EXECUTIVE SESSION

PERMANENT SELECT COMMITTEE ON INTELLIGENCE,

U.S. HOUSE OF REPRESENTATIVES,

WASHINGTON, D.C.

INTERVIEW OF: ANDREW BROWN

Wednesday, August 30, 2017

Washington, D.C.

The interview in the above matter was held in Room HVC-304, the Capitol, commencing at 10:04 a.m.

Appearances:

For the PERMANENT SELECT COMMITTEE ON INTELLIGENCE:

[redacted]

For ANDREW BROWN:

MARK ELIAS, ESQ.

GRAHAM M. WILSON, ESQ.

PERKINS COIE POLITICAL LAW GROUP

700 13TH Street NW

Suite 600

Washington, D.C. 20005

[redacted] Good morning. This is a transcribed interview of Mr. Andrew Brown. Thank you for coming in and speaking with us today.

For the record, I'm [redacted] a staff member with the House Permanent Select Committee on Intelligence for the majority.

Also with me is --

[redacted] from the majority staff.

[redacted] And --

[redacted] with the minority staff.

[redacted] So before we begin, I just want to state a few things for the record. The questioning will be conducted by staff, as you see. During the course of this interview, members -- members will not -- staff will ask questions during their allotted time period. Some questions may seem basic, but that is because we need to clearly establish facts and understand the situation.

Please 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 will take any breaks that you desire. There's 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 we ask is unclear, or you're uncertain in your response, please let us know. And if you do not know the answer to a question or cannot remember, simply say so.

You're entitled to have counsel present for this interview, and we see that

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

you have brought them. So if counsel would please state their names for the record.

MR. ELIAS: Marc Elias from the law firm PerkinsCoie.

MR. WILSON: Graham Wilson from the law firm of PerkinsCoie.

[redacted] Thank you.

[redacted] My colleague, the [redacted] from the minority staff just came in.

[redacted] [redacted] counsel for the mino.

[redacted] Thank you.

As I said, the interview will be transcribed. And because the reporter cannot record gestures, we ask that you answer verbally. 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, individually or together, if you wish, 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. Then the minority will be given 40 minutes to ask questions. We can take a break thereafter or we can proceed to a final 15 minutes of questioning per side.

These time limits will be adhered to and no extensions will be granted. The time will be kept for each portion of the interview and warnings will be given at

the 5- and 1-minute mark, respectively.

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. You are reminded that it is unlawful to deliberately provide false information to Members of Congress or staff.

And, lastly, the record will reflect that you are voluntarily participating in this interview under oath.

Do you understand everything that I have said so far?

MR. BROWN: Yes.

[redacted] And would you mind raising your right hand to be sworn. Do you swear or affirm that everything you are about to say will be the truth, the whole truth, and nothing but the truth?

MR. BROWN: I do.

EXAMINATION

BY [redacted]

Q Thank you. And if you could just give us your full name for the record.

A Andrew Brown.

Q Mr. Brown, as I said, my name is [redacted] I'm a staffer for the majority. [redacted] and I will do some questioning and then the minority will do some questioning.

A Okay.

Q Could you give us your current occupation and how long you've held it.

A I'm the technology director at the DNC. I've had that position since April of 2013.

Q And so, just for the record, the DNC is the --

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

A Democratic National Committee.

Q Okay. Thank you.

Have you always maintained that same position at the DNC?

A I started at the DNC in February of 2013 where I was brought on as the data director. After 2 months, I was promoted to the technology director.

Q So, in total, how long were you doing work for the DNC?

A Since February of 2013.

Q Okay. And prior to February of 2013, where were you employed?

A I was employed at a small consulting firm known as ISSI that did work consulting with nonprofits who were doing issue advocacy or civic engagement work engaging directly with voters or members. So I was working with that small data consulting company who would help those sorts of organizations run their data operations.

Q What brought about your transition from the consulting firm to the DNC?

A After the 2012 presidential election, the DNC -- typically, after most elections, the DNC turns over staff when there are new openings, as staff that have spent the previous 2 to 4 or longer years working on election move on. So there was openings at the DNC. That was an opportunity for me to step in and have a job there.

Q Did you seek it out? Did they recruit you? Or how did that come about?

A I was recruited and -- but it wasn't like a formal recruitment. It was, you know -- people who I had worked with previously who worked at the DNC suggested this might be a position that I'd be interested in and --

Q Any folks that stand out in particular in transition?

A So the previous technology director at the DNC -- his name is Brian Whitaker -- he was somebody I worked with previously when -- and he was the one who was my boss for those first 2 months while I was there as the data director.

Q So when you came on board as the data director, can you give us a description of what that means?

A Yeah, so the data director at the DNC is focused on providing services to campaigns. So the DNC acts as a service provider for State parties and campaigns and provides long-term infrastructure that -- since campaigns are ephemeral, they come and go, it's important that some of the technologies and the data sets that they require to do their jobs are maintained, not just over the course of the campaign, but in between campaigns.

So the data director's job is to focus on those services and -- that the DNC is providing to campaigns when it comes to data and technology, ensure that those services meet the needs of the campaigns, that they're being delivered and supported in a way that makes them effective for the campaigns that are using them.

Q Okay. Let me try to break that down a little bit. So when you say data, can you give me examples of types of data that you're involved with?

A Sure. So primarily the data systems involved with voter-related, so it's information about campaigns' interactions with voters, so maybe conversations that a campaign would have with a voter or information about preferences that a voter may have for specific candidates or around particular issues is the primary data set.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

And then on top of that is opinion research information, so polling and other, you know, more aggregate, physical information about the electorate.

Q So in a -- in your day-to-day, when you first came on there in, I think you said February of 2013, correct?

A Uh-huh.

Q Are folks in the DNC coming to you saying we need you to do data services for this election, this particular race, or how does that work? Are you just doing it across the board in general?

A So we work in partnership -- the DNC works in partnership with State parties across the country. So for the most part, State parties are the ones interacting directly with the campaigns in their States, and the DNC is providing those services via the State parties.

Q So do you have direct engagement with the State parties and the people that are actually running and their campaigns, you as the data director, or is that someone else? How does that interaction work?

A So there's a staff of people that interact on a day-to-day basis primarily with the State parties, on occasion with the campaigns as well, as needed.

Q Okay. So when you first came on for the first few months, what were some of the campaigns that you worked on at the DNC?

A In particular, 2013, the primary campaigns were around the Virginia Governor's race, the New Jersey Governor's race.

MR. ELIAS: Just to be clear, do you mean primary as an electoral primary or principal?

MR. BROWN: Oh, no, sorry. Principal, the main campaigns, sorry, and, for instance, the Kentucky Governor's race. It's been a few years since then.

But those elections that were happening in the November 2013 timeframe was the primary focus -- was the focus.

BY [redacted]

Q Now, does your role in those campaigns involve you to travel to those local districts or States and engage directly with the campaigns, or are you doing it all remotely from D.C.?

A Like I said, it doesn't involve travel to work directly with the campaigns. That's unusual, because we're dealing -- like the State parties are the main interface to the campaigns directly.

So, in those instances, the State parties would have been interacting on a day-to-day basis with the campaigns as needed, and we would be providing kind of second-level support to the State parties to make sure the State parties had what they needed to help those campaigns.

Q Got it. And so now, I'd like to ask you some more about the breakdown of the cyber component. Maybe you can help me understand it.

A Okay.

Q So what exactly are you working on in sort of the, quote/unquote, "data universe" for these races?

MR. ELIAS: For what time period? Sorry.

BY [redacted]

Q For the first 6 months that you on-boarded with the DNC.

A With regards to security or with regards to --

Q Security, yes.

A So the DNC was not responsible, or did not provide security services to the campaigns.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

Q At all?

A At all.

Q Has that changed since your -- since you've been with the DNC at all?

A No.

Q Okay. So how does the DNC protect, for lack of a better word, its data that it collects?

A Yeah. So the DNC maintains a data warehouse. There are, you know, industry standard protections in place, everything from two-factor authorizations and VPN connections, virtual private networks, that allow access to those systems.

So all of that information is stored on DNC maintained or, you know, systems maintained by third parties on behalf of the DNC. And that's the parameter that the DNC establishes is that the work occurs on DNC-provided systems.

Q Okay. So let me see if I have this right. So you get -- you're brought on -- or excuse me, not brought on. That is not the right word. You engage a campaign --

A Yeah.

Q -- for a certain race in a certain State or a certain area --

MR. ELIAS: Or a State party.

BY [redacted]

Q Thanks. Or a State party. And you start receiving data and you start aggregating that data. Now, where is that data held or stored?

A Yeah. So for the most part, there is a -- it's essentially a CRM, or a customer relationship management database. It's a piece of software that's

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

provided to the DNC by a third-party vendor. The third-party vendor is responsible for development of the software, for hosting the software, for servicing the software and maintaining it.

And the DNC pays for a hosted instance, a software as a service instance of that CRM software. The software has controls built into it such that campaign -- that we can provision access to the software of the database it contains to State parties, to individual campaigns.

It works in a hierarchical fashion so that we can, for instance, grant a State party access to information in the CRM relevant to that particular State. And the State party can then subdivide provisional access to particular campaigns, for instance, you know, particular congressional district or particular, you know, legislative district that that campaign needs access to.

It also has controls so that campaigns can segregate the data that they care about. So, for instance, if they are keeping track of their volunteer list, that campaign can see that was to volunteers, whereas other campaigns using the same system can't see another list.

Q Now, is this a crowd-based infrastructure or --

A Yeah. It's not hosted by the DNC. It's provided -- it's hosted by the software company.

Q Okay. So as I understand it, there's a third party. Is it always the same third party?

A It is the same third party, yeah.

Q And who is that?

A The company's name is NGP Van.

MR. ELIAS: Initials NGP, and then new word, Van.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

Looking out for you.

BY [redacted]

Q I appreciate it.

So with NGP Van, since you've been at the DNC, have they always been the third-party provider for your universe of information?

A Yes.

Q And so they do it for everything the DNC engages on?

A So there's -- that is the primary -- or, sorry, I should stop using the word "primary." That is the main way that campaigns access the data the DNC provides. The DNC also maintains an in-house data warehouse, so this is a database where the information from that CRM and from other places is stored for the long term.

Q Got it.

A So that is maintained internally at the DNC, and access is restricted. There's many fewer users that have access to that -- to the data warehouse environment than have access. I mean, the Van environment, that's what we call the CRM software, has tens, or potentially hundreds of thousands of users; whereas, the data warehouse environment has, at most, potentially 100 or 200 users.

Q And so if you could simplify for me, what's the biggest difference in terms of information that's in the Vans versus data warehouse?

A So Van, most of the information would be -- all of the information that is located in the Van would also be in the data warehouse. But the data warehouse is where it is aggregated over time.

So some information in Van that isn't relevant for the current election cycle

may be removed, may be taken off or simplified; whereas, that data is maintained in the data warehouse in case it's ever needed in the future.

Q So am I correct in picturing it in the following way: The data warehouse is sort of like, you know, the mother ship. It has everything of all data ever collected and it stays there. And then the Vans are sort of spun off from there as needed and access is given to folks depending on the campaign, depending on the State and whatnot?

A Essentially, yes.

Q Is there any other entities that interface with those two main sets of data?

A What do you mean by entities?

Q Any other -- I think you called them host instances earlier. How does that interplay with the Van and the data warehouse?

A So I'm not 100 percent sure I'm understanding your question, but, you know, all of the data that is -- so there's the base layer of voter file information. So that's information that's publicly available from elections officials across the country.

So that information includes everything from, you know, a voter's name and address, potentially a phone number, whatever the information they provide to the registrar. So a lot of times, it includes things like date of birth or gender, and information about their electoral profile.

So, for instance, if they registered with the party, what their party registration is, potentially their voting history, so have they voted in previous elections or previous primaries, and that sort of information is publicly available from elections officials across the country.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

So that is what we call the voter file. So that the DNC works with the State parties to compile a voter file. That is the base layer of information that is in both the Van as well as the data warehouse.

So in the Van then, a campaign will access that list of voters for their particular election, for their -- so for their district that they're working in. And they'll be able to see, okay, so we have X number of voters who are eligible to vote or are registered to vote, for instance, and they will be able to formulate a program to go out and contact those voters.

And as they are working their way through, you know, attempting to either, you know, contact a voter to persuade them that their candidate is the candidate that that voter should choose, or to make sure that that voter realizes the election is coming up and remind them to go vote; they're able to keep track of those programs inside of the Van.

So they're able to know, here are the voters we've contacted, here are the voters we haven't contacted yet, here is the responses we're getting from the voters that we have contacted and keep track of that level of detail.

And there's a lot of software features built into Van that makes it easier for campaigns to do that. So, for instance, there's an interface that makes it easy for a volunteer whose making phone calls on behalf of a campaign to know which people -- which voters they should be calling next and what the phone number is that they should call and to be able to record that response from that call.

Q Okay. And so in terms of access to that information, maybe walk me through the following hypothetical, what I have right and what I have wrong.

A Sure.

Q I'm sitting in Kentucky and I'm asking the DNC for assistance to

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

access the database. I access it virtually and you guys -- you all provide sort of a password and an online login and then you have access to certain pieces of the information you and the Kentucky delegate deem relevant?

A Yeah. So the way it would work is in Kentucky, the State party would have a State-wide administrative account for the system that covers Kentucky. They would work with the campaign in question to decide what level of access that campaign needs, so what voters that campaign would need access to.

They would create logins to the system for the campaign, and those logins would, you know, be specific to individual users, and would allow those users to log in and see the specific, either list of voters or information about those voters that was deemed appropriate in that instance.

Q So is there any other way into your system from the outside, outside of that process?

A In terms of --

Q Accessing that data.

A Accessing the Van data?

Q Yeah, or the Van or the --

A So the Van provides APIs, application programming interfaces, that can be used by third-party software developers to write software that can interface with the Van software.

So, for instance, if a software vendor wrote an application that worked on a smart phone, and that smart phone app made it easier for a campaign to go door to door and keep track of the voters that they're talking to door to door, the API could allow that software to interface with the data in Van, following all the same, you know, access controls and protocols in place to make sure that it is limited to

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

the data set that is appropriate for the campaign that is using the software.

Q Okay. Now, in terms of sort of security infrastructure or cybersecurity, whatever you want to call it, as it relates to each of these, both the outside and the inside within the DNC, I know we briefly touched upon it earlier, but can you give more details as to how the DNC protects its information in its databases?

A Yes.

MR. ELIAS: Can I just ask what timeframe again, because I don't know whether you're up to the present or you're still back in those first 6 months.

BY [redacted]

Q Yeah, so when you first on-boarded and how that's changed through now.

Thank you.

A So the DNC maintains its internal data warehouse on systems that are separated from the DNC's kind of corporate network system, so the corporate network. By that I mean -- the corporate network would contain things like the email server or the file share servers or, you know, the things that DNC staff uses day-to-day in terms of office productivity.

And then a segmented network is in place for the data warehouse environment, so that is used for the information that is collected from campaigns -- or, sorry, from campaigns regarding specific voters, and that information we've been talking about is in the data warehouse. So there's two separate environments.

To gain access into the data warehouse environment, you would have to have -- a user would have to have a two-factor guarded account to gain access, right. So they would need to be able to create a virtual private network

connection.

That connection is secured through two party -- or, sorry, two-factor authentication, and that would allow them onto the data warehouse network. And then beyond that, they would still need to provision access to individual databases or servers or data sets inside of that environment.

Q So obviously, you control who has access to the information. Then you provide the overall security for that infrastructure. Is that correct?

A So me being the DNC?

Q Yes.

A Yes, the DNC does.

Q Okay. And they have that -- is that run within the DNC, or that's also sort of farmed out to third party?

A So the data warehouse is maintained by the DNC.

Q And it has its own internal, for lack of a better word, if there is a better title, security person who oversees that --

A So the security for that environment is overseen by the DNC information technology team.

Q Are you a part of that team?

A So I oversee the DNC information technology team as well as the data team, the software engineering team, and the data and analytics team.

Q Okay. So you oversee sort of the data component and the security component at the DNC?

A Yeah.

Q Is that fair to say?

A Sure.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

Q Okay. And you've been doing that for how long?

A So the technology director position that I started in April of 2013 in that position is -- was responsible at that time for those four other teams, including the IT team, which does the security component.

Q Okay. And, I'm sorry, we're going to get into that.

A Sure.

Q When did you start that?

A I started in that position in April of 2013.

Q And it remained through this --

A Yeah.

Q So in terms of other folks from the outside trying to access your system, be it local State parties or what have you, they go through this process that you described for us. How vulnerable is your system at home through other folks trying to get in, you know, for lack of a better word by hacking?

MR. ELIAS: When you say "at home"?

[redacted] Your home base at the DNC.

MR. ELIAS: Oh, at the DNC. Not his home.

[redacted] No, we're not here to talk about that.

MR. ELIAS: Okay.

BY [redacted]

Q But if you understand my question.

A Yeah. I think I do.

So over the course of the events that have transpired over the past 2 years now, we've -- the DNC has completely revamped its security capabilities and the way that the systems work. So as you know, we were -- we discovered intruders

on our network in late November of 2016 -- or sorry, late April of 2016.

At that point, we engaged with an outside firm, CrowdStrike, who are widely recognized as experts when it comes to cybersecurity. And they're led by a person named Shawn Henry, who spent over 20 years at the FBI leading cybersecurity investigations for the FBI.

So when we engaged with CrowdStrike after we had discovered these intruders on our network --

Q I'm sorry. Can you just maybe tell us how you discovered the intruders or what they were looking for. Do you guys have any awareness of that?

A Yeah, so the intruders were discovered in April when our IT team noticed logins into some servers on the DNC corporate network that were being accessed by administrative-level accounts that only members of that team had, but that they were -- they knew the individuals on that team were not doing.

So they noticed these suspicious logins occurring, and that was the first indicator that we had that there was, you know, an unknown actor on our network.

Q Okay. And so now my questions will focus on from that time period forward to the present, from April, end of April, as you described, to basically now.

So when you discovered this, you sought out CrowdStrike and they came on board to do what exactly?

A So they came onto lead the investigation into who these attackers were and what was happening with the system and to provide support and guidance for the remediation and updating of our security protocols at the DNC.

Q At the time or during the time -- is CrowdStrike still involved with the DNC?

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

A Yes.

Q Okay. So that sort of employment is ongoing since April of --

A Yes.

Q Sorry. Remind me of the year.

A April of 2016.

Q 2016. So what has CrowdStrike been able to sort of flesh out in terms of who did it, what did they get, what did they retrieve, and was any of that information disseminated on unauthorized?

A So when CrowdStrike deployed they had software technology that allows them to do forensics on a network and to monitor what is happening on a network. So over the course of late April into May, I believe that software was deployed on all computers on the DNC network.

And that allowed CrowdStrike to not only monitor what the intruders were doing during that time period, but also to forensically look back and see what actions the intruders may have taken previously.

And over the course of that investigation, CrowdStrike was able to see that there was actually two actors, two individual actors on our network: One, APT-29, Advanced Persistent Threat-29, was focused mainly on access to our email and communications server and they were stealthily sitting there with access to our communications server.

And then a second adversary actually came on in April that tipped us off that there was intruders, which was APT-28, also known as Fancy Bear. Fancy Bear seemed very focused on gaining access to the research files that the DNC compiles.

These research files, in particular, were of the President -- the Republican

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

presidential candidates; so, for instance, President Trump or the other candidates that were at that time running for the nomination on the Republican side. There was evidence of them going directly to that information and trying to take it off of the system.

Q So when you say -- just help me out here because I'm not a tech guy, probably one of the few [redacted] that isn't. But when you say APT-28 and 29, are those sort of like screen names or what is that?

A So, yeah, I am also not a cybersecurity expert. That's not my background. But those are names that are agreed upon. I'm not sure who sets them exactly, but the security industry --

Q But that's how you --

A -- referenced them, and they're referencing not an individual person, but a group, you know. For instance, APT-28 is believed to be the Russian GRU, so it's a military operation from -- you know, supported by the Russian military.

Q Now, were you --

MR. ELIAS: I could be wrong about this. I'm not a tech guy either. I think that some government agency designates --

MR. BROWN: I believe so.

MR. ELIAS: -- so that everyone uses a common nomenclature.

[redacted] Got it.

MR. ELIAS: So they designate someone APT-whatever, you know, 21, 22, 23, you know, and then everyone then knows that that's the designation that they use, I think. I don't know that.

BY [redacted]

Q I got it.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

And so through CrowdStrike you're able to identify both APT-28 and APT-29. Now, were they able to identify for you sort of with concrete evidence that these folks are related to X or this government or this agency or this group of people?

A Yeah. So that's -- through the evidence that Crowd Strike gathered in the course of their investigation, you know, both seeing what the attackers were doing on the system, being able to monitor what systems outside of ours that the attackers were talking to and using the so-called command-and-control structures that were in place to execute the attack on the DNC, looking at the tools that the attackers were using once they were inside of our system to, you know, maintain access and to pivot and move laterally through the system.

It was a toolset that CrowdStrike had seen before and that it was -- had led them to be confident in their -- in saying that this was actually the APT-28 and APT-29 actors.

Q So -- right. And I understand that. So it sounds like the assessment was based off tradecraft in that industry?

A Yeah.

Q But were -- not you specifically, but the DNC via CrowdStrike, were you able to link APT-28 or 29, either or, to -- directly to an agency, either by some sort of trace or some other information that they receive saying we know this individual, this entity is directly related to this Russian agency because of this fact? Did that ever come out?

A I mean, those level of details, I'm sure, CrowdStrike would be happy to provide. But they were confident in their assessment that this was the known APT-28 and APT-29 actors, which I don't think there's -- based on my limited

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

knowledge, it's well known that these are, you know, state-sponsored actors.

Q Right. So it's fair to say you in your role and the DNC in its larger role didn't make that assessment?

A No. Yeah. Yeah.

Q You actually made the assessment, you agreed with it, and then sort of moved forward?

A Yeah, exactly.

Q Okay. And you said there was -- between APT-28 and APT-29 there's sort of one focused on emails, and another is focused on other information. Were you able to figure out exactly what was removed or accessed from your servers through CrowdStrike or any other entity?

A Yeah. So the capabilities that the CrowdStrike tools provided we were able to see which computers the adversaries actually accessed and what types of accounts they were using to gain those -- that access.

So we were able to see, you know -- you can't prove a negative, but we were able to see with some level of confidence which systems that had been targeted and information had been accessed on versus which systems.

Q So what'd they get?

A So, like I said, they seemed to be focused on -- they had access to our email servers so the servers that were -- are responsible for, you know, housing the @DNC.org email accounts and that are used day-to-day by DNC staff and officials. And the level of access they had on those servers would have permitted them to, you know, export any emails from any accounts that they wanted to.

[redacted] And "them" as just used now is APT-28, APT-29, or both?

MR. BROWN: Both.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

And then they had access to a database server that contained records of donors to the DNC, so a donation database. They had access to the servers that controlled our internal corporate file shares, so this is where, you know, the files that DNC staff use day-to-day for their work and, for instance, where the research files that were being compiled by the DNC research team were stored. Yeah.

[redacted] And so once that -- so do you know with certainty that that information was removed and disseminated, or you don't know that? And if so, by whom?

MR. ELIAS: You may want to break that into two questions. You lost me on the last two.

MR. BROWN: Yeah.

BY [redacted]

Q So the information that those two entities, APT-28 and 29, gathered or had access to --

A Yeah --

Q -- did they actually -- do you know for certain that they actually pulled that information out of your databases, and if, so did they disseminate to anyone that you know of?

A So based on the evidence that we saw, we were confident that information had been actually traded off of our systems. And, you know, I can't say for certain what the adversaries did with that information once it was exfiltrated, but, you know, based on the reports from the U.S. Intelligence Community, it seems pretty clear that they did disseminate it.

Q I've only got like 7 or 8 minutes before I turn it over, so I just want to change gears a little bit.

So when all this happened, did you, the DNC, contact the FBI or any other law enforcement agency?

A Yeah. So as soon as we discovered the intruders on our network in April, at the same time that we were reaching out to CrowdStrike, who began their engagement the very next day, we were also in contact with the FBI and notifying them of the situation.

Q Now, did the FBI ever receive access to DNC servers to do their own exploitation?

A Yeah. So at every step of the way we fully cooperated with everything the FBI requested of us. And to my knowledge, everything that the FBI requested they received.

Once -- you know, with the expertise and the background and experience that CrowdStrike had, they became the main point of contact in dealing with the FBI on behalf of the DNC. So requests that the FBI would have while they were doing their investigation, they would give to CrowdStrike, and we always said, yes, please do that.

Q But do you know, or does the DNC now know if the FBI ever had access to the infrastructure to do their own analysis?

A It's my understanding that, yes. So the servers that were compromised in this attack were imaged. So what that means is most of these servers were not like a physical box --

Q Sure.

A -- running an OS. They were a box that had multiple servers running on them in a virtual environment. So the images of those virtual servers, as well as the physical servers, were taken.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

And that is an important distinction because that means that not only were the -- it means that the running state of the server was captured, so not only the information that was on the hard drive and maybe logs that existed but the actual working memory of that server was captured. Those server images were, as far as I know, turned over by CrowdStrike to the FBI, so the FBI could investigate them.

Q Now, during this timeframe that we're talking about, from April 2016 up until now, do you have any or does the DNC have information that other individuals or entities had access to -- had unlawfully, or in an unauthorized fashion, accessed your databases?

A The databases that we've been discussing?

Q Yes.

A No.

Q Nobody else.

Now, do you, throughout your time there and going up to the present, have any information that folks that worked at the DNC and had access to that information that we've been discussing unauthorized sent it out to other parties?

A No, we have no reason or indication to believe that.

Q Have you done sort of an internal audit to follow people's emails or whatnot to see what was going out from the DNC to other groups to check that?

A Yeah. So part of the capability that the CrowdStrike provided us was the ability to see exactly what was happening on the network. Over the course of that time, you know, the unauthorized access was clearly happening by these intruders. It was not happening by internal staff or by others with access to the system.

Q Okay. So can you say for certainty on behalf of the DNC that no one at the DNC was, in an unauthorized fashion, disseminating or copying information and putting it to outside sources?

A Yeah. I mean, based on the investigation that we've conducted to this point and based on all the information that we have, there's no reason to think that that occurred.

Q Okay. But you don't know for sure?

A I mean, you can't prove a negative, but --

Q Okay. And with this overall security of the DNC, from April to -- April 2016 to now, would you say the cybersecurity infrastructure at the time was poor, was average, was good, or how would you describe it?

MR. ELIAS: The time being April.

BY [redacted]

Q April 2016. And then how would you change it to now?

A So coming into April of 2016, we were in the process of -- you know, cybersecurity is difficult because it's an evolving threat that you're facing, right. There's always new adversaries, new exploits, new things you need to protect yourself against.

There's always updates to the software, to the capabilities that you can use in your defenses. You know, we were, you know, constantly improving our cybersecurity position leading up to April.

As the events in April un -- happened, in June, on the weekend of June 10, we did what was known as a remediation, right. It was where we kicked the adversaries off of our network.

In order to do that, over such a short time period, usually a remediation of

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

this scale, I've been told, would take months, multiple months to plan and carry out. We had weeks, given the timeframe of the convention starting in July and the presidential election coming up in November.

The way that we remediated the system was we built a completely new system. And so the thing about building a new system was it was an opportunity to forego legacy systems that have been in place for years or potentially decades and start from scratch and build it using modern best practices as it comes to security.

So we were able to redesign the network architecture to provide more segmentation, which is a way to, you know, if there is an incident where an intruder gains access to limit the scope of what those intruders can access until they can be removed, and to put in place a more modern best practices. You know, there's always newer ways to build the system. And after the June remediation we had in place, you know, a very modern security architecture at the DNC.

Q And so at the time of April 2016, going back there, would you say, in your role as sort of the overseer of data and sort of the other operations, that DNC infrastructure was vulnerable?

A Well, I mean, the adversary we faced, right -- vulnerable to who, right? So the adversary we faced is a nation state-sponsored attacker. So I'm not -- it's not clear to me that there was necessarily any level or anything in particular we could have done to thwart such a well-resourced adversary.

That being said, yes, we were constantly doing enhancements and improvements to our cybersecurity posture and, you know, doing what we could to maintain the -- you know, like I said, this was a legacy system that had been built

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

over years. And so that is much harder -- that's harder to defend than a system that is designed up front from scratch using modern best practices.

Q So I just have 2 more minutes.

A Okay.

Q So when the attack, or whatever you want to call it, hack occurred in 2016 to now, the information that was accessed, where have you seen sort of the -- that information appear in the public sector? And I'm talking about --

MR. ELIAS: You mean in the public sector?

BY [redacted]

Q In the public as it relates to our investigation that we're talking about here, you know, some of the bigger pieces of information. Where have you seen that?

A Yeah, I mean, this is -- I don't have any information that's not already publicly available, but it's everything from the emails appearing on WikiLeaks to some of the documents released by the Guccifer 2.0 persona.

Q When you say the emails, you mean John Podesta emails?

A No. No. Sorry. The DNC emails that WikiLeaks released in, I believe it was July 25, or around then, 23 maybe. Just before the National Convention started for the Democrats, WikiLeaks dumped what were emails taken from the DNC servers, largely emails between DNC staff and -- but all emails that were from the DNC.org email account.

And there was other information leaked on, you know, DCLeaks and a few others. I think those are the three main. But that's a little bit outside of my area of expertise in terms of tracking where all this information may or may not have gone.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

[redacted] All right. Well, thanks for your time. Minority is going to ask some questions.

MR. BROWN: Okay.

[redacted] We can go off the record.

EXAMINATION

BY [redacted]

Q The time is now 10:50, and I guess we have 40 minutes to talk with you.

Mr. Brown, we appreciate you being with us today and appearing voluntarily. We've been trying to schedule this for a little while.

On behalf of Ranking Member Schiff and the other Democratic Members of Congress who serve on this committee, we appreciate, you know, all that you've done in the last few years.

As you know, this is a bipartisan investigation looking into four key questions as approved by the chairman and ranking member on March 1 of this year. The first area we're looking into is what Russian cyber activity and other active measures were directed against the United States and its allies.

The second area we're looking into is whether the Russian active members included links between Russia and individuals associated with political campaigns or any other U.S. persons.

The third area we're inquiring and investigating is what the U.S. Government's response to these active measures by the Russians was, and what we need to do to protect ourselves in the future.

And, finally, we're looking into possible leaks of classified information that took place related to the Intelligence Community assessment.

Our questions with you, Mr. Brown, focus primarily on the first and third prongs, based on your senior position within the DNC as pertains to the hacking and dumping of sensitive Democratic Party emails.

I'd like to start off by going back to a conversation you were having with my colleague. My colleague was asking about an internal audit at the DNC and whether, you know, staff within the DNC could have been the actor who stole the information from the DNC during the 2016 campaign.

And I believe my colleague said that you don't know for sure and you said that you can't prove a negative. But you did discuss that you had the -- the DNC had conducted an internal audit. Is that correct?

A Yeah. CrowdStrike led the investigation into the incident that, you know, occurred over the course of April and were able to, over the course of that investigation, not only see who was accessing what servers and services inside the DNC network, but also to look forensically backwards using logs and access logs and server logs to see what had happened in the past.

Over the course of that investigation, the only unauthorized access that was uncovered was on -- was carried out by these outside actors.

Q And was any evidence uncovered that an internal DNC employee could have been the hacker?

A There was no evidence that would lead anybody to believe it was an inside hacker.

Q Are you confident about that assessment?

A Yes.

Q Would you say that CrowdStrike was confident about that assessment?

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

A I believe they would say yes.

Q And as you sit here today, Mr. Brown, do you have any doubt whatsoever that Russian state actors were behind the almost year-long hack into the DNC servers?

A No. I mean, I don't have -- you know, based on the assessment provided by CrowdStrike during their investigation and then based on the statements released publicly by the U.S. Intelligence Community and their assessment that this was a state-sponsored attack sponsored by Russia, I don't have any reason to doubt those highly qualified and professional assessments.

Q And, Mr. Brown, prior to working for the DNC, had you worked in politics?

A Yes. So I worked -- in 2003 and 2004 for the Iowa Democratic State Party, and that continued through 2006. I briefly worked on presidential primary campaigns in 2007 before moving to Washington, D.C. and taking the job that I mentioned earlier for the consulting firm helping nonprofits do data analysis and data management.

Q And in those experiences, do you recall ever being hacked to the extent -- at all? I'll ask you that first.

A No.

Q Do you recall hearing about hackers breaking into computer systems of the Obama and McCain campaigns during the presidential race in 2008?

A Just through what was reported publicly.

Q And I think press reports claimed that the hackers downloaded large quantities of information that U.S. Government cyber experts believe originated in China. I don't recall if you recall that.

A Okay.

Q That information was never disseminated or anything.

Do you have concerns about the threat posed by state-sponsored hackers at the DNC for future elections?

A Yes. I mean, I think -- and I agree with the assessment that the Intelligence Community put out that this is now a tactic that has been proven to have an impact and undermine the confidence in the U.S. electoral system; and that, based on the campaigns that these actors have waged in other countries since the 2016 presidential election here in the United States, that this is a tactic that they are going to continue to employ and continue to use to try to undermine democracy.

And I have no doubt -- you know, I would be highly surprised if this didn't occur again in 2018. And given the advanced nature of the adversaries carrying out these attacks, it is very difficult for any political organization or campaign, which has limited resources and a small staff, to deploy the types of defenses that would be necessary to prevent these attacks in the future.

When you look at everything from the large multinational corporations that are successfully hacked, such as Sony or Target, to even U.S. agencies, including the Pentagon, the White House also being successfully hacked, it's hard to imagine that the -- an organization like the DNC or a political campaign would ever have the resources to wage an entirely effective defense against these sorts of attacks.

Q I want to ask about the server or the servers at the DNC, and you talked with my colleagues a little bit about that. I just want to clarify, were the actual physical servers turned over to the FBI?

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

A So images of those servers. So the physical hardware itself was not removed from the premise, but a virtual image of the running servers were taken and turned over.

And that was the level of detail, which, again, is greater than what could -- if the servers were turned over, they would have to be unplugged and turned over, and there would be information that was lost when those servers were taken offline.

So based on the recommendation and request of CrowdStrike to create images of those running servers that would contain not only the information stored on disk, but the working information stored in the memory of the computer; that was what CrowdStrike requested for the purpose of their investigation, and is what I believe that they passed along to the FBI for the FBI to conduct its own investigation.

Q That's what I thought. I wasn't sure from your conversation earlier. But the former Director of the FBI, James Comey, actually testified before the Senate Intelligence Committee earlier this year and said that while the FBI did not have access to the servers themselves, they were able to obtain the relevant information they needed to understand the intrusion and that they had obtained that from CrowdStrike.

A Yeah.

Q So that was my initial --

A And at every point we fully cooperated with all of the requests that the FBI made. I'm not aware of any request that the FBI made of the DNC for access or information that was not complied with.

Q And you never received any complaints from the FBI that they weren't

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

receiving the assistance they needed?

A Not that I'm aware of. But like I said, CrowdStrike was doing the day-to-day back and forth with the FBI, so --

Q Did you have any reason to believe anyone at the DNC would have wanted to interfere with the FBI's investigation in any way?

A No. I can't imagine why anybody inside the DNC would have wanted to mingle with the FBI investigation.

Q Was it your sense, being in a leadership position, that your employees and your staff cooperated with the FBI and did everything they could to --

A Yes. The members of the information technology team that were the -- at the forefront of all of these activities were extremely dedicated and professional in all the activities that they carried out over the course of this.

And it was a very trying and demanding time, especially for them as, you know, they take pride in their work. And the activities that happened on their watch, so to speak, on our watch, you know, were unfortunate. And to -- remedying the situation was top of mind and everybody was very diligent and active in remedying that situation.

Q Mr. Brown, there have been, unfortunately, a number of conspiracy theories that have floated around about what really happened with the DNC hacks. And I just want to clarify, and hopefully dispel with one or two of those conspiracies.

In one case, there was a tragic murder of a former DNC staffer, and that murder has been exploited to create a completely unsupported theory that that staffer was somehow the one who stole the DNC information. Have you heard of that theory?

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

A I've heard of that theory.

Q What do you make of that?

A That theory is preposterous. So I knew Seth Rich very well. I worked closely with him in his capacity at the DNC. Seth's job at the DNC was to work on collecting information sets to provide to voters on where they could participate and vote.

Seth was not a hacker, so to speak. Like, he did not have the types of skills that would have been necessary to carry out these attacks. And Seth was a very patriotic person. Like, he would not have even thought about colluding with a foreign government to try and undermine the democratic process.

So the idea that he was somehow involved in these attacks, to me, is a nonstarter. And then based on his personality. And then just knowing his skill set, it doesn't make any sense that he didn't have the skills to carry out these attacks.

And then beyond that, he would not have had access or privileges to be able to access the type of information that these conspiracy theories claim that he would have been leaking. So it was -- on all levels, the conspiracy theory just makes no sense.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

[11:04 a.m.]

[redacted] Shifting gears from that, do you recall during the 2016 election cycle learning that the DCCC was also the victim of hacking?

MR. BROWN: I do.

MR. ELIAS: Do you want to state for the record what "DCCC" is, what it stands for?

[redacted] Democratic Congressional Campaign Committee.

BY [redacted]

Q The DCCC itself announced on July 29, 2016, that it had also been the victim of hacking. When did you personally learn about that?

A We learned over the course of our investigation in May that the means by which APT-28 or Fancy Bear had gained access to DNC systems was through an account that -- sorry, from a computer at the DCCC, which led us to believe that the DCCC itself had probably been compromised as well.

Q Did you reach out to them and talk to them about this development?

A So, based on the recommendations of CrowdStrike during the period when we first discovered the attackers in late April of 2016 until we were able to remediate over the weekend of June 10th, the advice was that we keep the number of people who were aware of the situation to the smallest group as possible, which was only a few people in DNC leadership and a few people in the DNC IT operation.

And that -- best practices based on if the attackers would have known that we knew they were on our system, they could have carried out further activities, either destructive activities or found ways to burrow in, so to speak, and make it harder for the remediation to occur. So it was very important that their operational

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

secrecy was kept during that period while we were planning the remediation and carrying out the remediation.

So it wasn't until after remediation on the weekend of June 10th, to my knowledge, that we talked with DCCC. I was not party to that conversation with the DCCC, though.

Q One of the sort of unique facets of the Russian operation to interfere in the election last year is sort of the magnitude of how they used the data.

The unclassified Intelligence Community assessment states that, quote, "Russian efforts to influence the 2016 U.S. Presidential election represent the most recent expression of Moscow's longstanding desire to undermine the U.S.-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations."

Was the breach that you experienced unprecedented, in your experience?

A Yes.

Q You spoke earlier about the two entities CrowdStrike identified as having entered your systems. And the Intelligence Community also similarly assessed, quote, "with high confidence that the GRU used the Guccifer 2.0 persona, dcleaks.com, and WikiLeaks to release U.S. victim data obtained in cyber operations publicly and then in exclusives to media outlets," end quote.

Did you find the timing of the release of your data unique in that Presidential election?

A I mean, it was very clear, based on the timing of when particular information was released and the type of information that was released, that this was an effort to influence the election.

So, for instance, the first Guccifer 2.0 leaks started happening the day after the DNC announced that it had been hacked, which is interesting that around that timing that it almost seemed to appear to be trying to build on the story that the DNC had released that it had been hacked.

The WikiLeaks dumps of DNC emails started just days before the Democratic National Convention in Philadelphia in late July and drove the narrative in the public media leading into the convention, at a time that normally the media would have been focused on the nominees and the Democratic Party Convention, instead was largely talking about these leaks and the information in the emails that were leaked, and the timing of that was very suspicious.

And then again in the fall, when John Podesta's emails were leaked, that occurred at the same time, you know, the afternoon after a story had broke about then-Candidate Trump making some remarks to "Access Hollywood" years previously and seemed to be timed to take the wind out of that story.

So the timing of all of these releases is very -- seems to indicate that the goings-on of the election were being taken into account to time and to decide which materials were released.

Q You mentioned earlier that CrowdStrike was hired also to help rebuild the DNC infrastructure. Do you believe your infrastructure is better equipped to deal with these types of events?

A So, like I said previously, the remediation tactic that was decided upon, in consultation with CrowdStrike, with DNC leadership, was to, in essence, burn down the old infrastructure and build brand-new infrastructure. That rebuilding of our infrastructure afforded us the opportunity to put into place more modern best practices and capabilities into the DNC's network. So I believe the

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

DNC is much better positioned in terms of its security stance today than it was before the remediation in June of 2016.

But I believe, you know, given the level of resources the DNC has to spend on security and the size of the organization, that we are still undermatched when it comes to facing the type of adversaries that we faced in 2016.

Q Does the DNC collaborate with DHS or the FBI or even other political parties more than it did previously, in terms of sharing information? And was that a shortfall during the 2016 --

A So our relationship, working relationship, with the FBI previous to April was a developing relationship. Since then, through the experiences that we've had, we now have a much better relationship with law enforcement, with the FBI. We now have working points of contact.

The DNC, in August of 2016, put in place a Cybersecurity Task Force Advisory Board. This advisory board is compromised of --

MR. ELIAS: Comprised.

MR. BROWN: That's what I said, didn't I?

MR. ELIAS: You said "compromised."

MR. BROWN: -- comprised of, for instance, Rand Beers, the former Acting Secretary of DHS, Department of Homeland Security; Anish Chopra, former CTO of the U.S. Government; Nicole Wong, a former Deputy CTO of the U.S. Government and lawyer for both Google and Twitter; as well as Michael Sussmann, who is a practicing attorney at Perkins Coie and a former cyber law -- used to work at the Department of Justice in their cyber law division.

So, with that type of advisory board in place and the relationships formed over the course of dealing with these attacks, I feel like we're in a much better

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

position in terms of being able to both talk with and receive assistance from the government.

[redacted] Can I follow up on that?

[redacted] Please.

[redacted] As a result of this body that -- was this body stood up after the election?

MR. BROWN: It was stood up in August of 2016.

[redacted] And are there specific protocols that have been put in place, both either internal to the DNC or by the FBI, about how communication should occur in future incidents?

MR. BROWN: Specifically with law enforcement you mean?

[redacted] Yes. So if there are future cyber intrusions, are there new protocols that have been shared with the DNC, or have you internally created any?

MR. BROWN: So, yeah, there's now a clear protocol to follow internally at the DNC. And, like I said, with this advisory task force in place, with relationships to law enforcement and existing relationships between DNC leadership and law enforcement, it's much clearer what needs to happen when outreach to law enforcement is needed.

BY [redacted]

Q You know, one of the concerns we have is the protection of our elections going forward. And the unclassified Intelligence Community assessment also reported that Russian intelligence obtained and maintained access to elements of multiple U.S. State and local electoral boards.

Do you recall or have you learned about those types of interference? And what is the extent of your awareness of that?

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

A Yeah. So I am aware of that report that was made public by the Intelligence Community and their findings that actors had gained access to electoral official computer systems. I'm not aware of any knowledge beyond what was made public in that report.

But, you know, those systems that are maintained by elections officials and State governments and local governments are, you know, completely separate from any systems that the DNC or other political campaign organizations would maintain but, you know, are obviously vital to the carrying out of our electoral process.

Q Just in the course of your work, have you heard of concerns at the State and local level about cybersecurity in 2016 or going forward?

A I haven't been a part of any detailed conversations with elections officials with regard to cybersecurity, but I do know that it was identified and there was a conversation, which may still be ongoing, but I heard about it last year, about the elections infrastructure being deemed critical infrastructure so that it could be, you know, better resourced by DHS and others to be protected the same as other critical infrastructure is protected.

[redacted] Can I ask one more clarifying question?

[redacted] Yes.

BY [redacted]

Q This goes back to, I think, the earlier discussion with our colleagues where you described the difference between the DNC-owned and -operated data warehouse and then the DNC network server --

A Uh-huh.

Q -- if I understand that correctly, which housed the email servers, other

file-sharing systems, all the day-to-day working files.

A Uh-huh.

Q To clarify, the DNC, the foreign intrusions by APT-28 and 29, were those detected in both systems? Or was it principally in the network server that had to do with the emails and other files, including the research files? Was there also an intrusion and possible exfiltration of data from the data warehouse?

A Yeah, during the course of the investigation in May and June, we didn't see any evidence that the attackers had gone after the data warehouse environment. They seemed to be completely focused on the DNC corporate network.

Q Corporate network. Okay. And the forensics that have been done and the images were all of the corporate network. Is that right?

A I believe so.

Q Okay.

I just wanted to avoid confusion.

[redacted] Okay.

I am about out of questions. I would just ask you, Mr. Brown, if you have any recommendations for Congress for any type of legislative action or -- probably you don't, but --

MR. BROWN: No, I don't at this time.

[redacted] We can go off the record, then, at this time.

[redacted] Let's take a brief break, and then we'll resume with up to 15 minutes of questioning.

MR. BROWN: Okay. Sounds good.

[Recess.]

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

BY [redacted]

Q All right, Mr. Brown, on behalf of the majority, I'll follow up on some of the things we discussed before. In particular, I'd like to cover the period prior to April 2016, when you first detected an intrusion on your system.

I'm going to make reference to a New York Times article from December of 2012 entitled "The Perfect Weapon: How Russia Cyber Power Invaded the U.S." Are you familiar with that article?

A From December of 2012?

Q Sorry. December 13th of 2016.

A Okay. Yes.

Q And, in fact, you are quoted in the article, so I assume you were a source for at least part of the information that's in this article.

A Yes.

Q And if you have any questions, I'm happy to read you specific quotes.

So the article begins by referencing a call from an FBI special agent to DNC in September of 2015. Are you now aware of that phone call?

A Yes.

Q And were you aware of that phone call at the time it occurred? Or when did you first become aware of that call?

A I don't remember the precise date, but sometime in the following days or weeks I was made aware of the call, yeah.

Q And the call was received by an individual named Yared Tamene. Am I pronouncing that correctly?

A Correct. You are.

Q And what was his role with respect to the DNC and you?

A So Yared reported to me. He was on the technology department. He was the information technology director, so the IT director. So he was responsible for overseeing the DNC network and operations, so, for instance, everything from our email servers and capabilities to our file share capabilities to our internal networks and the connectivity of those networks to the internet and the overall security for that system.

Q And could you just describe, was he based -- where is he based?

A He was based in Chicago at some point. I can't remember when he moved full-time to D.C., but he was in the D.C. office most days.

Q And you said that you became aware of the September 2015 call from the FBI shortly thereafter.

A Uh-huh.

Q Do you recall specifically how you became aware of the call?

A Yared told me in person about the call. He said that an FBI -- somebody had called to the main line at the DNC and was transferred to the IT help desk, where they had been put in contact with Yared.

They said Yared relayed that the FBI was investigating something and was asking if we could cooperate and provide them some information about the investigation they were conducting. And they asked us to look for some specific indicators on our system, which we looked for and did not see those indicators.

Q And can you briefly describe what steps you took in response to this information from the FBI?

A So, I mean, we followed up on the information that the FBI passed along to us. I don't know the specifics of what the IT team would have done to, you know, do that, but I know that they followed up to look for those indicators.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

And we did not find any indicators. And we were expecting another contact from the FBI at some point in the future.

Q Now, once Yared talked to you about this call from an individual purporting to be from the FBI, who did you speak with about it?

A Sometime later in October, I think after the second contact from the FBI, I reported that to my superior, the CEO, Amy Dacey.

Q Okay. So, during this time period, your direct report was the CEO --

A Yes.

Q -- who was Ms. Dacey.

A Yes.

Q And what did you communicate to her regarding these contacts with --

A Yeah. I passed along the tenor of the conversation, that the FBI had reached out and was investigating, but that, you know, the particular details that they asked to us look for, we didn't see any indicators that were, you know, in line with what they were asking us to look for, you know, that there wasn't any specific actions that the FBI was asking us to do beyond that, and that, you know, at this point it wasn't clear that there was -- you know, that nothing in this interaction with the FBI, that it wasn't clear to us that the FBI was, like, trying to tell us that our systems had been compromised. Like, that was not the tenor of the conversation as it was relayed to me.

Q And once you conveyed this information to Ms. Dacey, what was her response?

A She asked to be kept apprised of the ongoing conversations.

Q And in addition to Ms. Dacey, did you talk to the DNC Chairwoman about this interaction?

A No, I did not directly.

Q Do you know if anyone did in the October time period?

A I am not aware.

Q Now, according to this article from The New York Times, it says: "Amy Dacey said in interviews that neither she nor Ms. Wasserman Schultz was notified about the early reports that the committee system had likely been compromised."

Can you help me square that with your statement that you had a conversation with her in October of 2015?

A Only insomuch as that the understanding of the conversations that I had at the time were not that the FBI was relaying that the DNC had been compromised; they were asking us to cooperate in an investigation they were doing. The details provided by the FBI on what the DNC's role in that was or what they were investigating were very minimal. And it was not relayed to me in any sense that the FBI thought that the DNC itself had been compromised and that's what they were investigating.

Q When did you first understand that the FBI thought that the DNC had been compromised? Do you recall?

A I don't recall, but probably -- I don't recall.

Q But the September contact wasn't the only one, correct?

A Correct.

Q And, in fact, at least according to this article, Mr. Tamene received several calls from the FBI special agent in the month of October. Is that your understanding as well?

A It's my understanding that, yes, Mr. Tamene talked to the FBI again in

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

October.

Q And so we're discussing the first contact that occurred in September. When did you next become aware that the FBI had been in touch with the DNC?

A Sometime later in October, after the second contact.

Q Now, there's a subsequent reference to a call in November where a DNC computer was reportedly calling home, where "home" meant Russia. Are you aware of this November contact?

A Yes.

Q And when did you become aware of this November contact?

A Sometime shortly after that. I don't remember specific dates.

Q And once you became aware of it, what, if anything, did you do, particularly with respect to a followup conversation with Ms. Dacey or others in DNC leadership?

A Yeah, I believe that was what triggered me to talk with Ms. Dacey again.

Q The second conversation with her.

A I believe so, yes. And -- yes.

Q But different than the one you described taking place in October.

A Yes. And the FBI specifically said, it looks like there's a computer on the DNC network talking to a particular known bad guy, so to speak, out on the internet. And based on the information that was provided by the FBI, we, Yared and his team, looked to find any indication of that communication happening, and there was no indication found on our systems that that was happening at the time.

So it was something we were made aware of that we continued to try and trace down. I remember there was discussions around if there were other ways

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

that we could try and find or corroborate this information being passed on by the FBI, but that everything we tried was unsuccessful in confirming what the FBI was saying.

Q And this article says that in March Mr. Tamene and his team had met at least twice in person with the FBI. Were you aware of these meetings at the time they occurred?

A Yes, I was.

Q Were you part of these meetings?

A No, I was not.

Q Besides Mr. Tamene, who else was a part of these meetings?

A Members of his staff, but I don't know specifically who.

Q And what, based on your understanding, was the substance or result of these meetings?

A I know that in early April Mr. Tamene participated in a tabletop exercise hosted by the FBI. The tabletop exercise was not specific to the DNC but included other similar organizations and was meant to help think through how to respond to incidents that might occur in the future. It was not relating to any incident that had already occurred.

Q Now, according to this article, in April of 2016, shortly before the intrusion we discussed earlier was detected, the DNC finally installed a robust set of monitoring tools. Is that accurate, that you installed some new monitoring tools in April of 2016?

A It most likely is. I can't specifically think of what that would be, but like I said previously, we were continuously upgrading and enhancing our capabilities.

Q And it was shortly after that time, in late April, that you discovered the

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

intrusion which set off the chain of events and remediation that you described earlier.

A Yes.

Q So, understanding that a private entity, like the DNC, may be the underdog, so to speak, against a nation-state actor, looking back, based on what you know now, is there more you could have, should have, would have done between September, when you had the first contacts from the FBI, September of 2015, and April of 2016, when you discovered intruders on your system, to follow up on the information you received from the FBI?

A I mean, yeah, knowing what we know now, obviously, we would have -- I would have done things differently, I think a lot of people would have done things differently, you know, on all sides, if the breadth and depth of the nature of these attacks was known. You know, there was more we could have done to follow up with the FBI, and having a more robust relationship with the FBI would have been helpful at that point.

But I do want to stress, you know, the information we received from the FBI, you know, never led me to believe that they were trying to relay to us the fact that the DNC had been systematically hacked. We fully cooperated with the FBI in every request they made along the way, and we took everything they gave us seriously.

And so, you know, I think having that established relationship today with law enforcement hopefully will help, you know, prevent the type of circumstances that occurred in the fall of 2015.

Q Now, you're quoted in this article as saying there was never enough money to do everything we needed to do. I take that as something of a general

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

statement, given the realities of, you know, working for a nonprofit organization. But was there anything in particular during this 2015-2016 timeframe that you sought to do and were not able to do because of resource constraints?

A So, in 2015, we had put together a cybersecurity -- a series of steps that we would like to do, you know, and we took as many of those steps as we could, given the existing budget that we had to operate with.

There were a few items that required additional budgets that we eventually got to do, but, you know, I can't think specifically of what those items are. But, you know, we were constantly improving our security systems, given the resources that we had to do that with.

Q Just a couple final questions.

You discussed briefly earlier that in July of 2016, approximately, those 44,000 DNC emails were dumped publicly.

A Yes.

Q In addition to those 44,000 that were dumped, were there others that were stolen but not dumped, based on what you've been able to piece together after the fact?

A It's hard to say precisely what was taken, but given the nature of which emails were released and the selective nature of that, it's likely that more emails were taken and then selectively released. It would've been hard for them to select just the ones that were released in the midst of the breach.

Q Do you have a sense of how many emails were released?

MR. ELIAS: Were released or were taken?

BY [redacted]

Q Or were taken, total?

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

A I don't know that number off the top of my head, no.

Q And then -- last question, with my colleagues' indulgence.

Of those emails that were released publicly, dumped, are you aware of any that were forged, manipulated, or in any way altered such that they weren't actually, you know, real emails or real documents that had resided on your systems?

A Yeah, I mean, I was not directly involved with auditing the information that was released. I'm not aware of any -- I'm not aware off the top of my head of any doctored documents, so to speak, that were released.

Q Thank you.

A But I was not involved with that aspect of the investigation.

Q Thank you.

BY [redacted]

Q And on my colleague's note, it appears that the Russians targeted, to a certain extent, both political parties. The Intelligence Community assessment says that, quote, "Russia's intelligence services conducted cyber operations against targets associated with the 2016 U.S. Presidential election, including targets associated with both major U.S. political parties."

The assessment goes on to identify with high confidence that the GRU relayed material it acquired from the DNC. However, the assessment says, quote, "Russia collected on some Republican-affiliated targets but did not conduct a comparable disclosure campaign," end quote.

Did you become aware during the campaign of Republicans being the target of hacking as well?

A No, I was not aware of Republicans being targeted.

Q Does it surprise you that the Republican-affiliated targets were not the subjects of disclosure in the same way that the DNC was?

A In hindsight and having seen the assessment made by the Intelligence Community and released publicly that the Russians were attempting to undermine the democratic process as well as to target Secretary Clinton, in particular, to diminish her chances of winning a potential Presidency, it's not surprising in hindsight.

BY [redacted]

Q If I can just go back to the line of questioning by my colleague, [redacted]

A Okay.

Q Just so we understand the timeline correctly, would you say that the timeline that's outlined in the New York Times article is accurate? And, specifically, that there was a first contact by the FBI in September 2015, but the way you described the information that was relayed, it was minimal and did not describe a systematic hacking campaign --

A Correct.

Q -- but, rather, specific indicators were shared?

A I don't know what specific indicators were shared when, but, yes, in general, that the nature of the conversation was not that the DNC had been systematically compromised.

Q And then there were a number of subsequent -- there was outreach by the FBI a number of subsequent times, primarily to your colleague Mr. Tamene, that was then relayed to you, that led you to engage the DNC chief executive --

A Uh-huh.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

Q -- over the course of the fall and then the winter, so the fall of 2015 and the winter of 2016. Is that correct?

A Yes.

Q And just so we can place some context, when specifically did you -- or what prompted you to decide to hire this outside party, CrowdStrike, and how does that fit into that timeline?

A So, in April, late April of 2016, Mr. Tamene's team discovered, like I relayed earlier, that unauthorized access on our servers was occurring by accounts that should have been under his team's control but that they were not doing the acting on. So, at that point, we immediately reached out and sought outside expertise to help us understand what was happening.

Q And that was not identified earlier, the unauthorized access. That happened only at that point.

A So, based on the investigation that CrowdStrike conducted, it appears that Fancy Bear, APT-28, entered the DNC system around April 18th or mid-April of 2016. And they were the actors that set off the alarm, so to speak, for Yared's team to discover.

Q Okay. However, based on the forensic evidence, including the review going back in time, it was the other actor that was identified as having been there previously.

A So it was the Cozy Bear actor, APT-29, that forensically had been identified the earliest known evidence of compromise. Based on the CrowdStrike investigation, I think had it dated back to June of 2015 that APT-29 had entered the system.

Q Okay.

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

And based on your conversation with our colleagues, you mentioned that you were updating your cybersecurity tools regularly. Were those updates what prompted the ability of your team or Mr. Tamene's team to be able to identify these new unauthorized accesses, or would those have been identified in any event? Is that what kind of tipped everybody's hand, that didn't have, you know, more sophisticated tools at your disposal?

A It was definitely the activities that the second intruder, Fancy Bear, was undertaking on our systems that were less covert that tipped us off. It's hard for me to say specifically what capabilities we had in April when we did discover them, whether when -- I believe those are capabilities we would've had the whole time.

Q Okay.

BY [redacted]

Q Just along this exact line, because I think the distinction between the two actors is illuminating and, I believe, sometimes gets lost.

So APT-28, your understanding forensically is they penetrated your system sometime in April and then were discovered later in April due to their noncovert activities.

A Correct.

Q With respect to --

A Or less covert.

MR. ELIAS: Nonsuccessful covert.

MR. BROWN: Nonsuccessful, yeah.

BY [redacted]

Q With respect to APT-29, is it correct to say that you had never

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES

discovered them on your system until you hired CrowdStrike and they engaged in this forensic --

A Correct. It was the investigation that CrowdStrike was conducting over the end of April and over the course of May that they uncovered that there was actually a second actor that had been there since June of 2015.

Q Which is a significant period of time.

A Yeah.

BY [redacted]

Q Why do you think Cozy Bear was harder to detect? Was there something about the way they were in your system that made it harder to see them?

A So the way it was --

Q This may be too detailed for any of us probably, but --

A Yeah, this is something -- but the way that it was relayed to me by CrowdStrike was that Cozy Bear was focused on having access, persistent access, to our system in case they ever wanted to use it and that that was kind of their operating -- they'd operated that way in other situations.

So they limited what they accessed to the specific email servers and were trying to be covert and persist that access over time, whereas when Fancy Bear came in, they seemed less concerned about, you know, the long-term access to our systems and more concerned with directly getting to the information that they wanted and extracting it in a more rapid manner.

Q So they were more active, so to speak.

A Yeah, they were more active.

[redacted] So, based on the upgrades you made in your system, if

Cozy Bear were to attempt a similar intrusion today, what's your confidence level that you'd be able to stop or detect that?

MR. BROWN: So the capabilities -- so part of the ongoing capabilities that we now have are the systems from CrowdStrike that they used to do their investigation in April and May and beyond. And those capabilities are still deployed on the network. And those were the capabilities that did detect both of these adversaries in the course of the investigation.

Beyond that, the nature of the layers of defense we were able to put into the post-remediation, the new system that we have in place, would hopefully make it less likely that an actor like that would be able to persist that type of access without us noticing.

[redacted] If I could just ask, based on the experience that you and your colleagues had, is there any other information that you think the committee should be aware of, whether it's factual information, observations -- we asked this previously -- in case you are willing to discuss proposals you think other organizations like the DNC, Federal/State/local entities should be considering in light of possible future attacks or hacks in future elections?

MR. BROWN: Can I take some time and come back to you on that one?

[redacted] Sure.

MR. BROWN: Okay.

[redacted] Thanks very much. Appreciate it.

[redacted] That concludes our questions.

[Whereupon, at 11:56 a.m., the interview was concluded.]

PROPERTY OF THE UNITED STATES HOUSE OF REPRESENTATIVES