLAS
8	W. JACOBSON, Ph.D. was taken by me in shorthand
9	and thereafter reduced to typewriting by use of
10	Computer-Aided Transcription, and the foregoing
11	fifty-five (55) pages contain a full, true and
12	correct transcription of all the testimony of
13	said witness, to the best of my ability;
14	That I am not a kin or in any way
15	associated with any of the parties to said cause
16	of action, or their counsel, and that I am not
17	interested in the event thereof.
18	IN WITNESS WHEREOF, I hereunto affix
19	my signature and seal this 1st of April, 2024.
20	
21	_____ CHERYL A. ROONEY, RPR GENERAL NOTARY PUBLIC Registered Professional Reporter
22	
23	
24	My Commission Expires: November 24, 2026
25	

11, 15, 18 56:16

actions 26:5 45:13 actual 49:22 50:7, 8 add 53:20, 24 54:6 additional 18:23 19:14 address 16:23 25:1 40:12, 13 46:23 50:17, 19, 25 55:5 addresses 19:21 45:13 Adjournment 55:7 adversary 49:4 affix 56:18 after 12:23 again 8:4 11:7 14:10 15:21 16:9, 25 19:6 22:9 25:6 34:2 36:14 45:10 46:15, 18 50:15 51:23 52:9 aggregation 48:2 ago 31:23 ajafri@kramerlevi n.com 2:16 alarm 33:15 34:2 alarms 34:10 algorithm 50:1 algorithms 50:12 allow 23:5, 8 33:22 46:2 allowed 16:24 already 30:21 alter 53:21, 25 54:6 altering 53:14 always 49:2 Americas 2:13 ancient 42:24 and/or 18:24, 25 19:15, 16 28:19 another 31:5 answer 16:7 31:4	any 4:21 5:9 6:11, 15, 22 18:23 19:14 41:14, 19 42:2, 5 45:20 48:22 52:21 56:14, 15 anybody 49:18 anything 5:18 23:11, 13 52:18 anyway 41:21 apologies 45:1 53:7 apologize 5:20 APPEAL 1:2 APPEARANCES 2:1 3:2 Appearing 2:2, 5, 9 application 27:2, 4 applied 7:22 8:14 20:18 30:3, 9, 15 31:6 April 55:2, 4 56:19 Are 5:9 14:1, 3, 6 16:24 19:1 20:15 22:8, 9, 22 25:24 26:12, 21 27:1, 2, 6, 17 29:12, 20 31:12 33:9 34:17 41:6, 8 42:14, 16, 17, 22 47:11 49:8, 20 51:9 52:16 53:15 54:8 aren't 18:11 arising 48:2 asked 31:11, 20 36:16 40:22 46:8 53:25 associated 36:4 56:15 assume 21:14 assuming 52:17 attack 18:25 19:17 attention 39:11	automatic 34:1 38:24 automatically 32:19, 24 33:17 34:4 Avenue 2:13 < B > back 6:3 20:20 24:1 25:8 33:13 bad 45:18 50:18 based 14:4, 15 16:9 17:10, 17 20:1, 4 33:15 45:22 48:4 51:10 52:9 53:22 54:3 Basic 16:14 basically 37:15 46:14 50:20 basis 14:3, 8, 14 beginning 1:16 16:3 19:2, 9 believe 51:20 believing 50:4 best 22:25 36:15 56:13 better 22:11 bigger 20:25 billing 6:8 bit 11:4 block 17:25 19:24 23:21, 24 blocked 46:12 BOARD 1:2 bottom 53:6 boundaries 20:15 boundary 7:23 8:15 29:22 boxes 21:6 Boy 8:3 26:23 43:11 break 34:23 bridge 26:10 built 52:15 built-in 29:3	business 51:23, 24 52:3, 20 buy 29:2 buying 52:16 byte 41:20 bytes 41:21 < C > CA 2:8 call 7:6 18:12 22:25 49:10 54:10 called 42:24 calls 6:5 37:7 49:4 Can 5:25 6:19 7:11, 14 13:19 15:13 16:10, 11 17:14, 17, 18, 20 18:4, 15 20:20, 21 23:7, 11, 13 24:19 25:14, 19 30:20 31:4, 5, 24 32:3, 4, 10, 18, 23 35:5 36:13 37:8, 13, 19, 24 38:6, 8 39:7 41:14, 21, 22 43:23 44:7 45:3 47:4, 22 48:15 50:14 52:24 53:24 54:4, 6 cancels 8:7 cannot 4:21 can't 5:17 21:18 capable 31:1 CAPTION 3:2 car 27:15 28:6 carries 38:20 carrying 38:23 CASE 1:3 3:2 4:16 5:5 46:10 47:15 catch 44:22 cause 56:15 CENTRIPETAL 1:6
---	--	--	--

certain 16:14, 20 19:22 26:4 40:11, 12 52:20 CERTIFICATE 3:4 certify 56:7 cetera 34:14 43:1 44:12 chance 49:9 changed 33:17 chemical 26:9 27:12, 14, 22 Cheryl 1:14 56:4, 21 choose 46:2 claim 7:19 12:19 claimed 38:15 clarification 15:3 classic 26:15 clear 45:11 clearer 8:9 client 24:22 25:8 clients 28:10 close 26:6 27:18, 19 39:9 collect 33:6 collecting 47:11 49:8 Column 7:14, 17 12:20, 21 40:19 41:11, 14, 17 53:1, 8, 9 combining 50:13 come 21:22 23:11 34:10 37:13 43:23 44:2, 6 46:16, 21 50:18 comes 46:4, 9, 19 47:1 52:19 coming 30:1 41:5 51:12 Commission 56:24 common 42:9, 10, 12, 17, 19 45:7 communicate 24:8	communication 17:4 18:8 24:10 26:21, 22 28:23 29:25 communications 15:6 26:14 28:2 complexity 17:18 comprising 7:20 8:13 10:7 computer 24:4, 9, 23 39:14 Computer-Aided 56:10 computing 25:25 conclusion 14:9 condition 40:19, 23, 24 41:10 43:5 44:10, 11 conditions 32:20 40:4 41:6 configure 28:12 35:17 53:24 configured 19:11 23:10 36:9 53:20 connected 28:4 connection 24:25 25:7 console 34:6 constructing 50:11 contain 20:11, 12, 14 31:13 42:2 44:14 46:24 56:11 continue 30:14 42:7 continuing 19:13 23:16 contractual 51:25 52:11 control 15:6 17:4 18:13, 24 19:15 23:7, 8, 14 25:13, 17, 20, 24, 25 27:6, 7, 11 28:11, 13, 14, 15, 18, 19, 20, 22 29:23 32:13, 18,	23 33:22 34:12, 13 43:16 controlled 23:5 controlling 18:8 controls 34:13 correct 5:2, 3 10:16, 21 11:1 12:8, 10, 14, 15 13:14, 17 14:16 17:4, 15 20:16 21:4, 6, 8, 12, 13, 17 25:17 27:8 28:21 30:4, 10 32:14, 20 35:16 36:2, 20 37:2, 18 39:1, 19 40:6, 14 43:7 44:18 45:13 46:23 48:6, 23 51:8 53:4 54:5, 14, 18 56:12 corrections 5:9 correlated 48:21 correspond 41:25 correspondingly 25:5 corresponds 38:15, 18 39:22 could 16:7, 22 17:22 18:3, 12 23:17, 23 27:21 33:20, 21 41:17 42:2, 5, 17 44:17 48:17 49:17, 25 couldn't 33:13 counsel 5:23, 24 6:1 7:4, 6 56:16 COUNTY 56:3 couple 26:24 34:7 42:4, 8 course 7:7 50:3 COURT 15:2 54:24 crash 49:6 create 16:15 17:19 48:18 54:4	created 49:5 creating 53:14 criteria 17:8 criterion 39:23 40:4, 9 43:6 cross 16:24 crossing 40:8 CRR 1:15 cut 6:13 8:4 11:4 16:3 22:1 44:19 cutting 5:15 cyber 26:2 38:14 < D > data 26:2 34:15 35:11, 13, 14, 18, 25 36:1, 4, 7, 19, 22, 24, 25 37:1, 3, 6, 8, 9, 10, 13, 20, 21, 25 44:5, 8, 18, 21 45:23, 25 46:1, 3, 4, 9, 11, 12, 16, 19, 21 47:10, 11, 13, 25 48:1, 3, 5, 6, 12, 20, 22 49:1, 8, 13, 20, 23 51:2, 6, 7, 12 dead 42:22, 25 decision 18:12 Declaration 3:12, 14, 16, 18 5:8 6:18 13:20 15:9 20:21 38:3 39:8 47:23 declarations 5:4, 6, 10, 22 6:7, 12, 16, 24 21:12 default 45:18 define 27:9 defines 33:3 depend 47:8 depends 45:16, 24 47:18
--	---	--	--

DEPOSITION 1:5, 13 4:15 7:1, 9 21:11 describe 5:25 24:19 described 25:18 38:21 describes 15:9 20:2 33:18 34:3 37:4 describing 29:9 48:14 53:13 description 21:23 22:4 34:12 destination 25:1 46:23 detail 26:17 detected 32:20 determine 23:11 46:5 DETRIXHE 2:5 8:2, 19 10:17 11:2 13:6, 15 15:7, 18 16:1 17:6 18:1, 9 20:10 21:24 22:6, 16 24:12, 21 29:16 30:19 31:8 32:15 33:24 35:20 37:22 39:2 40:15 43:25 48:7 49:15 51:21 52:13 53:17 54:22 55:3 device 14:19, 24 15:6, 11, 16 17:8 18:3 21:2, 23 22:1, 5, 8, 15, 19 23:1, 19, 25 25:4 27:14, 22, 25 30:17 32:4 35:25 devices 14:22 15:24 16:6, 10, 17, 18 17:17, 20 18:22 19:10, 11 20:6, 18 22:8, 10,	21, 22 23:14 25:25 26:3, 4, 5, 7, 10, 12, 13, 20 27:5, 17 28:3, 4, 12, 13, 16 29:1, 4, 5, 11, 14 36:6, 9 37:1, 7, 19 53:23 device's 23:3 device-specific 25:12 devises 36:18 diagram 14:11 30:5 did 5:21, 22, 23 6:11, 15, 22 7:1, 4 16:2 21:22 31:17 didn't 33:12 44:22 46:7 50:22, 24 different 15:9 16:11 25:22 28:5, 22 31:12 34:16 37:4 43:24 44:2 45:3 47:10 49:21, 24 51:10 difficult 51:11 digital 26:11 DIRECT 3:4 4:9 12:20 direction 30:13 directly 48:3 disclosure 21:16 47:25 discovered 47:19 discussed 31:22 discussing 6:5 Discussion 8:10 9:1 distributed 54:13 distributing 38:25 Do 4:13 5:4 7:23 8:15 10:8 12:19, 21 13:2 14:18, 24, 25 15:24 16:5 17:3 18:21 19:11, 18,	20 24:1 25:11 32:22 33:14 35:10 38:16, 18 39:18 41:2, 11 42:20 44:9 49:17 50:1, 13 53:12 56:6 document 38:9 documents 6:22, 23 43:19 Does 15:1, 12, 22 16:15 23:8 24:9, 14 29:13 46:21 doesn't 16:25 17:19 24:15 done 46:6 48:14 51:4 don't 6:20 8:3 16:8 26:17 33:2, 15, 17 34:3 36:16 38:10 41:24 42:15, 22 43:20, 22 44:1 46:17 53:5 dougj@iastate.edu 55:6 DOUGLAS 1:6, 13 2:3 4:6 56:3, 7 down 14:13 19:1 37:13 46:16 52:8 Dr 4:11, 24 5:14, 21 7:24 8:12 10:5 12:5, 19 13:19 21:10 26:19 32:9 34:20 35:5 39:5 47:21 52:24 draft 6:2, 3 55:1 drafts 6:5 draw 39:10 drawn 21:5 30:12 dropped 11:5 duly 4:7 duplicate 44:17, 20, 24, 25 45:5, 8,	11 48:1, 5, 20 50:3 duplicates 47:7 48:17, 22 duplication 47:17 dynamic 7:20, 25 8:13, 17 10:6, 10, 13, 23, 24, 25 12:5, 14, 18 13:5 53:15 54:8, 12 < E > easier 20:22 easy 47:20 echoey 5:19 8:5, 7 either 20:20 31:2 32:23 37:20 54:4, 23 elaborate 23:7 electronics 16:18 email 6:4 55:5 embodiment 13:25 15:15 embodiments 15:10 53:19 ensure 49:14 enter 51:25 entirety 21:15 entities 48:18 environment 53:23 equals 50:20 equipment 47:15 error 48:25 49:3 errors 49:14, 19 especially 45:5 46:10 et 34:14 43:1 44:12 event 56:17 events 34:10, 18, 19 everything 21:19 46:14 52:15
---	---	---	---

exact 33:2 exactly 33:16 EXAMINATION 3:4 4:9 examined 4:8 example 23:3, 17 27:12 29:25 40:3, 9 42:23 exceptions 16:21 Exhibit 3:10, 11, 12, 15, 16 4:25 7:11 18:16 38:3 52:25 53:6 EXHIBITS 3:8, 9 4:3 6:11, 15, 18 exist 44:7 exists 29:22 expedite 55:4 expedited 55:2 experience 16:10 Expires 56:24 explain 13:24 external 27:21 52:19 < F > facilitate 30:3 fact 32:1 factor 49:25 factors 25:12 familiar 43:12 far 19:1 features 25:12 field 40:19 41:10, 20 42:1 43:5 45:15, 16 46:18, 22, 23 fields 40:24 44:10, 11, 15 45:12 fifty-five 56:11 Figure 13:24 14:4, 5, 10, 15, 18, 22 20:20, 22 21:2 22:19 24:1 30:2 37:15 39:15, 18,	22, 25 42:10 46:13 figures 21:16 filtering 7:21 8:14 10:7 12:6, 10, 12, 24, 25 13:4, 8, 12, 14 39:23 53:14 final 55:3 find 26:16 47:20 fine 6:20 53:8 firewall 30:1, 8 31:7 40:8 45:20 48:1 firewalls 14:2 firm 38:14, 23 49:12 51:5 first 4:7 7:21, 24 8:13, 16 10:7, 9, 14, 24 12:6, 9, 11, 13, 16, 24 13:4, 13 31:10 five 7:10 flow 28:3 flows 28:24 following 4:1 10:2 12:2 35:2 follows 4:8 48:3 foregoing 56:7, 10 forget 36:23 54:10 forgot 34:8 form 8:19 10:17 11:2 13:6, 15 14:1, 3 15:7, 18 16:1 17:6 18:1, 9 20:10 21:24 22:6, 16 24:12, 21 29:16 30:19 31:8 32:15 33:24 35:20 37:22 39:2 40:15 43:25 48:7 49:15 51:21 52:13 53:17 formed 5:5	forth 6:4 25:8 found 47:20 Francisco 2:8 FRANKEL 2:13 freezing 39:15 front 4:24 6:8 full 56:11 FULLER 2:12 3:4 4:10 8:5, 11, 24 10:4, 22 11:6 12:4 13:10, 18 15:4, 14, 23 16:4 17:2, 12 18:5, 14 20:13 22:2, 13, 20 24:18 29:24 31:16 32:17 34:21 35:4, 23 38:1 39:4, 6 40:18 44:3 48:10 52:23 54:1, 20 55:1 function 33:2 38:22 functionality 27:3 33:19, 23 functions 26:4 38:20, 24 further 14:13 37:13 54:20 < G > gap 26:10 gateway 10:16, 20 12:13, 15, 23 13:13 39:1 54:14 gateways 54:18 General 1:15 45:15 56:5, 22 generally 46:16 generation 38:24 generic 27:18 giant 34:14 give 4:15, 22 39:14 42:23 45:17	given 28:6 43:12 gives 25:22 33:1 go 8:24 11:6 20:20, 21 26:18 29:2 31:4 33:6, 11 35:5 36:11 39:7 52:21 goes 33:7 37:11 going 7:15 24:1 30:12, 13, 16 31:7, 19 45:8 48:11 49:5 51:25 52:4 Good 4:11, 12 26:19 graphical 34:15 37:16 41:23 Great 35:10 guess 18:12 22:24 27:9 36:5 < H > had 4:2 6:4 7:6 8:10 9:1 10:2 12:2 19:25 34:1, 11 35:2 happen 33:20, 21 34:11 38:11 46:17 hard 50:6 hardware 16:23 Hart 26:24 43:17 has 14:21 17:24 30:11 32:6 34:1 37:3 40:4 46:14 48:12 50:6 have 4:24 5:5, 7 7:11, 14 10:12 14:10, 11 15:8, 12, 19, 22 16:8, 12, 19 17:9, 20 25:11, 16 26:13, 21 28:22 29:2 30:2, 9, 11, 23, 25 31:5, 11 32:22 33:4 36:16 39:15 43:3, 11, 20 45:3, 5, 8, 11, 15
--	---	--	--

46:5, 17 47:10 48:16, 17, 21 49:20, 25 50:4, 12, 21 51:4, 7 52:17 53:5 54:20, 22 he 14:21 15:10, 20, 21 16:25 26:25 29:17 30:5 33:3, 7, 13, 16, 17 34:3, 5, 7, 9 37:7, 11 42:14 43:17, 18 46:14 55:4 head 42:15 headed 18:17 headers 44:15 headphones 8:8 hear 5:18 hereunto 56:18 he's 25:18 36:3 hey 49:5 high 47:5 higher 28:6, 8 45:6, 7 50:4 his 14:12 29:18 30:5 43:18 46:12 history 42:24 hope 28:8 hour 34:22 hours 6:6, 9 7:8, 10 hundreds 41:22 hypothetical 24:7 50:16 < I > ICMP 41:15 IDENTIFIED 3:9 48:12 identifiers 16:24 identifies 48:5 identify 47:2, 6 48:15 49:7, 9 if 5:17 8:4, 8 15:20 16:8 17:20, 23 19:22, 25 23:11, 12, 20 25:6	29:1, 5 31:11 33:1, 3, 5 40:8, 10 41:7, 20 45:22 46:10, 15 47:16 49:17 50:2, 6, 22 52:15, 18 implement 23:9, 10, 23 implementations 45:20 implemented 18:3 29:21 implication 31:21 implies 25:24 imply 46:7 inbound 23:15 include 5:4 15:11 18:23 19:14, 20 20:7 41:14 44:9, 10 45:12 46:22 included 7:25 8:17 10:9, 24 12:13 53:15 includes 12:6 47:25 incorporated 46:19 independent 45:4 INDEX 3:3 indicate 23:12 43:5 51:19 indicates 14:5 information 17:18 26:3 37:5, 8, 12 46:25 47:2 49:8 53:22 54:3, 4 initial 6:1 24:25 25:2 input 26:7 inside 12:16 instance 17:22 40:2 54:2 intelligence 16:19 intercepts 23:20	interconnected 26:12 interconnection 28:11 interested 56:17 interface 34:15 internal 19:10 Internet 22:9, 24, 25 23:2, 6 26:16 28:3, 18 29:6, 8, 19, 22 30:1, 8, 25 31:15 32:8 interpretation 31:11 interrupted 42:7 intimately 43:12 invoke 17:24 invoked 17:9, 14 involving 4:16 IP 25:1 50:17, 18, 25 IPR 4:16, 25 5:1 IPR2023-00445 1:3 isolation 29:19 iterated 6:2 iterations 6:3 its 21:15 25:24 < J > JACOBSON 1:6, 14 2:3 3:12, 14, 16, 18 4:6, 11, 24 5:14, 21 7:24 8:12 10:5 12:5, 19 13:19 21:10 26:19 32:9 34:20 35:5 39:5 47:21 52:24 56:8 JAFRI 2:12 jdetrrixhe@reedsmi th.com 2:9 JEHRA 2:12 JENNA 2:12 jfuller@kramerlevi	n.com 2:14 joined 14:1, 3, 6 JONATHAN 2:5 < K > KEYSIGHT 1:3 kin 56:14 kind 8:6, 7 11:3 42:10 44:23 51:23 know 5:17 6:3 7:15 8:3 16:15, 23 17:17 23:5 25:23 26:17 27:16 29:7 30:23 32:6 33:5 38:4, 10 42:9, 15, 16, 23 44:1 45:6 47:9, 14, 20 49:25 50:2, 5, 15, 20, 21, 22 51:2, 11, 12, 15 52:6, 15 knowing 50:6 known 50:18 KRAMER 2:13 < L > lack 22:11 language 7:20, 23 12:20 13:2 LANs 13:25 14:3 LANtastic 42:25 Law 3:15 13:25 14:4, 11, 15, 18 15:9, 20 18:15, 18 20:22, 24 21:2, 10, 14, 20, 21 22:3 24:1 25:21 26:23 28:25 29:8 32:10, 12 33:1, 6 39:16 42:3, 8 43:13 48:3 lawn 27:24 Law's 14:15 21:16, 22 22:4
---	--	--	--

25:16 29:13 35:5 38:14 47:24 48:2 lays 37:15 leave 23:13 left 10:5 level 51:19 52:20 levels 49:21, 24 51:10 LEVIN 2:13 likelihood 45:4, 5 47:5 limited 29:3 Line 7:15, 17 12:21 27:17 lines 53:9 listed 6:17, 23 little 8:22 11:4 34:22 46:13 LLP 2:7, 13 long 41:20 42:22, 25 look 7:11 17:10, 18, 21, 22 20:3 38:2 40:10 49:21 50:10 looked 21:15 41:6 looking 18:6 21:1 41:10, 18 46:15 49:23 looks 18:11 20:5 34:21 lost 33:7, 12 lot 16:10 33:13 lots 25:22 34:15, 16 37:4 low 47:16 < M > malicious 18:25 19:16 manage 25:25 28:11, 16 35:17 management 10:15 12:8 27:12 29:9, 13 34:13 36:3, 5 38:14, 16	53:13, 20, 24 54:15 manager 10:19, 20 manages 34:6 37:16 managing 27:8 manual 32:24 34:2 manufacturer 28:6 manufacturers 47:14 manufacturing 27:16 March 1:17 MARKED 3:9 4:5 match 20:4 38:11 41:1 50:7, 19 matches 42:2 51:15 matching 39:23 40:4, 9 43:6 materials 6:18, 23 7:7 matter 24:15 mean 4:18 6:19 7:24 8:16 10:9 13:3 17:16 19:25 27:9 38:19 42:20 44:2, 11 45:2 46:7 52:14, 18 meaning 44:4 meet 7:4 meets 19:22 40:11 memory 53:22 mentioned 14:13 mentions 26:24, 25 34:7 43:18 met 41:7, 8 method 33:3 methodology 34:4 methods 47:10	middle 6:13 11:4 mind 8:21 minute 34:23 misinterpreted 31:10 misleading 46:13 misunderstand 31:17 Mm-hmm 24:3 MOBILE 1:5, 13 moment 33:5 monitor 15:6 17:3 18:24 19:15 20:14 27:20 monitoring 18:7, 13 20:7 23:19 morning 4:11, 12 mowers 27:24 multiple 6:2 34:18 48:15, 17 < N > NAFTALIS 2:13 name 25:24 nature 16:25 45:25 47:18 49:22 Nebraska 1:16 56:2, 6 need 6:20 24:16 35:25 52:21 55:3 needed 47:2 needs 10:11, 12 neighborhood 6:10 network 7:22 8:15 14:2, 7, 16, 19, 21, 23 15:5, 16, 24 16:5, 10, 12, 16, 17, 18 17:8 20:6 21:1 22:15, 18 23:18 25:3 26:13 30:22 31:4, 5, 18, 19, 24 32:2, 3, 20 34:16, 19	NETWORKS 1:6 17:19 20:9, 16 24:10, 20 New 2:14 49:5 NO 1:3 4:23 5:12, 13, 15 6:25 30:20 42:7 43:22 49:14, 19 54:20, 22 Notary 1:15 56:5, 22 November 56:24 nuclear 26:9 27:23, 25 28:5, 13, 15 34:14 number 18:23 19:14 41:14, 19, 24 42:1, 2 53:6 numbers 53:5 NY 2:14 < O > Objection 8:2, 19 10:17 11:2 13:6, 15 15:7, 18 16:1 17:6 18:1, 9 20:10 21:24 22:6, 16 24:12, 21 29:16 30:19 31:8 32:15 33:24 35:20 37:22 39:2 40:15 43:25 48:7 49:15 51:21 52:13 53:17 obsoleted 43:3 obviously 42:9 49:18 occur 24:10 off 8:10, 24 9:1 10:5 11:6 16:9 26:6 29:2 42:15 offhand 33:15 OFFICE 1:1 Oh 4:20 7:10 26:23 39:9 42:14 44:25 54:19
--	---	--	--

Okay 5:17 18:20
24:4 27:13 32:11
33:7 35:9 38:5,
11 39:9, 17 42:21
44:25 45:2 52:9
53:2
old 42:21
Online 1:15
open 27:18, 19
operator 33:14
34:5 46:5
operators 33:22
34:17 35:17
opine 48:20
opinion 16:9 48:4
opinions 5:5, 7
optionally 14:1
order 6:9 17:9
30:3
ordering 50:13
orders 54:25
organization
22:10, 11, 23
23:13 29:10
originate 10:25
12:7
originates 54:13
outbound 23:15
output 26:5
outside 6:23 21:3,
7 22:9, 12, 15, 17
OWNER 1:8
2:11

< P >

packet 7:21 8:14
10:7, 15 12:6, 12,
15, 17, 22, 23, 25
13:4, 8, 11, 13, 14
17:18, 23, 24, 25
19:22, 24 20:2, 3,
5 23:20, 21 24:25
25:3 38:25 39:23
40:1, 4, 9, 10 41:5
42:1 43:6 44:15

46:25 47:2 49:5
53:14 54:14, 17
packets 12:24
17:10, 21 23:22
26:2
Page 3:2, 3, 4
38:8, 9, 10
pages 56:11
papers 6:12, 15
Paragraph 13:20,
24 14:13 18:15,
19, 21 19:1, 3, 8, 9
20:21 32:10, 12,
13 33:8, 9, 10, 25
35:6, 10 37:14
38:7, 13 39:11, 16
47:22, 24
parameters 27:21
paraphrase 36:16
Pardon 5:13
part 12:17 16:16
46:25
particular 17:1,
11 19:22 22:18
23:25 27:3 42:1,
3, 16 50:6, 15, 17,
25 51:15 52:4
parties 10:1 12:1
35:1 56:15
parts 25:23 40:1
party 54:3
passage 53:12
PATENT 1:1, 2, 3,
8 2:11 3:10, 11,
12, 15, 16 4:16, 18,
19 7:12 14:12
52:25 53:3, 5, 9
patents 4:17
PDF 38:10
people 28:17
perfect 38:6
perform 26:4
33:2, 18
performing 12:23
perimeter 20:8
21:23 22:1, 5, 8,

15, 21, 22 23:1, 3,
14, 25
person 36:10
PETITIONER
1:4 2:5
Ph.D 1:6, 14 2:3
4:6 56:8
physical 26:1, 2,
11 27:14
picture 20:25
pieces 25:23
place 23:14, 17
33:8, 12 50:10
places 34:7 49:7
plainly 10:8
plan 45:25
plant 26:9 27:12,
15, 23 28:1, 5, 14,
15, 17 34:14
play 8:21
please 25:15
policies 53:21
policy 7:20 8:1,
13, 18 10:6, 10, 11,
13, 15, 19, 20, 23,
25 11:1 12:6, 7,
14, 17, 18 13:5, 9
17:8 38:15 53:13,
16, 19 54:9, 12, 15
portion 12:24
POSITA 48:21
positioned 21:3
possibility 34:9
37:4
potential 48:19, 25
potentially 23:12,
21 48:12
power 26:6
27:15, 23, 25 28:5,
14, 15, 17 34:14
practice 45:16
preparation 7:5
prepare 5:21 7:1
preparing 6:7, 12,
16 7:9 21:12

present 10:1
12:1 35:1
pretty 50:21
previous 4:5
17:13
PREVIOUSLY
3:9
privileges 28:2, 23
30:18
probability 45:6,
8 47:7, 17 49:2
50:4
probably 6:9
7:10
problem 48:1
proceeding 4:5,
25 5:1
proceedings 4:1
10:2 12:2 35:2
process 5:25
21:11 24:19
25:13, 17, 20, 23
27:5, 6, 7, 11
32:13, 18, 23
33:18, 22 34:7, 12
43:14, 15 49:13
51:24 52:3, 20
processes 50:9, 13
producing 52:5
production 27:16
Professional 56:5,
22
program 16:19
prompt 34:2
protect 18:24
19:15 29:4, 7, 11,
12, 14 30:9, 12, 24
protected 14:2
protecting 32:7
protection 29:22
30:4
protects 31:14
protocol 17:24
23:16, 18 24:24
26:24 34:3 40:10,
11, 12 41:19 42:3,

24 43:4, 9, 14, 15, 18, 21 44:12 46:22 protocols 16:14 17:14, 23 18:7 19:21 26:14, 15, 21, 22 27:1, 2 40:5 41:15, 17, 19, 22 42:9, 11, 12, 16, 22 43:2, 23 44:6, 7 prototype 45:12 provide 25:19 32:24 44:4, 17, 19 47:5 49:20 51:6 provided 6:1 32:6 provider 49:22, 23 51:20 providers 45:17 51:3, 7, 9, 11 52:2, 10 provides 29:18 44:9 52:7 providing 44:16 Public 1:15 56:5, 22 purpose 15:17, 21 22:14 23:4 pushes 54:16, 17 put 7:9 23:13, 17 29:6 50:9 < Q > question 16:7 24:13 25:14 31:10, 20, 21 36:13 44:7 46:8 questions 31:23 54:21, 23 < R > reactor 26:9 read 7:7 19:6 21:15, 19 26:8 55:4	reading 7:19 8:12 10:6 19:6 21:21 22:3 real 27:21 really 8:5 29:4, 12 47:17 51:2 realtime 36:17 reason 4:21 reasons 43:1 recall 6:25 33:3 receive 36:19, 21 37:6, 8, 20 47:13 54:2 received 10:20 49:1 53:22 receives 12:9, 11, 13, 16 34:15 37:25 49:12 receiving 12:22 Recess 9:2 11:8 34:24 recollection 43:21 record 8:10, 25 9:1 11:7 25:19 34:22 54:25 reduced 56:9 REED 2:7 refer 26:1 27:1 34:1 reference 14:15 referenced 43:13 referring 14:11 22:18 32:13 37:14 Registered 56:4, 22 relationship 52:11 relationships 52:1 relative 5:7 relays 26:6 rely 29:4 remember 33:1 41:20, 24 42:21 remotely 1:14 2:2, 5, 9	remove 48:22 50:3 53:21, 24 54:6 repeat 5:19 8:22 rephrase 25:14 44:7 Reply 3:16 5:6, 8, 10, 22 6:16, 17 13:20 39:7 REPORTER 3:4 15:2 54:24 56:5, 22 representation 41:23 represents 50:7 51:15 Requests 15:2 54:24 requirements 19:23 25:13 30:17 re-read 6:19, 21 15:19 research 43:11 respond 25:5 responding 34:17 response 32:19 restate 40:21 restrictions 16:20 review 6:11, 15, 22 reviewed 6:19 21:10 reviewing 21:14 right 13:23 19:2, 8 36:13 38:6 40:20 41:20 50:22, 23 53:2 risk 38:14 rod 28:19, 20 room 5:19 Rooney 1:15 56:4, 21 Rough 55:1 row 39:22 40:3 RPR 1:15 56:21	rule 17:7, 9, 10 18:3, 23 19:15, 20 20:2, 4, 7 23:17, 18, 23 30:23, 24 39:19, 22, 24 42:2 46:15 48:16 50:6, 15, 17, 19, 23 51:3, 14, 16, 17, 18 52:1 rules 7:21, 25 8:14, 17 10:8, 9, 12, 14, 24 12:7, 10, 12, 16, 25 13:3, 4, 9, 12, 14 16:14, 22 17:1, 20 20:1, 12, 14, 18 23:12, 16 28:2, 23 30:24 31:12, 13 33:16 41:11 44:9, 10, 14, 16, 17, 19, 20, 23 45:5, 9, 12, 14, 17, 18 47:6 48:2, 5, 13, 18, 20 49:23 52:7 53:15, 25 54:5, 8, 16, 17 ruleset 14:19, 24 15:1, 5, 10, 11, 13, 16, 22 17:22 18:6 30:2, 9, 11, 14, 15 31:6 32:5, 7 35:14, 18, 25 36:7, 19 37:1, 9, 20, 21 48:1 51:4 rulesets 15:25 16:6, 13 17:3, 14 19:25 23:11 29:20 32:4, 19, 25 33:4 34:5 35:17 37:24 38:25 45:14 50:11, 14 52:5 ruleset's 15:17 < S > San 2:8 saw 34:8
---	---	--	---

says 10:11 12:22 18:22 19:9, 14 33:16, 19 35:15, 21 36:21 47:24 49:4 50:16, 17 51:13 SCPI 42:14 43:4, 9, 21 seal 56:19 Second 2:7 8:9, 25 12:25 13:3, 11 39:14 security 7:20, 25 8:13, 17 10:6, 10, 13, 15, 16, 19, 23, 25 11:1 12:5, 7, 12, 14, 15, 17, 18, 23 13:5, 9, 13 23:14 28:7, 8 29:3 38:14, 15, 25 43:1 52:18 53:13, 15, 19 54:9, 12, 14, 15, 18 see 8:8 12:19, 22 14:18, 21, 24 15:20 18:4, 21 19:11, 18 24:2 33:8, 15, 17 34:3 35:10 38:16 39:18 41:7, 11 42:11 send 24:24 sense 33:12 sent 13:12 37:10 sentence 19:13 separate 17:19 22:10, 23 27:14 31:22 separating 23:2 serve 52:11 server 10:15 12:8 13:9, 12 24:2, 7, 23 25:4, 8 28:10 38:16 53:14, 20, 24	54:13, 16 serves 38:21, 23 service 52:16, 19 set 7:21, 24 8:8, 13, 16 10:7, 9, 12, 14, 24 12:6, 9, 12, 13, 16, 25 13:3, 4, 8, 11, 13 16:23 25:25 52:7 shelf 29:2 shorthand 56:8 should 20:3 showing 14:11 25:4 shown 14:22 shows 13:25 14:19 15:15 26:3 30:6 39:25 40:17 42:10 side 24:14, 15, 23 41:1 sides 30:25 sign 55:4 signature 56:19 simple 16:11, 13, 14, 22 single 14:1 sits 21:7 sitting 22:15, 17 23:1 43:20 six 7:10 slow 8:22 SMITH 2:7 software 28:10 34:13 somewhat 27:17 sorry 4:20 6:13 8:20 14:12 18:17 19:7 22:1 32:11 33:9, 11 42:6 48:8 54:19 sort 47:14 sorts 27:20 source 36:8 49:4 50:19	sources 34:16, 17 43:24 44:2, 4, 16 45:3, 4 46:20, 22 47:1, 4, 5, 10, 11 48:15 49:1, 3, 19, 20 51:6 speak 26:14 specific 15:21 27:2 28:1 30:17 33:3 43:6 47:13 specifically 13:20 14:23 39:10 47:23 53:1 specified 15:20 specify 16:25 speculate 43:13 spends 33:13 spent 6:6 Ss 56:2 standard 41:22 standpoint 51:25 52:3 start 25:6, 7 State 1:16 36:13 38:13 56:2, 6 STATES 1:1 10:18 13:8 32:21 53:18 station 26:7 stop 16:13 17:14 23:24 50:24 stopping 50:23 store 35:11, 13, 18 36:1, 19, 22, 24, 25 37:3, 6, 8, 10, 20, 25 stored 35:18, 22 37:10 53:22 stores 35:14 straight 29:7 Street 2:7 subscribes 52:8 substation 27:24 subsystem 23:2 24:2, 5, 8, 9 30:18	subsystems 21:3, 7 Suite 2:7 supplier 52:22 sure 31:3 41:25 45:10, 14 49:19 switch 16:12, 15 switches 16:12 27:19 28:20 sworn 4:7 system 18:24 19:16 25:13, 17, 21, 24 26:2 27:6, 7, 8 28:14, 15, 19 29:10, 14, 23 30:10 32:14, 18, 23 33:22 34:12 36:4, 5 37:16 43:16 45:20 49:6 systems 27:11 28:22 46:2 47:15 < T > table 39:19, 22 41:12 tables 18:23 19:15, 20 20:7 take 17:11 27:22 34:23 36:12 40:2 51:16, 17 taken 1:14 9:2 11:8 34:24 56:8 takes 52:7 talk 16:21 24:23 31:24 32:3 talked 30:21 31:23 talking 24:15 28:9 33:14 36:3, 23 talks 15:10 28:25 29:17 34:5, 9 35:11 37:5, 11, 23 42:3, 8, 14 43:17 tank 26:8 TCP 25:6, 7 41:15
--	---	---	--

TCP/IP 24:24 26:17	today 4:14, 22 7:2 21:11 43:20 top 42:15 to-wit 4:2 10:3 12:3 35:3 TRADEMARK 1:1 traffic 7:22 8:15 18:4, 11 20:7, 15, 17, 19 23:15, 19, 20, 24 24:16, 20 29:19 30:7, 12, 16 31:1, 4, 7, 18 40:8 50:23 transcript 54:25 Transcription 56:10, 12 transmitted 10:14 traverse 24:16 25:2, 3 traverses 20:17 24:20 traversing 7:22 8:15 20:8, 15 23:24 26:16 30:1, 7, 22 31:1 trigger 19:23 triggered 34:8 true 51:14 52:18 56:11 trust 49:21, 24 50:21 51:10, 19 52:15, 17, 20 trusting 51:2, 5 trustworthiness 52:10 trustworthy 52:2 truthful 4:22 try 5:19 36:15 42:23 49:18 trying 8:20 33:1 36:10 49:16 turn 7:14 13:19 18:15 26:6 32:10 38:6 47:22 52:24	two 6:5 21:5 41:21 48:8 50:2 type 42:3 43:14 44:12 45:20 49:25 types 16:13 34:18 typewriting 56:9 typically 46:1, 10, 11 47:1 < U > U.S 1:3 UDP 17:23, 24 18:7 23:18, 19, 21, 24 40:11 41:15, 23 unable 29:12 uncommon 47:13 understand 4:13 5:18 7:23 8:16 10:8 13:2 14:14 21:16 31:3 53:12 understanding 17:5 21:22 22:4, 7 25:11, 16, 20 28:21 32:2, 22 35:16 36:20 37:18 39:21 45:11 unfiltered 29:8 unique 27:6, 10, 11 30:17 uniqueness 47:8 UNITED 1:1 unwanted 18:25 19:16 update 13:13 32:19, 24 33:3 34:2, 4 54:4 updated 12:25 13:3, 8, 11 37:9, 12, 21, 24 updates 32:24 34:1 updating 13:4	use 15:24 16:6 26:15 27:22, 23, 24 43:2 46:2 56:9 usually 16:20 45:22 UTMS 19:10 UTMS-configured 18:22 19:10 35:24 36:6, 18 37:1, 7, 19 < V > valve 28:19 valves 26:6 27:19 various 16:13 28:10 43:1 44:14 51:5 vendors 16:21 52:4 vendor-specific 47:12 verbatim 21:18 verify 51:1 versus 27:15, 16 43:2 vet 51:9 vetted 51:7 vetting 51:4 video 7:6 VIDEOCONFERE NCE 1:5, 13 view 52:2 viewed 47:19 visual 36:10 < W > waiting 49:25 walked 48:9 want 26:18 28:17 32:5, 6 33:5 39:10 46:17 49:18 50:24 wanted 49:17 wants 24:8
------------------------------	--	--	--

way 18:6 22:25 31:2 33:2 46:8 49:3 50:1 56:14 Well 5:17 17:7 23:9 24:15 29:17 50:12 52:5 we're 18:17 33:8 51:23 53:2 we've 30:21 34:21 WHEREOF 56:18 widespread 47:9 window 39:9 within 1:15 14:12 25:13 27:5 28:4 30:18 53:23 56:6 Without 6:8 WITNESS 2:3 8:3, 6, 20 10:18 11:3 13:7, 16 15:8, 19 16:2 17:7 18:2, 10 20:11 21:25 22:7, 17 24:13, 22 29:17 30:20 31:9 32:16 33:25 35:21 37:23 39:3 40:16 44:1 48:8 49:16 51:22 52:14 53:18 55:5 56:13, 18 won't 46:13 word 21:25 22:12 44:22 work 5:23 28:13 worked 5:24 works 49:6 world 22:12 26:11, 12 27:21 would 5:10 6:6, 10 7:8 16:3, 8 17:9 18:2, 7 19:23 20:1, 6 21:14 23:9, 10, 17, 21, 24 24:16, 24	25:1, 3, 5, 6, 7 27:13 28:1, 5, 12, 14, 16, 17 29:6 30:2, 9, 11, 23, 25 31:13 33:14, 16 35:18 36:1, 7 37:9 40:10, 13, 24 41:8 42:12 43:13 44:14 45:3, 4, 15, 17, 19 46:5, 6, 16, 22, 24 47:7, 16 48:16, 21 49:13, 18 50:3, 20 51:1 wrap 29:14 wraps 29:10 write 5:22 written 53:6 < Y > Yeah 4:15 5:15 6:1, 17 7:3, 6, 17 8:6 10:11, 12, 18 11:3, 4 12:9, 17 13:7, 16 14:21 17:16 18:10, 11 19:25 20:1, 17, 24 21:5, 9, 18 22:24 25:18, 22 28:8 30:5 31:20 32:21 33:7 36:21, 22 37:11, 23 39:25 40:1, 16 41:1, 13 43:8, 17 44:8, 14 45:2, 24 46:7, 24 48:14, 24 49:2, 9 51:22 52:14 53:19 54:6, 17 Yep 7:18 yes 4:20 7:13 13:1, 22 14:17, 22, 25 16:5 18:19 19:5, 12, 19 20:1, 12, 17 21:18, 19 23:23 24:3, 6 25:18 28:17 30:13 32:5, 16	35:8, 12, 15, 21 36:5, 6 37:3, 24 38:17 39:3, 13, 20 40:7, 23 41:4, 9, 16 44:13 45:2 50:2 54:2, 7, 10, 11, 19 York 2:14 < Z > zero 47:16	
---	---	---	--