EXECUTIVE SESSION

PERMANENT SELECT COMMITTEE ON INTELLIGENCE,

U.S. HOUSE OF REPRESENTATIVES,

WASHINGTON, D.C.

INTERVIEW OF: YARED TAMENE WOLDE-YOHANNES

Wednesday, August 30, 2017

Washington, D.C.

The interview in the above matter was held in Room HVC-304, the Capitol, commencing at 2:08 p.m.



PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

Appearances:

For the PERMANENT SELECT COMMITTEE ON INTELLIGENCE:

[redacted]

For YARED TAMENE WOLDE-YOHANNES:

MARC ERIC ELIAS

GRAHAM WILSON

PERKINS COIE POLITICAL LAW GROUP

700 13TH Street NW

Suite 600

Washington, D.C. 20005

[redacted] All right. Well, good afternoon now. This is a transcribed interview of Mr. Yared Tamene. Thank you for speaking to us today.

For the record, I am [redacted] attorney with the House Permanent Select Committee on Intelligence with the majority. And also here is --

[redacted] [redacted] also with the majority staff.

[redacted] [redacted] with the minority staff.

[redacted] Before we begin, Mr. Tamene, I just want to say a few things for the record. The questioning will be conducted by staff, as you see here. During the course of this interview, we may ask questions during our allotted time period, should we choose to do so. Some questions may seem basic, but that is because we need to clearly establish facts and the underlying situation. Do not assume we know any facts you have previously disclosed as part of any other investigation or review.

During the course of this interview, we'll take any breaks that you desire. There is a reporter making a record of these proceedings so we can easily consult a written compilation of your answers later. We ask that you give complete and fulsome replies to questions based on your best recollections. This interview will be at the unclassified level.

If a question is unclear or you are uncertain in your response, please let us know. If you do not know the answer to a question or cannot remember, simply say so. You are entitled to have counsel present for this interview and you have brought them here with you.

For the record, if you can please make your appearances.

MR. ELIAS: Marc Elias from the law firm of Perkins Coie.

MR. WILSON: Graham Wilson from Perkins Coie.

MR. ELIAS: And that's C-o-i-e.

[redacted] Thank you. As I said, the interview will be transcribed. And because the reporter cannot record gestures, we ask that you answer verbally to everything. If you forget to do this, you might be reminded to do so. You may also be asked to spell certain terms or unusual phrases.

Consistent with the committee's rules of procedure, you and your counsel, collectively or individually, will have a reasonable opportunity to inspect the transcript of this interview in order to determine whether your answers were correctly transcribed. The transcript will remain in the committee's custody. The committee also reserves the right to request your return for additional questions should the need arise.

The process for the interview is as follows: The majority will be given 40 minutes to ask questions, followed by the minority for 40 minutes to ask questions. We can break thereafter shortly if you'd like, and followed by 15 minutes from the majority and 15 minutes from the minority again. These time limits will be strictly adhered to by all sides and there will be no extensions granted. Time will be kept by us, with 5- and 1-minute warnings, respectively, when appropriate.

To ensure confidentiality, we ask that you do not discuss the interview with anyone other than your attorneys. Our record today will reflect that you have not been compelled to appear here; you are doing so voluntarily. You are reminded that it is unlawful to deliberately provide false information to Members of Congress or staff.

Lastly, the record will reflect that, again, you are appearing voluntarily for this interview and it will be under oath.

Do you understand everything that I have said?

MR. TAMENE: Yes, I do.

[redacted] Would you raise your right hand so I can swear you in?

Do you swear or affirm the testimony you are about to give is the truth, the whole truth, and nothing but the truth?

MR. TAMENE: I do.

[redacted] Thank you, Mr. Tamene. I'll turn it over to my colleague for questioning.

EXAMINATION

BY [redacted]

Q Mr. Tamene, thank you for being here. What I preliminarily would like to do today is sort of walk through the period from approximately September 2015 to April 2016. Before doing that, I would just like to set the stage with a little background information.

Currently, what is your job title, roles, and responsibilities as of today?

A As of today, I serve as the IT director for the DNC.

MR. WILSON: One thing before we go further. Yared goes by Yared Tamene. Do you want to give him your full legal name for the record?

MR. TAMENE: I'm sorry. My full name is Yared Tamene Wolde-Yohannes. That's spelled W-o-l-d-e, hyphen, Y-o-h-a-n-n-e-s.

BY [redacted]

Q So you said IT director for the DNC?

A Correct.

Q Which is the Democratic National Committee?

A Correct.

Q And what is your employment relationship with the DNC?

A I work under a contract with the DNC. I work for a company called the MIS Department, which stands for the Management Information Systems, Incorporated. And I -- there's a contract that exists between the MIS Department and the DNC, and it has -- embeds roles, embeds personnel like myself in the DNC. So one of those embedded roles is the IT director, which I fulfill.

Q And do you know how many people work for the DNC from the MIS Department, pursuant to this contract?

A It varies. There are currently I believe seven personnel, including myself, who serve in various roles within the technology department as a whole.

Q And what are your -- as the IT director for the DNC, what are your primary roles and responsibilities?

A Are you asking me that question at present or in the timeframe you mentioned at the beginning?

Q First answer right now.

A Right now. So my role is -- well, I share the IT director role per se now with another individual. And that role has the purview of overseeing the systems engineering team that works on DNC systems and overseeing the help desk team, which is the team charged with supporting staff, like printing issues, installing applications, that kind of stuff. And I would receive staff training for people who start -- interns or individuals who start jobs at the DNC.

I also oversee the IT budget, manage vendor relationships, and manage the toolsets that are used by various departments within the DNC.

Q And how long have you served as the IT director for the DNC?

A I -- January of 2013. And prior to that, I was -- the IT director role

was split into two. There was an information services role, and there was a systems director role in 2011 and 2012. And I served as the information services director in 2011 and 2012.

Q Since you began your current position in 2013 --

A Correct.

Q -- at a high level, how have your roles and responsibilities -- you indicated that your roles and responsibilities might have changed or evolved during that time. Can you walk us through that?

A Not during that time. Recently, only because I've been sort of preparing for a vacation, and so there's someone covering for me is what I mean to say. I'm still the IT director at the DNC. Yeah, so --

Q And the duties and responsibilities that you described then would have been roughly the duties you were performing --

A Correct.

Q -- in September of 2015?

A Correct.

Q And, indeed, since you took this position in 2013?

A Correct.

Q So, in September 2015, my understanding is that the DNC received a call from the Federal Bureau of Investigation. Is that correct?

A Yes. There was a phone call from an agent at the Federal Bureau of Investigation that was placed to the main DNC switchboard. That call was transferred to the help desk, and a help desk personnel answered and transferred that call to me. And I took that call.

And in that conversation with the person on the other line, I was asked if I



PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

was able to corroborate, to look into specific activities that the FBI had noticed emanating from the DNC network that could be nefarious, and if I could take a look at our systems to see if I can corroborate that -- if I could find any evidence to corroborate their suspicions.

Q How did you respond to this individual?

A So, after this call, the first thing that I did was start looking with my colleagues as to our firewall logs, our system logs, to see if we can find evidence to corroborate what the person on the phone had said.

Q Which was? What was he telling you that you should be looking for?

A He said -- I remember specifically he asked for us to look at email -- I'm sorry, not email -- web traffic that was hitting a website that ended with forward slash [redacted]. That was the only information we had. The agent didn't provide us with timestamps, meaning the date and time as to when that traffic had occurred or the destination IP address or the source from whence that traffic was coming.

So I informed my direct supervisor, Andrew Brown, about that conversation and our efforts to investigate and corroborate, corroborate the information that we got from the phone call. And we found nothing. We couldn't confirm the type of traffic that the FBI agent had mentioned on the phone.

Q Now, in addition to this [redacted] marker, did the FBI agent mention anything about attribution, what group or entity might be behind this activity?

A If I remember correctly, in that phone call, he had mentioned that the adversaries that may be on our network were referred to as Dukes, D-u-k-e-s. And we did, me and my colleagues, looked at any article we can find about Dukes.



PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

And we found one.

And one of the things I should mention that the FBI had requested was that, if we do any investigation, we should do it in as stealthy a way as possible so that, in case his suspicions were proven to be true, that there were adversaries on our network, we wouldn't tip our hat to them. And so we did.

So we looked at systems -- at articles using systems that were not DNC systems or on the DNC network to read up on what the Dukes were. We found one article, if I remember correctly, that was written by the Palo Alto Network, which is a cybersecurity firm -- well, cybersecurity, a technology firm specializing in cybersecurity in Palo Alto. And --

MR. ELIAS: Conveniently have the --

MR. TAMENE: Exactly, yes. And -- but we didn't find -- so they had some markers for us to look through, and we did that as well in addition to what the FBI agent had recommended that we do. And so we looked at those items. We found nothing on our networks to suggest that what the FBI agent was suspecting were actually true.

BY [redacted]

Q So, when you did some research for Dukes, you mentioned you found one, at least one article. Did the article shed any light on who the Dukes are or were?

A I don't believe it did. Again, this was 2 years ago. I don't remember exactly what the article stated, but I don't remember thinking that these are, you know, Russians or some other entity. In that first read, we weren't actually looking for -- I mean, we -- our aim was to find tools to assist us in corroborating the activities that the FBI agent had mentioned on the phone.



PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

Q And I believe we've said that this call happened in September. Do you know or recall the particular date on which it occurred?

A I'm sorry. I do not recall.

Q So you mentioned that you talked to Andrew Brown about what you had done. Did he direct you to do anything, or what was his response?

A If I remember correctly, his response was, well, keep me posted about any findings that you have. And I did. And we had daily meetings, me along with other tech department leads. And in those meetings, I mentioned to him -- and other meetings as well in person or over the phone -- about our efforts, our findings, which were, unfortunately, none at this time. We didn't have any.

And so we -- the kinds of things we were doing was looking at it from a different perspective. Like let's say we can't find this [redacted] business, but let's see if we can find any activity that is untoward, unusual for the DNC traffic in general, right. And so we looked at those kinds of activities as well, and we found nothing that was sort of alarming or warranted further investigation.

Q Just to step back for a moment before we move forward in the timeline, had you previously, during your time at the DNC, received a call of this or similar nature from FBI, or was this the first time?

A This particular kind of phone call, me personally, was my first time. Yeah.

Q Were there other interactions you had had with FBI that were similar, or was this a sort of --

A Me personally, this was my first interaction with the -- well, relative to cybersecurity and relative to the DNC, yes.

Q Were you aware of any other interactions, even if you weren't

personally involved in them, between the FBI and the DNC relative to cybersecurity during your time there prior to September 2015?

A No, I was not aware of any.

Q So when you -- this is going to be imperfect, but I sort of want to trace the sense of urgency. When you first got the call and when you hung up the phone, if you had to sort of rank your level of concern on a level in a 1 to 10, based on everything you're dealing with on a given day, how would you have rated your concern at that time?

A Ten being the highest, is that what you're saying?

Q Yes, 10 being the highest.

A I would say -- well, given that I had a moment of 10, I can actually compare that I think effectively. I think, at that point, it was probably a four or five.

Q Okay.

A And I -- having found nothing to corroborate what the FBI had said, it didn't reduce my concern, because it's hard to prove a negative, obviously, I understand. And so I couldn't -- couldn't, you know, be definitive in saying there was nothing there, meaning we were not actually compromised. And, in fact, it's hard -- since you can't prove a negative, it's hard for anyone at any time to say we're not currently compromised, right. I'm not just talking about me or the DNC; I'm talking about anyone working in computer systems.

And so I don't think my level of concern dropped from a five at all throughout this process. And in April, once we found evidence, it went up to a 10 and stayed there for a very long time.

Q I'll try not to make today another 10 moment.

So, after you got the phone call in September, you did some initial due

diligence, didn't find anything, reported this lack of findings to your boss, but, by your account, you know, didn't forget all about it, remained at a concern level of five. What was the next development in the story? Was it another phone call that you got from the FBI?

A So yeah. So, from September through February, the conversations that I had -- so the level of engagement I had with the FBI consisted of the FBI agent, the same agent calling me or texting me at times, and I would respond back. And every conversation had to do with here's -- we've seen similar activity.

My understanding from having spoken with him -- I'm going to sort of break the timeline a little bit here to sort of make this make sense -- is that he, that the agent was speaking with other Intelligence Community agencies, and they were providing him information that was about 3 weeks or a month or so old. And so when he called in September, for instance, he was talking about activity that was witnessed by some Intelligence Community member maybe in July, maybe in August. And then, so when we spoke again in October, it was following up on potentially new activity of similar nature of concern.

Again, so the type of activity that he was being provided was the same in nature. So he wasn't raising the alarm any more than he had back in September. So that kept going through in October and November and December. And I took his calls. Every call I took -- I, you know, redoubled my efforts with my team, reported that to Andrew Brown and Dawn (ph) to look at, you know, what ways we can help corroborate this activity.

One of the things that we did exercise is that, in December, one of the thoughts that we had -- as I mentioned before, we were thinking about what other ways are there to assist the FBI's investigation or API's findings or curiosity, is we

were concerned that potentially maybe the firewall that we had in use was not capturing the types of logs that would help us definitively answer his question.

So we looked into the Palo Alto firewall, partly because of our findings from, you know, from what we found in the article in September, but that wasn't the only reason. And so we got financial, budgetary approval to proceed with the purchase, and we took ownership of that firewall in February. It took some time for it to be delivered. And so we brought it online in March and what's called in transparency mode, which means it listens to traffic in and out of your network, but it doesn't apply policy.

So we thought that was -- installing a firewall is a rather involved process. You can break a lot of things. So we wanted to sort of make sure that we were doing it correctly without disrupting services at the DNC. So we put it in transparency mode, which would have sufficed in addressing what concerns we had about the firewall that we had in place not being adequate enough to find the logs potentially. Like we weren't sure about that. That's one of the things that we did.

So December happens. And in January, the FBI agent and I decide to meet in person, and so we do. And I took with me two of my systems engineers to meet with him. And --

Q If I can just stop. No, this is all very good, but if I could, we'll stop there, come back to it and then just try to fill in a little bit of the -- make sure I understand everything that happened between September and January.

A Sure.

Q So the first call was in September. You mentioned that there were repeated contacts between yourself and the FBI agent between September and

when you finally met in January.

A Correct.

[redacted] September of 2015.

MR. TAMENE: Correct.

BY [redacted]

Q Do you recall or can you sort of estimate the number of contacts, phone calls, text messages?

A I don't know if I can -- it wasn't daily or weekly, by any means. I would say at least monthly. That's probably the best I can do. At least monthly.

Q And, generally, when you received a call or a message, would you respond or reply?

A So I actually never got a situation where -- I think I might have gotten some missed calls from him, but I never called him myself directly. And that wasn't me trying to be coy or anything like that. It was simply a matter of timing. And so, if I missed his call, he would call back and I would talk to him, I would take his call. I never, like, not answered the phone because he was calling me, anything like that.

Q And was it the same one individual that you had contact with during the time --

A In the time period you described, yes.

Q -- between September and January?

And you mentioned that you continued searching for but did not find any evidence of the threat vectors that he was referencing. Did you communicate back to him that you had not found what he had --

A Correct.

Q -- asked you to look for?

A Well, yeah. I'm sorry. Threat vector is probably not the right term I would use in this context. It's actually -- we're looking at logs that capture web traffic, internet traffic, computer traffic between computer hosts, between the DNC network and the internet itself, and then back from the internet to the DNC.

That was the scope of work that the FBI was asking for, right. So threat vector in particular here is not -- I mean, to be sure, we did look at any threat vectors just in general to be sure, but that wasn't the kind of questions that the FBI was asking at that time.

Q Was it your impression during this time that the FBI was asking you to do them a favor, or they were trying to do you a favor, or both? I mean, can you describe for me what you thought was going on, in terms of -- what was the objective of this information exchange, as you understood it at the time?

A I wouldn't use the word "favor" in either direction, but I would say that the information that the FBI was providing honestly was frustrating in how redacted it was, I would say. But I was grateful that they were talking to us at all, obviously. You know, if you are responsible for a computer system and someone who -- you know, who's in the know, for instance, like the FBI would be in the know tells you there's something wrong, you take that seriously, obviously. And I took it very seriously, which -- and I don't know if I would characterize it as us doing -- the DNC doing the FBI a favor or the FBI doing the DNC a favor. I think it was someone saying that, you know, there's something that I think you can help us with, and it would help you to help us with it. So I don't know if it's a favor per se.

Q During this time, September to January, were you keeping Andrew Brown apprised of your interactions with the FBI?

A Yes. And so, in keeping with what the FBI had requested in the first conversation that we had in September, I did not write down these things on DNC systems and/or email these things to Andrew Brown, because, again, if what the FBI was saying was true, in the worst case scenario, these adversaries could be on our network listening and watching all of these activities. And so I didn't want to tip our hat. And so all the conversations I had with Andrew Brown were either in person or over the phone, but I did -- for every conversation that I had with the FBI, I informed him of that conversation.

Q And then, once you shared information with him, did you have any visibility into what he subsequently did with that information?

A Not at the time, I did not, no.

Q During this time period, September to January, did you do any more research on who the Dukes might be or who the identity of these actors were that you were looking for?

A Well, yes. My team did some investigations around the Dukes. Part of the problem is that the sort of nomenclature here is interesting here -- or challenging. Dukes are referred to by other cybersecurity firms by other names. It turns out, in hindsight, Dukes are the same as APT-29. APT stands for advanced persistent threat. And that's their sort of most common name now, but they have a lot of other names, including Cozy Bear, which is the name that we ended up using in April.

So I can't remember which entity -- I think Palo Alto may have referred to them as Dukes and maybe one or two other firms, cybersecurity firms. Definitely, the FBI referred to them as Dukes. And so it was hard for us -- I didn't see the linkage between Dukes and APT-29 at the time. And so that might have hindered

our ability to sort of figure out what signatures, what types of things to look for specifically.

I did ask the FBI for any information they could provide towards that end. And after we met in person in February -- did you want me to go that route or stop?

Q One last question on this time period. When did you -- when did you first -- it may or may not be about this time period. When did you first affiliate these actors, however named, as potentially being attributable to the Russian Government?

A So the first -- if I remember correctly, the first time the FBI agent mentioned Russia I think was in a phone call I had with him in November of 2015.

Q So it was -- it would have been during this time period?

A Correct. But he didn't give me any more -- he didn't say Russian state-sponsored actor. He said Russians in general. And -- at least I don't remember him saying Russian state-sponsored actors. And I don't know if that would have made me more concerned or less concerned or equally concerned, whether he threw in the word "government-sponsored" term or not.

However, once we met in person in February, I -- one of the things that he did was provide us with four or five sheets of paper that were cut, you know, a regular 8-and-a-half-by-11 sheet of paper that was cut into pieces, so four or five strips stapled together. And there were one line, one or two lines per page that were timestamps of the kind of activity that he had mentioned in September, the [redacted].

Now, the IP address and the actual web address was redacted. The only thing that was present was the [redacted] and the timestamp. But I should mention

timestamp is hugely helpful in sort of narrowing down when things happen, which we didn't have beforehand. I want to stress that, right. So that was huge for us. You know, still redacted, still limited, but great, let's go see if you can find this information to corroborate what the FBI is telling us.

And so we did. We went in and looked at our firewalls again. And in February, remember that, at this time, we had a new firewall, but we hadn't put it in place yet. So we were looking at the old firewall logs. And so -- and even if we had the new firewall, that firewall would not have had the opportunity to look at the timestamps that were in the past, correct.

And so what we did was looked at the logs that we had, looked at timestamps. We expanded the timestamp. These were, if I remember correctly, December 2015 timestamps. So we looked in November through January to see if just in case time zones and whatever were different. And we didn't find anything to corroborate what those strips of paper had mentioned.

Q So let me just catch up on a -- make sure I have everything straight. So you made the decision to obtain a new firewall when, in January?

A No. I mean, we had -- we had made the decision to obtain a new firewall months before. We were able to secure the funding, but -- get approval to spend the money in December of 2015.

Q And was the decision or desire to get a new firewall because of this specific incident or just a general desire to improve?

A A general desire to improve cybersecurity at the DNC. That's always the case. You want to improve your systems. You want to improve -- I don't think it's unique to the DNC. You want to improve your posture. As the adversaries are improving their tactics to sort of compromising your systems, you

want to be able to sort of meet them where they are or be better than that.

And so one of the things that we did, you know, in 2013, we got a new firewall. And in 2015, we got a new firewall again. And I'm sure we'll get a new firewall, you know, as soon as one is appropriate for the DNC.

Q And what triggered the decision to meet with the FBI agent in person?

A Well, I don't know if it was one thing. I think it made sense to meet with him. You know, phone calls over the -- you know, every several weeks over the past few months yielded no results, and I was hoping he would give us more information in person. And he did. I mean, the timestamp things were real. And I -- he made it sound like when -- during that first -- that in-person meeting that he was trying to get us more information. And this is what he was able to do in terms of the timestamps, for instance, right.

Q This first meeting was in February?

A Correct.

Q And who else attended from the DNC side?

A Two of my assistant engineers on my team.

Q Who are subordinates to you?

A Correct.

Q So you were the senior representative --

A Correct.

Q -- from the DNC?

A Correct.

Q And then, on the FBI side, do you recall who attended the meeting?

A Just one person, the same agent.

Q The same person that you had talked for a while.

So you have this meeting in February. He gives you this redacted timestamp information.

A Correct.

Q You then go and search for it and still do not find anything that matches that activity?

A Correct. Can I add more?

Q Yes.

A So --

Q We're in February.

A Yes. So in Sept -- I'm sorry, not September. In February, after the in-person meeting, after we were -- we failed to corroborate the evidence that he had provided to us, the activity he had provided to us, one of the other things he did was -- so we established a different sort of secure way of communicating over email that didn't involve DNC email systems, just in case his fears were realized and we were actually compromised and the adversaries would be reading those emails. And so we used different systems to email each other.

And one of the things that the agent did was send to me an email listing personnel, DNC personnel email addresses, stating that these email addresses were sent phishing attacks by the same adversaries that he's interested in, right. And so can I confirm that these mailboxes exist and if they were -- they got an email with subject lines and so on and so on, timestamp so-and-so, and, you know, anything you can tell us about that.

So we did. We looked at our spam filters. We looked at our email logs to figure out what had happened. We confirmed that most -- I can't remember the

exact number, I'm sorry, but let's say three or four at least of the email addresses that the FBI had listed were valid email addresses. And we did confirm that the subject line, email, and timestamp were valid, and emails were sent to those mailboxes on those dates with the subject lines that matched what the FBI had said.

The only problem is that they didn't actually make it to the mailboxes themselves, because our spam filter had caught them all as phishing attacks and blocked them from being delivered. We confirmed that they didn't actually make it. We sent him evidence to confirm that back in email form to the FBI.

And then, at that point, he -- another FBI agent joined the conversation -- whose name I can't remember -- but he had similar questions. This is in February, late February-March timeframe of 2016. So that conversation, that thread happened maybe two or three times I want to say with specific emails being sent to specific email addresses and us looking at it. And I think of all of them, one email had been delivered to a mailbox that was a phishing attempt that we confirmed using our spam filter logs and exchange logs, but we confirmed that that was not actually opened. It was immediately deleted.

And so phishing attacks, their nature is to sort of coax the recipient to clicking on a link and divulging confidential information. So, obviously, we were concerned about that even before the FBI told us about these things. We have spam filters and other checks to make sure that that doesn't happen, to help us ensure that doesn't happen.

Yes. So the conversation went from [redacted] to specific phishing attack targets, mailboxes, and then -- and so, you know, we responded as quickly as we could, which meant maybe hours, days. I don't remember the exact -- how long it



PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

took us, but we wanted to confirm what he was saying before we responded.

Then came the next question from the FBI, which was I want to say early April of 2016, where the FBI asked us to provide them logs, which is, in effect, metadata about emails, from our exchange servers. And so, at that point, the question was more involved than confirming something that's going on on our network. So I raised the question, as I have in the past with Andrew Brown, about what our engagement should be, you know, and that I'm engaged with working with the FBI, cooperating with the FBI as best I could. But I knew that us giving information of the kind that the FBI requested would require some legal assistance. And so I sort of insisted, if you will, that we bring in DNC legal counsel and the COO of the DNC.

Q Could you name those individuals?

A Well, Graham Wilson is one of the DNC counsel. And the COO at the time, the chief operations officer at the time, was Lindsey Reynolds. And so I walked to her office with Andrew and said: Here are the things that I need help with. I would like to give these logs to the FBI, but obviously, I can't do that without your permission, without legal counsel permission. So let's see if we can get that.

And so one of the things I should mention here is that gathering the logs of the type that the FBI requested is not a simple matter. The kinds of logs they wanted were rather elaborate, and it would take -- I think they ended up being something like 15 gigs of data, which is significant. You can't just email that to somebody. That's a lot. Even just downloading it ourselves into sort of a searchable format would take days to do, right.

So I asked my systems people to start doing the work. Even if we didn't

get permission, we weren't going to get permission, it doesn't matter, let's just -- I didn't want to make this wait. You know, once we had approval, I didn't want to make them wait another 2, 3 days. So they started working on that. And we got on the phone.

MR. ELIAS: With who?

MR. TAMENE: I'm sorry, with Graham Wilson and another partner at Perkins Coie, Michael Sussmann, who worked -- who works at Perkins Coie, but before then, he's worked at the U.S. Department of Justice on the cybercrime and intellectual property section. So he had lots of experience with this type of request, activities. And so I described --

MR. ELIAS: I'm going to cut you off on what took place with legal lawyers.

MR. TAMENE: Sure. So --

MR. ELIAS: I tried to give you enough on the record so you get a flavor, but not with respect to the specifics of the conversations.

MR. TAMENE: So we eventually delivered those logs. I think the actual date that we were able to get it to the FBI was 10 days later. So like April 29th I think was the date that we actually sent them the logs. And the FBI agent confirmed receipt by sending me a text message saying: You know, thank you for sending that. That's great, very helpful. I'll let you know what we find.

MR. ELIAS: I never texted with an FBI agent before.

[redacted] It's not that great.

BY [redacted]

Q So, at that point, you still had not corroborated any activity that was particularly concerning or that the FBI had told you to look for, correct?

A Well, when you say "that point," what point is that?

Q When you delivered the logs on --

A Interestingly, I had. So April 28th is the first day that we found activity on our network that was unusual, nefarious by adversaries. It just so happened that April 29th was when we were able to gather all the information, get all the approvals we needed, and send that information to the FBI.

Q And how did you detect this anomalous or concerning activity on the 28th?

A On the 28th. So we saw sort of very loud activity, if you will, on one of our Window servers that couldn't have been done by one of us, right, an authorized user. The kinds of activity we were looking at was accessing multiple different password vaults of different users, which is not something that anyone would do. And so that triggered an alarm for us, and so we started looking at I want to say like maybe 11 a.m. on Thursday, April 28th, I believe, right around that time.

Q Ballpark.

MR. ELIAS: Give or take a few minutes.

MR. TAMENE: Yeah. And I mean this is when it went to 10, right, I remember that. And so I spent with my team, maybe three or four of us on the phone, using systems that were not, again, DNC systems to communicate and collaborate all day long, almost all night long, on what kinds of activities we're talking about.

And what we were looking there was sort of two things. One is make sure that whatever we do is not being noticed by these potential adversaries. So, again, I want to say here that we weren't sure that there was one or more adversaries. We were sure that we had probably unauthorized access. It could

be that an application was doing something weird. We have that all the time where an application, for instance, installed on a computer scans all the computers around it to be able to talk to them that looks nefarious, but it's just benign and really silly, silly coding, if you will.

So we weren't sure if that was what was going on, but we wanted to be certain. So we were looking at every log, every access, that was every new user created, every password change that happened on the network from about 11 a.m. until I think we fell asleep at like 3 a.m. I told Andrew that we were doing that. And, you know, I think I went to bed at like 4 a.m. and was back at it at 8 a.m. with my team, and we spent all day doing more of that kind of work to sort of pick up the scope of the problem.

BY [redacted]

Q Which was -- the next day being the 29th?

A The 29th, Friday.

Q Which is the same day you delivered the logs that the FBI had requested?

A Right. They were finally ready. So we -- I mean, we probably started doing the upload on Wednesday. I don't remember, but probably Wednesday, then let them go for -- until Friday, and then Friday finally sent them an email saying: Here's the information; here's the password to download the information.

Q So -- and I don't mean to cut you off, but I just want to get through a couple more things before turning it over to my colleague, and we can circle back, if necessary, later.

So the loud activity that you noticed on the 28th, that was not necessarily

something that the FBI had told you to look for or didn't necessarily relate --

A Correct.

Q -- to your conversation with the FBI?

A Correct. It had nothing to do with anything that the FBI had said up to that point.

Q Right. And, indeed, up to that point, you had not corroborated any of the activity that the FBI had --

A That's true.

Q -- engaged with you?

A That's true. I want to also say that the actors that we noticed, it turns out, on the 28th of April were different actors than the FBI had been looking at. These Dukes and APT-29, they were different than those. That was Cozy Bear that the FBI was talking about. What we found was another one called Fancy Bear or APT-28 on April 28th, right, unfortunately.

Q 28th and 29th and --

MR. ELIAS: Good luck to you.

MR. TAMENE: Sorry about that. That's just a coincidence. So yeah. And -- right. So did you want me to --

[redacted] Well, so the -- I think we may get more into Fancy Bear.

MR. TAMENE: Sure.

[redacted] But --

MR. ELIAS: Which is 28 or 29?

MR. TAMENE: Fancy is 28.

BY [redacted]

Q Which you discovered on the 28th?

A Correct.

Q And then the logs related to the FBI's Cozy Bear inquiry turned over on the 29th and related to 29.

A Yes.

Q So, basically, at least up until late April, looking back, why do you think you were unable to identify the actors that the FBI was alerting you to over basically a period of seven or so months? Was it the status of the DNC's systems? Was it the skill of the adversary? Was it the incomplete information of the FBI? Can you weigh those factors as to why? Setting aside Fancy Bear and everything that happened later --

A Sure. Just Cozy.

Q -- on the Cozy Bear, it's basically a 7-month engagement with the FBI that at least up until that point was not particularly fruitful. Why, in your opinion?

A Well, I -- my opinion here is formed by what CrowdStrike, the firm we ended up engaging with to help us through this, these cyber attacks. And I want to stress here that I don't know if it was one thing. I think it was a combination of things. And I don't know if I can weigh any one of them more importantly than another one.

I do know that the reason -- I'm sorry -- the way in which we were able to discover Cozy on the DNC network eventually was using toolsets that were provided to us through CrowdStrike [inaudible] CrowdStrike. I don't know for a fact whether or not we would have found out about Cozy Bear on our own, given the toolset that we had. I don't know that we wouldn't have found out about them specifically. There are lots of things one can do, given the right amount of time

and opportunity to figure out what's going on on one's network from activities carried out by these advanced persistent threat people, 28 and 29 specifically.

And it's important for us to note that those activities may have triggered an alert that we already had set up or may have gotten us -- you know, once we had tweaked some firewall holes, once we had turned on some future sets in the new firewall set that we had that could have caught them. I don't know, to be -- I can't tell you for sure.

I want to say that we stopped looking for what-ifs as soon as we had CrowdStrike in place, because they're experts in the field, and they had toolsets that were able to get the full scope and nature of what was going on relatively quickly, within, I don't know, a few days of us engaging with them.

[redacted] Thank you.

[redacted] We can go off the record. We're going to flip spots.

[Recess.]

[redacted] We can go back on the record. It's 2:58.

Did you say 40 or 45?

[redacted] Well, I took 45, so you can have 45.

EXAMINATION

BY [redacted]

Q Mr. Tamene, again, my name is [redacted] I'm with the minority staff. On behalf of Ranking Member Schiff and the other Democratic members of the committee, we thank you for agreeing to be here voluntarily to talk with us as part of our investigation. As you probably know, this is a bipartisan investigation looking into four key questions, as approved by the chairman and the ranking member of this committee earlier this spring in March.

The first area we're looking into is, what Russian cyber activities and other active measures were directed against the United States and our allies?

The second question we're looking into is, did the Russian active measures include links between Russia and individuals associated with political campaigns or other U.S. persons?

The third area we're looking into is the U.S. Government response to the Russian activities and what we need to do to protect ourselves and our allies going forward.

And, finally, we're looking into possible leaks of classified information related to the Intelligence Community assessment. You may be aware of the unclassified version of that assessment.

I think I'll start off just continuing where my colleagues left off.

A Sure.

Q So I understand, on April 28th, you discovered this loud activity that we now know was Fancy Bear.

A Correct.

Q Okay. At that time, did you report that discovery to your colleague at the FBI?

A On Friday, I did. On Friday, April 29th, I sent him a text message, several text messages. One of them was: I think we found something that's worth talking about.

And I also said: By the way, I've just sent you a link over email with the logs that you requested maybe some 10 days ago.

I can't remember the exact date that he requested them. And he wasn't able to talk on the phone that night. He was busy at some sort of triathlon or

triad, as an FBI agent would be.

And so he said: I won't be able to help you tonight, but, you know, if you need anything over the weekend.

And I said: Okay. I'll keep that in mind.

And the following day -- I'm sorry, that evening, I spoke with the chief operating officer at the DNC, COO Lindsey Reynolds, and I -- and obviously, also Andrew Brown, and she convened a call the next day, Saturday.

Q April 30th?

A Correct. With legal counsel and Amy Dacey, who served as the chief executive officer at the DNC at the time. Obviously, Lindsey Reynolds, obviously Andrew Brown. And we got on the phone. We spoke at length about what we had found and that we need help and to sort of figure out what we can do next.

And so, thankfully, one of the people on the phone was, I had mentioned before, Michael Sussmann, who knows a lot about this space and knew Shawn Henry from CrowdStrike as well. And so we got on the phone with Shawn Henry, who's, you know, a former FBI employee, served as executive assistant director investigating cybercrimes, which is the kind of expertise that we needed. And so we got on the phone with Shawn Henry and another gentleman named Chris Scott, who worked for CrowdStrike. And so we got on the phone with them for a bit. So we sort of gave them the lay of the land, that we had been speaking with the FBI, that this could be what the FBI had been talking about with us or it could be something else. We didn't know.

And on Monday morning at 9 a.m., this is now May 2nd -- am I getting that wrong? May 1st, May 2nd, the first Monday of May of 2016. They -- I was on

the phone at 9 a.m. with a project manager that was assigned to us by CrowdStrike, "us" meaning the DNC. His name is Robert Johnson. He's a former marine [redacted]

Q And he is an employee of CrowdStrike?

A Correct. He's an employee of CrowdStrike. I was on the phone with him at 9 a.m. and sort of gave him the lay of the land. He already had spoken, obviously, with Shawn Henry and Chris Scott the night before.

And so we spent the next, I don't know, 12 days straight it feels like doing a plethora of activity in trying to figure out -- and deploying a bunch of toolsets and -- stealthily deploying, I should say, a bunch of toolsets on DNC computers to assess what was going on on our network, so to better monitor as many endpoints as we can possibly monitor. Right. And so --

Q Was Mr. Johnson or CrowdStrike able to see the same loud activity that you had seen?

A Yes. I'm trying to remember now. I'm sorry. I don't remember the exact date that they said there's -- these are APT-28 and APT-29 on your network. In fact, I think they found one of them first and the other one later, like a day or two later. I can't remember the exact date. I'm sorry about that.

Q No, that's okay. Do you know like approximately how many days after you engaged them on that Monday that --

A I think, at most, within 15 days.

Q And is it fair to say they discovered these two actors prior to the FBI identifying these two actors?

A Well, so the FBI had already identified APT-29, Cozy Bear, as having

been on the DNC network. They had suspected, I should say, that the DNC network was compromised by APT-29. They hadn't given us concrete evidence to say that this was actually happening. Now, we had concrete evidence that -- from CrowdStrike's investigation that this was actually happening, both APT-28 and APT-29 were on several different DNC systems, within I want to say 10 days, 15 days.

Q How did CrowdStrike describe these two actors to you at that time? Did they understand them to be Russian derived?

A Correct. They had given them the name Cozy Bear for APT-29 and Fancy Bear for APT-28. And CrowdStrike uses terms like "bear" to refer to Russians, Russian Government-sponsored agents or adversaries. And like they use "panda" for Chinese and other things like that.

Q At some point, did you link up the FBI and CrowdStrike so that everyone --

A Absolutely. On Monday, that first Monday in May, we did. I let the FBI agent that I was working with know that CrowdStrike was engaged. He was aware of CrowdStrike and aware of their expertise. And he spoke with Robert Johnson and sent me -- the agent sent me a text message -- I don't remember the exact date, but it probably was Tuesday, Wednesday that week -- saying: I spoke with Robert Johnson. You're in good hands. Good luck. Let me know if you need help.

So, from that moment on, the FBI's requests for information were being handled directly from CrowdStrike, since CrowdStrike was the expert in the field and their requests would be better served by that kind of expertise instead of me. That was sort of me and my team handling the workflow that CrowdStrike needed

to fulfill their investigation and fulfill their forensic analysis.

Q At some point, did the FBI reach, independently, conclusions consistent with CrowdStrike's, do you know?

[3:07 p.m.]

MR. TAMENE: Well, I don't know if it was independent or influenced or -- I don't know. But I do know of reports that were published, statements and reports that were published by the FBI, the Department of Homeland Security, by the Office of Director of National Intelligence that came in the fall, in October, in December, and then in January of 2017, that had statements that were concurrent or confirmed the conclusions that CrowdStrike had reached from their analysis and their forensic analysis and their investigation of web traffic, systems logs, any unusual behavior within the DNC systems.

BY [redacted]

Q And, Mr. Brown, as you sit here, do you have any doubts about who --

A I'm Mr. Tamene.

Q I'm sorry. Mr. Tamene, do you have any doubts about the conclusions that CrowdStrike and also the U.S. Intelligence Community have come to, that Russian state actors were behind the hack?

A No, I don't have any doubts. I don't have any evidence to doubt their findings.

Q You may be aware that there have been conspiracy theories that have floated around surrounding the DNC and the hacking, that it could have been someone internal and not the Russians.

I know in one case there was a tragic murder of a former DNC staffer that has been exploited to create this unsupported theory that he perhaps was the cause of the leaks.

Have you heard of these stories?

A I have heard of some of them, and I do know -- I worked with the person you mentioned there, and I'm really sad to see that his name is sort of associated with this kind of theory.

I don't have any -- I mean, we looked at logs, we looked at end-user behaviors, activities, me and myself and my team and, again, CrowdStrike and their team of experts, not just looking at current activity but forensic activity, meaning looking back in time, on laptops, servers, desktops, you know, all the systems that we can get our hands on, to see if there's any evidence that suggests untoward or unauthorized access by DNC personnel, and we've found nothing to corroborate such theories.

Q There's also been some discussion about the DNC servers and, you know, whether they were appropriately provided to the FBI. Were you involved in that process?

A Me and my team were involved in quite a bit of that. So I can say this: So, in the end, I think there were 38, I think, systems that were compromised by either APT-28 or APT-29, some of them by both. And some of those were end-user devices, like laptops or desktops. They were of less interest to, sort of, forensic analysis and investigation. To be sure, we looked at all logs that were generated from those systems, but I think the question you're asking me about is, sort of, providing the full image or cloning the server itself.

And so we did that for, I think, 26 systems that were selected by CrowdStrike's team of experts as needing further analysis to determine the types of activities that could have been carried out by these adversaries.

And the FBI requested, I believe, some of these or all of them -- I can't remember -- these images, these clones that me and my team had worked to

clone, and we did. And we provided it to CrowdStrike, and CrowdStrike provided those images to the FBI. That happened, I believe, in the month of May and the month of June of 2016.

Q So it seems that the FBI obtained what they needed?

A Yes, the FBI obtained what they needed, definitely obtained what they asked for. I would characterize that whatever the FBI had asked for of me and my team we were able to provide, some September 2015, all the way through this whole process.

Q On July 29, 2016, the DCCC announced that it was also the victim of hacking.

A Okay.

Q Do you recall when you learned that they also had been hacked?

A I don't know if I recall the exact date. I knew that they had been hacked for sure the week after the DNC had remediated its network, meaning we had successfully kicked out the adversaries. That work started on June 10 of 2016, and we completed it, if you will -- we completed it on Monday, June 13, I believe.

And so, the week after that, I was aware that the DCCC was undergoing remediation efforts themselves, because Robert Johnson, for instance, of CrowdStrike and -- there was another team of individuals that CrowdStrike had brought in to help us with the effort of remediation to do, sort of, the legwork, if you will, on the ground. And so I knew that that team of individuals was now contracted, if you will, to work with the DCCC.

So, by those two metrics, I knew that the DCCC was undergoing. I might have known before that time, but I don't remember.

Q It's been a few days since.

A Yeah.

Q Well, according to press, anyway, thousands of documents were stolen from the DCCC by hackers, and those documents were made available to Florida reporters and bloggers. Do you recall seeing this transpire sort of simultaneously?

A No. I don't recall really anything about the DCCC outside of what I said in the months here that you're asking about at all. I was entirely too busy trying to make people have computers that work.

Q That makes sense.

Prior to 2016, had you seen any breaches of networks on the scale of what ultimately transpired?

A Nothing on the scale of what ultimately transpired. We have seen phishing attacks that were successful, that compromised some credentials here or there. We had seen ransomware, which is sort of a malicious software that an adversary would install on your computer using an attachment to an email that would then be used to encrypt a file or folder or a drive, then ask you for money to decrypt it. We've had those kinds of activities happen, and we were able to deal with those specifically without having to pay the ransom.

Q The unclassified Intelligence Community assessment reports that Russian intelligence obtained and maintained access to elements of multiple U.S. State or local electoral boards. Do you recall in your role at the DNC becoming aware of concerns at the State or local level?

A I mean, I think I remember reading a news article in the fall of 2016 that had to do with State and local voting or election apparatus being targeted. I

think one of the reports that the U.S. Intelligence Community released -- maybe a statement -- in October 2016 mentions that.

But I do think that that same statement falls short of actually attributing those activities to the Russian-sponsored -- the Russian Government-sponsored efforts, at least at that time. And I think they may have released more information in December and January after that.

Q And you mentioned in your discussion with my colleagues earlier that -- I believe it was the second FBI, sort of, request of you was to look into a series of email addresses.

A The second set of requests, yes.

Q And it sounds like you looked into those and discovered all of those were in a spam folder. Is that right?

A Spam filter.

Q A spam filter.

A Caught by a spam filter. All but one.

Q All but one. Okay.

A Yeah. All but one were caught by a spam filter. And the one that was not caught by a spam filter meant that it was delivered to the recipient's mailbox, but it was not opened by that individual. We confirmed that by looking at the logs.

Q That seems to indicate to me that your firewall worked pretty well at that point in time.

A Well, I wish. It doesn't indicate that. What it does indicate is that the spam filter, which is different than the firewall, worked really well.

Q Oh, okay. That shows my ignorance. The spam filter --

A Yes. Right.

Q That was the spam filter.

A Yeah.

Q Interesting. Okay. What would the firewall catch? What types of things?

A So the firewall would have caught if there was an attachment, for instance, to one of those emails that was nefarious. Or it would have caught a link that was embedded in an email, potentially, that went to a site that was blacklisted, for instance. Or if that traffic, once the person clicked on the link that sent them to a website that was nefarious, let's say, and that website triggered activity back to the DNC network, the firewall would have caught that, potentially. It's designed to.

Q So the spam filter is what caught these.

A Correct.

Q And that was in place before the firewall, I guess, or --

A Correct.

Q Okay.

A Yes. I mean, DNC at the time had more than one spam filter as well, but that's not important.

Q This is great, because it's very educational for me.

I would just ask you, Mr. Tamene, is there anything you think that we should know about what happened during the 2016 election that would assist in our investigation? This has been very helpful.

A Yeah. I don't know if I have, sort of, any more useful information than the answers that I've provided. I do think -- and this may not be specific to

the activity that pertained to 2016 that the DNC underwent with these attacks, but, in general, I think that the U.S. Intelligence Community does quite a good job, a great job maybe even, in assessing and analyzing all of this information. There's a ton of it.

Even just looking at the DNC itself, like I mentioned to you before, it's 15 gigs of data, which is a lot of data. And that doesn't include the actual emails, just information about emails, right? It's just metadata about emails. It's just a ton of it. And so imagine what that looks like for the entire U.S., you know, corporations, universities, and all that stuff. I get that that's a lot. And so they do quite an amazing job in looking at all that stuff and figuring out bad things, you know, that are happening.

What I would like to do -- what I would like to see, I should say, is better sharing of information at the declassified level. I mean, they do that already. They have websites, they have maybe even seminars, that kind of stuff. But these are not readily available, easily digestible, well-marketed. I would love to see, you know, a small organization like the DNC, which has a really big profile but it's a really small nonprofit organization, can use that kind of assistance from the U.S. Intelligence Community and others, potentially, right? Yeah, so I would love to see that kind of thing.

Q Is it your sense or your observation that the coordination between the DNC and perhaps other political organizations is better now than it was?

A I can't speak to that. I do know that I've had a couple of conversations -- and, you know, maybe Andrew Brown has had more; I think maybe he has -- with other organizations, political organizations, around cybersecurity. But I don't know enough about that to say more.

Q Is it your sense that the DNC is better protected for elections going forward? And, for example, if these actors were to come back, or others, would you be able to detect them?

A That's a tough question, right? So saying "yes" is terrifying, and saying "no" is also terrifying, right?

So one thing I want to say is that the business of cybersecurity, which I've now become really familiar with, is one -- really it's sort of an arms race, right? So you have your adversaries getting smarter, evolving their tactics, and then you have organizations having to do the same to make sure that they're one step, several steps ahead of the adversaries' tactics, resources, mechanisms, right?

And so I think if the question -- and I know this isn't the exact question you're asking, but if the question is, given the systems, tools, practices in place today at the DNC, could the same types of nefarious activities or threat vectors employed by APT-28, APT-29, in 2015 and 2016, could those be successful today, the answer is no. But I guarantee you that APT-28 and APT-29 is not using those tools anymore. They're using other tools now, right?

And so I do think that the DNC has, you know, and continues to improve its cybersecurity posture. I do think that in 2 years, if you ask me that same question, I would give you a very similar answer, saying we are certain that we can probably stop the attacks of 2017 in 2019, but I don't know for a fact that we could stop 2019 attacks in 2019, right?

And that's the trick, right? You have to be able to match them where they are and be better than them. And that's a continuing struggle that the DNC is investing in, has invested in, will continue to invest in.

Q How do you invest in this issue? Is there collaboration with your

counterparts, with folks in other countries?

A Well, I can give you sort of concrete answers of things that have happened at the DNC, for instance, right?

You know, one of the things I mentioned before is that we improved our firewall in 2013. We improved it again in 2015, for instance -- or 2016 is when it actually took effect. You have more frequent, more elaborate, more tricky, if you will, training sessions with your DNC users, your staff members on how to use computers in a secure fashion.

You increase your communication with staff about, you know, "If you see something, say something," kind of encouragement. You use someone like CrowdStrike to, sort of, monitor your network 24/7.

You do penetration testing, which the DNC has been doing in the past, continues to do, and will do in the future. You test your responses to incidents. So, like, I don't know -- one of my favorite things to talk about is, for instance, Netflix has -- it's a big company -- Netflix has what they call Chaos Monkey. What it actually does is goes around and turns off servers randomly to see if their systems are resilient enough to keep going, keep working. So the Chaos Monkey goes around and turns off one or two servers. They have a Chaos Gorilla which turns off entire data centers to see if they can withstand it, which is crazy.

I mean, the DNC is not doing that. But that's the kind of thing that the DNC has done, not turning things off, but pretending like things are off and seeing what happens. Sort of like, your log-in system is off; how do you know that the adversaries are doing things or not if there's adversaries on your systems. You know, if the check engine light is off, for instance, how do you know, you know, you're actually working in good shape or not, right? That's the kind of thing that

we have to keep doing, we have been doing, will continue to do.

So, yeah, I think looking at disaster repair, looking at incident response plans, looking at prevention tools like CrowdStrike's toolsets, antivirus, making sure that your systems are up to date with Windows or a Linux or a Mac operating system security patches and getting alerts when such patches are out of date. And, you know, unfortunately, it includes mobile devices now, because they're too smart to ignore, right? And so they can be hacked and used to be leveraged against your systems.

Q I think the DNC is in very good hands with you.

A Thank you.

[redacted] That's actually all the questions I have.

[redacted] Do you want to push on, or did you need a break?

MR. WILSON: Want to just power through?

MR. TAMENE: Yeah.

MR. WILSON: Let's do it, if everybody's all right with that.

[redacted] Thanks again. My name is [redacted] with the majority. I just want to ask brief questions about, basically, DNC, CrowdStrike, and the FBI.

MR. KAMENE: Sure.

BY [redacted]

Q I think you said that -- well, when was CrowdStrike brought on by the DNC?

A So the first conversation I had with CrowdStrike was a Sunday. I want to say May 1st, Sunday, May 1st, 2016. That doesn't mean that the DNC didn't work with CrowdStrike beforehand. I don't know what they did. But my engagement relative to the APT-28, APT-29 activities was Sunday, May 1st.

Q Yes. And thanks. And we're just going to discuss as it relates to what we've been talking about here.

So when CrowdStrike was brought on, and correct me if I'm wrong, I think you said CrowdStrike made the decisions over which servers to mirror, copy, slash --

A Correct. Clone.

Q -- clone. Thank you. They did that based upon their expertise.

A Right.

Q Right. So they didn't copy all the servers that the DNC has, right?

A Correct. I want to stress here, the DNC has many, many servers, hundreds. And we looked at all of them in terms of nefarious activity of any kind, not just limited to APT-28 or APT-29. I want to stress that.

And in our investigation led by CrowdStrike but not limited to CrowdStrike's experts -- I mean, my team was involved in assisting with those efforts -- CrowdStrike's toolsets found and we found evidence of compromise. And, again, I'm sorry, I don't remember the exact number. I want to say 38 systems. Some of those systems were laptops, for instance, right? And, you know, I think one or two of them were interesting enough for us to clone them to see if they had any forensic value.

Now, this is going beyond my level of expertise here. I know a little bit about what forensic analysis looks like, but I don't know enough to speak to that.

Q That's okay.

A Now, in terms of what threshold or what criteria CrowdStrike used to determine which of the 38 needed cloning, I can't speak to that with any authority.

Q Sure.

A But I do think that what they were looking at -- my understanding, at the very least, was if they could find -- if we could find, in looking further into historic logs, meaning things that happened in the past instead of things that are happening -- you know, once you take an image of the thing, it's no longer logged. Like, the image is not mirrored after you copy it. So, like, looking at past evidence of activity that they can confirm scope, nature, and, you know, various types of activities used by the adversaries.

Q So, once CrowdStrike made the determination, with your assistance, you guys working together -- and forget the technical jargon because I'm not going to get it right --

A Sure.

Q -- but whatever servers and systems were copied, mirrored, cloned, that material was given over to the FBI.

A My understanding is yes. I don't know if all of it was given --

Q Okay.

A -- but I do know that whatever the FBI asked for -- and I know this from having another few text messages with the agent at the FBI -- that whatever they asked for they had received from CrowdStrike.

Q Okay. So I just want to -- so there may be some stuff that CrowdStrike copied, mirrored, cloned that wasn't given to the FBI. You just don't know.

A I mean, CrowdStrike didn't do any copying and mirroring. We did.

Q You did.

A Yeah, provided those to CrowdStrike. And CrowdStrike may not have given all the things to the FBI, but it doesn't mean that they withheld anything

from the FBI.

Q Sure.

A I want to make sure that that's -- that's really important.

Q No, I understand that. Who at CrowdStrike would have that answer?

A Well, I mean, I spoke with Robert Johnson, the project manager assigned to the DNC. I spoke with others since then, but I don't -- I think the agent -- the FBI agent that I spoke with was speaking directly, I believe, with Robert Johnson.

Q And who is the FBI agent you were talking to?

A The FBI agent -- so I call him [redacted], Special Agent [redacted]. His first name, I think, is [redacted]

Q And so CrowdStrike is brought on on or about May 1st, 2016. The DNC's first contacts with the FBI in relation to what we're discussing here were about when?

A Say that -- I'm sorry.

Q So CrowdStrike was brought on on or about May 1st, 2016, for everything we're talking about here.

A Correct.

Q When was the DNC's first contact with the FBI in regards to what we're discussing here?

A September 2015 is the first phone call that I received.

MR. ELIAS: I think he means in May, right?

[redacted] Right.

[redacted] Yeah, just so we're clear, you engaged CrowdStrike after

you discovered --

MR. TAMENE: Evidence.

[redacted] -- evidence --

MR. TAMENE: Right. Correct.

[redacted] -- not because of the FBI contacting them.

MR. TAMENE: Correct.

MR. ELIAS: No, but I think his question is -- you were talking to CrowdStrike then. When is the first contact with the FBI subsequent to that?

[redacted] Right. Exactly.

MR. TAMENE: Subsequently to CrowdStrike being engaged?

[redacted] Yes.

MR. TAMENE: So, I mean, I wasn't on the phone with CrowdStrike and the FBI at the same time. But I did get a text message, again, from Agent [redacted] from the FBI --

[redacted] After he finished his triathlon?

MR. TAMENE: Well, I mean, I think he was done on Monday or Sunday. It was, like, some [redacted] thing is what he called it. I don't know. And --

MR. ELIAS: I don't think that's a triathlon.

MR. TAMENE: I don't know what it is. But, anyway, so he -- Tuesday, maybe Wednesday, so May 3rd or 4th is when Agent [redacted] confirmed that he had reached out to Robert Johnson, they had spoken. And Robert Johnson confirmed that, as well, on the phone.

I mean, I had a 9:00 a.m. phone call with Robert Johnson everyday for, oh, I don't know, 2 months. So one of the things that we discussed was his engagement with Agent [redacted] and their progress, if you will.

BY [redacted]

Q And so, between the FBI and CrowdStrike, did the FBI ever make a request of the DNC to have full access themselves?

A No. No, that did not -- that never happened. I think Agent [redacted] would have asked for that if he needed it. I had a good relationship Agent [redacted], still do. I spoke with him last maybe 3 weeks ago, you know, again, texting but also a phone call as well. And there's no reason to think that he was sort of shying away from asking something.

Q Sure. I'm just trying to figure out if the FBI ever, either Agent [redacted] or otherwise --

A Sure.

Q -- asked the DNC for full access to everything.

A Agent [redacted] or any other agent never asked me, and I have no reason to think they asked the DNC other personnel about this.

Q Okay. And, internally, at some point, the DNC, did they make a decision to utilize CrowdStrike services versus turning the whole thing over to the FBI? Is that a conversation you all had?

A I didn't --

MR. ELIAS: What do you mean by turning the whole thing over to the FBI?

[redacted] Well, if there was a -- so there was an initial contact with the FBI in September of 2015 and then again in the coming months of early 2016, right? And, obviously, there was something afoot. Some bad, nefarious activity was going on.

MR. TAMENE: Sure.

[redacted] So certain individuals would turn to law enforcement; other

individuals would turn to private-sector individuals. So I'm trying to figure out --

MR. ELIAS: But with all due respect, the FBI doesn't remediate your problem.

[redacted] No, I get it. I'm asking --

MR. ELIAS: So it's not an either-or.

[redacted] I believe they say CrowdStrike also sort of helped rebuild some of those systems. This is not something you would --

[redacted] I know. But I'm asking him.

MR. TAMENE: Yeah. No. I think if I knew -- which I didn't, and I still don't -- knew that the FBI offered comparable, similar type of services that CrowdStrike offered, sure, I would've probably considered them as a resource. That was not known to me, is still not known to me, that they offer those kind of services.

The kind of services or the kind of support that Agent [redacted] had provided thus far was sort of, "Hey, maybe there's something going on here. You should take a look at it."

One thing in addition to that that he did is send a script to run on our systems to see if we could find some activity. And that was in April, I think, of 2016. And we ran that script or a modified version of that script in May. And I'm really glad we didn't run the script he sent us in April, because if we had, we would've been discovered immediately by the adversaries. I'm not saying that's him being incompetent. He was giving me a sample.

Q No, and I'm not saying the FBI is the problem-solver of the world.

[redacted] Well, let me try again with an analogy, which is, if your house is -- in the physical world, if your house is broken into, ransacked, a sort of

analogous, noisy activity to what you discovered on your systems on April 28th, at the end of the day, it's not going to be the police who's going to help you get your stuff back and inventory everything. You're going to call the insurance company.

MR. TAMENE: Sure.

[redacted] But in that situation, most people's first call would be to law enforcement. Come --

MR. TAMENE: Right.

[redacted] -- collect evidence, take pictures, so on and so forth. And then you get on with whatever private-sector engagements.

Now, I'm not saying it's a perfect parallel, but I think the question he was asking is, when you discovered this noisy activity on April 28th, understanding --

[redacted] To be clear, the noisy activity, he did not know it to be a burglar, in your example, at the time.

[redacted] [redacted] we don't interrupt you when you ask questions, so please allow us the same courtesy.

[redacted] When you discovered this noisy activity that you thought -- weren't certain but, you know, strongly thought was, you know, anomalous, you know, unauthorized activity on your systems, was there a discussion of bringing in law enforcement to directly look at what had happened, see what you had seen, call the FBI into your office, sort of like you would call the police after a burglary?

MR. TAMENE: So I did. I mean, my text message to the agent, Agent [redacted] of the FBI, on Friday, April 29th, yes, was saying, "Hey, I think we found some evidence that suggests nefarious activity on our network. Do take a look at the logs that I sent you." My hope was that the log that I sent him would

corroborate the evidence that we found. Turns out that it didn't, but that was one of the things that I was hoping for.

And he was, you know, gracious and responsive even though he was, you know, doing whatever he was doing. He said, "Let me know if you need any help over the weekend."

And, you know, by the time -- you know, the following day was Saturday. We had phone calls with, like I mentioned before, with folks who knew what they were talking about in the cybersecurity space and then again on Sunday when CrowdStrike was brought in. And by then, you know, the kinds of expertise that I was getting, that the DNC was going to get by Monday was, you know, sufficient, right? My fear level, which was a 10 starting Thursday, maybe went down to a 9, maybe 9.5 at that point, because I knew that I had the support that I needed, the DNC needed at that time.

And that was further, I want to say, supported by Agent [redacted] response after he spoke with Robert Johnson at CrowdStrike to say you're in good hands. I think if Agent [redacted] had said you're not in good hands, which he could have said, I would have freaked out, and I would have talked to DNC leadership in saying, "We don't have the right people on the job here. Agent [redacted] is telling me something different," right? But he didn't. He did the opposite of that. He confirmed my feelings or my belief that we were in good hands.

BY [redacted]

Q And then my last question before [redacted] has a couple more is, do you know how much the DNC paid CrowdStrike for their services in relation to this?

A I don't know, actually. That wasn't part of my budget.

Q No, sure. Do you know who would know over there?

A Well, I am pretty sure -- I don't know. I mean, the two people that I'm pretty sure would know are probably the CFO at the time and the COO, who wrote the check, right? I mean, the people who signed it, presumably they would know.

Q They were? Sorry. I don't know their names.

A Oh. I mentioned the COO's name, chief operating officer's name, at the time was Lindsey Reynolds.

And when would the check have been written? I don't know when the check was written. So we've had three CFOs in the past year. One of them is named Brad Marshall, the first one. And then another one is named Charles Olivier. And the third one, current one, is named Joe -- I don't know how to pronounce his last name. I'm sorry.

Q Thanks very much. Appreciate it.

[redacted] Just one question in the 1 1/2 minutes I have left.

There's a New York Times article in December 2012 that goes through most of the timeline we have talked about today, which repeatedly references and includes a Snapchat of a memo that it was reported that you wrote.

Can you just briefly describe the circumstances under which this memo came about? When? Why? What's in there besides what's --

MR. ELIAS: I'm sorry. What is the memo?

[redacted] It seems to be a memo recounting at some point in the future, or at some point in April 2016 or subsequent, the engagements that Mr. Tamene had with the FBI, beginning in December 2015.

MR. ELIAS: And how did the Times get it? Do you know?

[redacted] They said it was a memo that's been obtained by the Times.

[redacted] I don't know what memo.

MR. WILSON: This is actually a memo that was created at the request of counsel. So I think that we can have another conversation separately about getting further into that, but I think there's some privilege issues there we need to sort out.

[redacted] Okay.

I think that's our time.

[redacted] I don't have any further questions. I think that concludes the interview.

[redacted] Thank you. Thanks.

[Whereupon, at 3:44 p.m., the interview was concluded.]