RUSSIA INVESTIGATIVE TASK FORCE HEARING

WITH FORMER SECRETARY OF HOMELAND SECURITY

JEH JOHNSON

Wednesday, June 21, 2017

U.S. House of Representatives,

Permanent Select Committee on Intelligence,

Russia Investigative Task Force,

Washington, D.C.

The task force met, pursuant to call, at 10:00 a.m., in Room HVC-210, Capitol Visitor Center, the Honorable Michael K. Conaway presiding.

Present: Representatives Conaway, King, LoBiondo, Rooney, Ros-Lehtinen, Turner, Wenstrup, Stewart, Crawford, Gowdy, Stefanik, Hurd, Schiff, Himes, Sewell, Carson, Speier, Quigley, Swalwell, Castro, and Heck.

Mr. Conaway. Good morning. Before we call the meeting to order, I've asked Rick Crawford to open us with a prayer.

Rick.

Mr. Crawford. Thank you, Mr. Chairman.

Please bow with me.

Heavenly Father, we do bow humbly before you, thankful for every blessing of life, Lord. Thank you for the blessing of this Nation. Father, I just ask that her people would strive to be worthy of that blessing, Father. We pray for humility and temperance and all that we say and do be pleasing to you. In Jesus' name. Amen.

Mr. Conaway. Thank you.

Point of business, real quickly. In consultation with Adam, without objection, I make a motion to give each member 7 minutes to question the witnesses.

Is there a discussion on the motion? I ask unanimous consent that everybody would get 7, including Adam and I. Everybody good to go? All right. Thank you.

The meeting will come to order. I'd like to welcome our witness this morning, former Secretary of the Department of Homeland Security Jeh Johnson.

Mr. Johnson, thank you very much for being here this morning.

As a reminder to our members, we are and will remain in open session. This hearing will address only unclassified matters.

To our guests in the audience, welcome. We appreciate the public and media interest in the committee's important work, and we would expect proper decorum will be observed at all times, and disruptions to today's proceedings will not be tolerated.

At this point in time, Mr. Johnson, would you please rise and take an oath?

[Witness sworn.]

Mr. Conaway. Thank you.

I now recognize myself for 5 minutes.

Again, thank you, Secretary Johnson, for being here today.

As you know, this committee is charged with getting to the bottom of the facts regarding Russia's involvement in the 2016 election and what, if any, steps were taken by the U.S. Government to prevent such interference in our election.

While our investigation seeks to get to the truth of what happened during last year's election, it also seeks to provide recommendations for improvement.

One focus of the committee's investigation is the U.S. Government's response to Russian cyber activities during the '16 election. According to the Intelligence Community's unclassified January '17 assessment, Russian intelligence accessed elements of multiple State or local electoral boards. DHS also assessed that, thankfully, the systems Russian actors targeted were not involved in vote tallying. However, the prospect of any adversary meddling in our election system is extremely disturbing.

Our free and open election system is a cornerstone of our democracy and the foundation of our self-governing Republic. Any actions by a foreign adversary to access electoral systems threaten our basic freedoms.

As Secretary of DHS, you were at the helm when your agency became aware of Russian cyber intrusions into State and local election systems, and you made the decision to designate election infrastructure as critical infrastructure in January '17.

I hope your testimony today will provide this committee and the American public with a better understanding of what exactly happened and what more could have been done, if anything, to prevent the Russians from interfering in our elections. And while I commend your efforts to address the cyber threat emanating from Moscow and

successfully safeguard the integrity of the vote tallying systems, it's troubling that DHS and other agencies did not respond more quickly to the Russian hacking.

We are also here to talk about the future. Given all that we know about the growing threat posed by cyber intrusions, why did our election systems remain so vulnerable? What more can be done to address these weaknesses and vulnerabilities? And I hope you will discuss these challenges and assist the committee in identifying solutions.

With that, I recognize the ranking member, Mr. Schiff, for 5 minutes for his opening statement.

[The statement of Mr. Conaway follows:]

******** COMMITTEE INSERT ********

Mr. Schiff. Thank you, Mr. Chairman.

And thank you, Mr. Secretary, for your extraordinary service to the country.

Three months ago, during the committee's first open hearing, former FBI Director James Comey revealed for the first time that he'd opened a counterintelligence investigation last July to determine whether any U.S. persons associated with the Trump campaign had coordinated or colluded with the Russian efforts to interfere in our election.

Last month, we heard from former CIA Director John Brennan, who helped us to understand what the Russian Government did, how they did it, and what motivated them. He testified that information he was seeing concerned him so greatly that he feared some Americans could be suborned to the Russian cause and began sending counterintelligence leads to the FBI for investigation.

Today, we'll hear testimony from former Secretary of Homeland Security Jeh Johnson about how the U.S. Government responded to this unprecedented interference in our political affairs, what threat the Russians posed to our election's infrastructure, and what steps we took to protect our institutions, to inform the public what was happening, and to deter the Russians from further meddling.

By the middle of last summer, it was apparent that the Russians were not merely gathering information for traditional intelligence purposes, but were intent on weaponizing it by dumping tranches of stolen emails into the public domain and in a way intended to damage the campaign of Hillary Clinton.

As the ranking member of the House Intelligence Committee and part of the so-called Gang of Eight, I've been made aware of information concerning the Russian hack, as had my counterpart in the Senate, Dianne Feinstein, and other senior leadership. What we saw alarmed us, and we believed it was incumbent on the administration to

inform the American people what was going on.

And so on the same day that Donald Trump was urging the Russians to hack Hillary Clinton's emails, the Senator and I wrote to then President Obama urging that the administration declassify and release any Intelligence Community assessments related to the DNC hack and develop a swift and powerful response.

Over a month later, when the administration had still made no public statement informing Americans about what the Russians were doing, Senator Feinstein and I took the extraordinary step of issuing our own public statement, carefully vetted by the Intelligence Community, attributing the hack to Russia and senior levels of the Kremlin.

It would be yet another month before the U.S. Government would publicly declare Russia behind the interference in our election when you and DNI Clapper issued your October 7 statement, and it wouldn't be until well after the election that the administration would take steps to signal just how truly significant an action the Russians had taken when it imposed sanctions on Russia over the hack, expelled Russian spies, and closed facilities used by the Russians for espionage against America.

I hope, Secretary Johnson, that you will be able to share with us and with the American people a sense of the debate that was ongoing in the executive branch as evidence of the Russian involvement and hacked emails piled up through the late summer and early fall. What led to such a long delay in making attribution, and why would the most significant step of imposing costs on Russia for its interference come only after the election? And what are the lessons learned?

At its heart, our democracy relies on the trust of the American people in their institutions. The events of last year and the potential for worse in the future are a stark warning to all of us that we must guard our democracy jealously and that there are powerful adversaries that wish to tear down liberal democracy and America's role as its

champion. We have our work cut out for us, but the world is counting on us to be up to the challenge.

I thank you for your extraordinary service once again and your testimony today.

And I yield back.

[The statement of Mr. Schiff follows:]

******** COMMITTEE INSERT ********

Mr. Conaway. Well, thank you, Adam.

Secretary Johnson, have you got a statement for the record, and would you like to make an opening statement? If so, please proceed.

TESTIMONY OF FORMER SECRETARY OF HOMELAND SECURITY JEH JOHNSON

Mr. Johnson. Mr. Chairman, you have my prepared opening remarks. Just briefly, in the time permitted me, Representative Conaway, Representative Schiff, members of this committee, you have my prepared statement. I will not repeat it here.

In 3 years as Secretary of Department of Homeland Security, I had the privilege of testifying before Congress 26 times. Though it is no longer part of my job description, I voluntarily accepted the invitation to be here today as concerned private citizen.

In 2016, the Russian Government, at the direction of Vladimir Putin himself, orchestrated cyber attacks on our Nation for the purpose of influencing our election. That is a fact, plain and simple.

Now, the key question for the President and the Congress is, what are we going to do to protect the American people and their democracy from this kind of thing in the future?

I'm pleased that this committee has undertaken this investigation. I welcome it. My sincere hope is that in bipartisan fashion you find answers.

Last year's very troubling experience highlights cyber vulnerabilities in our political process and in our election infrastructure itself. With that experience fresh in our minds and clear in the rearview mirror, we must resolve to further strengthen our cybersecurity generally and the cybersecurity around our democratic process specifically.

I am prepared to discuss my own views and recommendations on this topic, and I

look forward to your questions. Thank you.

[The testimony of Mr. Johnson follows:]

******** INSERT 1-1 ********

Mr. Conaway. Thank you, Mr. Secretary.

I recognize myself for 7 minutes. Again, thanks for being here this morning.

A lot of questions will be asked, a lot of details. Can we start kind of a top-level kind of conversation about DHS' mission with respect to cyber, particularly given how intertwined it is with respect to voter registration, voting, vote tallying, all those kind of good types of things?

And also, if you wouldn't mind folding into that what appears to be a delay between when the FBI became aware of things that were going on and when it seems that DHS was informed about things that were going on. So how is the relationship with FBI relative to this particular infrastructure either at the time and then maybe going forward?

So if you'll weigh in on that, I'd appreciate it.

Mr. Johnson. A couple of things, sir.

First, I think the roles of the Federal agencies in cybersecurity were spelled out pretty clearly last year in PPD-41. Basically, law enforcement, the FBI, is responsible for threat response. DHS is responsible for asset response. So the crime, law enforcement, FBI. Patching vulnerabilities, detecting bad actors in the system, DHS. And the way I like to explain it publicly, when I was in office is Jim Comey is the cop and I'm the fireman.

On a personal level with Jim, we worked very well together. I've known him for 28 years, from the days we were assistant United States attorneys together in Manhattan, and on a personal level, at the top of both agencies we worked well together. Can I say that down to the field office working level we were always fully coordinated? No. But I was impressed that day to day, the process seemed to be working well. Every morning in my intelligence briefing there would be an FBI briefer there who was

with me to give his assessment, to tell me what the FBI feedback on something was. So there is that.

I spelled out in my opening statement, my prepared statement, the first time I recall hearing about the hack into the DNC, and I recalled that it had been some months before I was learning of this that the FBI and the DNC had been in contact with each other about this. And I was not very happy to be learning about it several months later, very clearly.

Mr. Conaway. Well, there's two things, I guess, going on. The DNC hack was at some point in time. What was the delay between the hacks that FBI was aware of, or who found the hacks to the -- or the scanning, as you call it, of the various voter registration systems, the attempted intrusions, perhaps, into the voter records? Who discovered that? And if it was the FBI, then how long was there a delay between that and your -- because using your analogy of the cop and the fireman, if the flames are going up, we need the fireman there first.

Mr. Johnson. Yes, sir.

Mr. Conaway. And so what was that delay between the infrastructure we're concerned about --

Mr. Johnson. My recollection, and part of this is from open source reporting I've read more recently, is that the FBI first discovered the intrusion. That's my recollection.

Mr. Conaway. Intrusion of the State systems?

Mr. Johnson. Into the DNC.

Mr. Conaway. Okay.

Mr. Johnson. And I recall very clearly that there was a delay between that initial contact with the DNC and when the report got to me as Secretary of DHS. It may have been that there were others at the staff level in DHS who were privy to this before it

filtered up to me in an intelligence report, but that's my recollection.

Mr. Conaway. But I was asking, let's ignore the DNC for the moment. Let's talk about the attempts at scanning or whatever the Russians did with respect to the election systems, voter registration documents. When was that discovered, and who discovered it, and if it wasn't DHS, then what was the --

Mr. Johnson. My recollection is that the initial scanning and probing around voter registration systems was discovered in late August -- could have been mid, could have been July -- but late August, in my mind. And my recollection is that once it was discovered that information came to me and other senior people pretty quickly.

Mr. Conaway. Okay. Is there enough of a -- it's one thing for the Director and the Secretaries to have good personal working relationships. Institutionalizing that is what we're about, because that ebbs and flows depending on who's in those jobs.

Is there a system of notification between FBI and DHS in that working? Are there any impediments to that not working on its own without the good relationship that you and Mr. Comey had at the time?

Mr. Johnson. In my observation, it worked pretty well but could stand improvement, very definitely. And I think it's incumbent upon the leaders of both organizations to instill that in their workforces. So I think it worked pretty well together in my 3 years, but there were glitches. There were instances where we did not communicate as effectively as we could have.

Mr. Conaway. So one of our purposes this morning was to reassure the American public with respect to the '16 election; and then also, secondly, look at what we do in future elections going forward.

You said in your opening statement or in your prepared remarks that, to your knowledge, there was no vote tallying changes, that no one's vote was -- they voted one

way and it recorded some other way. Is that still your opinion, that with respect to the '16 election, that the intrusions or attempted, whatever it is the Russians or others did, did not affect the actual voting itself?

Mr. Johnson. Based on everything I know, that is correct. I know of no evidence that through cyber intrusions votes were altered or suppressed in some way.

Mr. Conaway. Okay. The lessons learned and moving forward, you've designated the voting system as critical infrastructure. In the remaining time, can you give us kind of a quick snap as to why that was important in your mind?

Mr. Johnson. It was important in my mind because critical infrastructure receives a priority in terms of the assistance we give on cybersecurity. That's number one. There is a certain level of confidence -- of confidentiality that goes into the communications between critical infrastructure and the Department that are guaranteed.

And number three, when you're part of critical infrastructure, you get the protection of the international cyber norms: Thou shalt not attack critical infrastructure in another country.

And so those were the principal reasons to do this. There are 16 sectors already that are considered critical infrastructure. And in my view, this is something that was sort of a no-brainer and, in fact, probably should have been done years before. And I'm pleased Secretary Kelly has reaffirmed it.

Mr. Conaway. Reaffirmed it.

Does that include the parties and the related infrastructure around candidates, or is that just the mechanics of voting itself?

Mr. Johnson. If you read the way I wrote the statement on January 6, it's pretty much confined to the election process itself, the election infrastructure itself, not the politicians, not the political parties.

Mr. Conaway. All right. Thank you.

My time has expired. I recognize the ranking member for 7 minutes.

Adam.

Mr. Schiff. Thank you, Mr. Chairman.

Mr. Secretary, in the late summer of last year it became apparent that the Russians were doing more than gathering foreign intelligence, that they were, in fact, dumping it in a way designed to potentially influence outcomes, not by affecting the vote machines, necessarily, but by affecting American public opinion with the dumping of these emails.

So that's happening in late summer, mid- to late summer. Why did it take the administration so long to make a public statement that a foreign adversary was trying to influence the American election? The statement didn't come until October. Why did we wait from July till October to make that statement?

Mr. Johnson. Well, Congressman, I'm going to disagree with your premise that there was some type of delay. This was a big decision, and there were a lot of considerations that went into it. This was an unprecedented step.

First, as you know well, we have to carefully consider whether declassifying the information compromises sources and methods.

Second, there was an ongoing election, and many would criticize us for, perhaps, taking sides in the election. So that had to be carefully considered. One of the candidates, as you'll recall, was predicting that the election was going to be rigged in some way. And so we were concerned that by making the statement, we might, in and of itself, be challenging the integrity of the election process itself.

This was a very difficult decision, but in my personal view, it's something we had to do. It got careful consideration, a lot of discussion. My view is that we needed to

do it, and we needed to do it well before the election to inform the American voters of what we knew and what we saw and that it would be unforgivable if we did not pre-election. And I'm glad we did it.

You know, every, Congressman, every big national security, homeland security decision I've made in my time, somebody always criticizes you for doing it and then somebody else criticizes you for not doing it sooner. So Jim Clapper and I made the statement on October 7th, and I'm glad we did, frankly.

I think the larger issue is it did not get the public attention that it should have, frankly, because the same day the press was focused on the release of the "Access Hollywood" video. That's what made our news below-the-fold news that day.

Mr. Schiff. I want to ask you about that, as well. But a couple of things. There were certainly allegations by one of the campaigns, the Trump campaign, that the process was rigged.

Mr. Johnson. Yes.

Mr. Schiff. But the allegation wasn't that it was being rigged by a foreign power. Why wasn't it more important to tell the American people the length and breadth of what the Russians were doing to interfere in an election than any risk that it might be seen as putting your hand on the scale?

Mr. Johnson. Well --

Mr. Schiff. Didn't the public have a compelling need to know, notwithstanding the claims made by a campaign about a different kind of rigging, and the need to rebut the idea that this was being presented to the public deliberately to influence the outcome?

Mr. Johnson. Yes, yes, and yes, which is why we did tell the American public everything we were in a position to tell them on that date. You'll note from my

statement that we attributed the hacking directly to the Russian Government. We were not then in a position to attribute the scanning and probing to the Russian Government. We did say it was coming from a Russian-based platform at that point.

But at that point, we told the public everything we believed we could tell them, and I'm glad we did. So the priority of informing the American public did override all of those other considerations, which is why we did what we did.

Mr. Schiff. Mr. Secretary, you mentioned, though, that the statement you issued didn't get much attention because of the timing of "Access Hollywood." When it didn't get much attention, why didn't the administration go further? Why didn't the President, for example, speak about this? It was left to yourself and Director Clapper to issue a written statement without any further elaboration. There were no steps taken, for example, to impose sanctions on Russia.

Why weren't those additional steps taken when the first notice, really, was essentially overlooked by the public?

Mr. Johnson. Well, you shouldn't view the October 7th statement in isolation, sir. First, I had been engaging State election officials since August, and I had issued a public statement on August 15th. I issued a public statement on September 16th informing the public and State officials what we knew at the time. I issued another public statement on October 1st. There's the October 7th statement, then I issued another statement on October 10th.

So this was an ongoing effort to inform the public about everything we were in a position then to tell the public. It wasn't just the October 7th statement.

Mr. Schiff. Now, that October 7th statement was notable in another way, in that it didn't include James Comey's signature as the agency that would be foremost -- have the foremost responsibility for the forensics of attribution. Why wasn't Director

Comey's signature on that statement?

Mr. Johnson. Well, the thinking was that a statement should come from the Intelligence Community, and Jim Clapper then sat atop of the Intelligence Community as the DNI.

Separately, we wanted to put out a statement from DHS about what State election officials can do about this and, again, encourage them to come to us. At some point in the discussion Jim and I decided to just make it a joint statement, and that's what happened.

Mr. Schiff. There have been public reports in the last week or 2 that the Russian probing of our elections infrastructure was far more widespread than has been publicly acknowledged and may have affected dozens of States. What can you tell us about what was known at the time and what you know now in terms of the length and breadth of Russian probing of our elections infrastructure, how widespread was it, and did it go beyond penetration of voter databases or manipulation of data in any way?

Mr. Johnson. It was very definitely in the fall a growing list of States where we saw scanning and probing around voter registration databases, which concerned us greatly. As I think I stated in one of my public statements, probably the October 1st statement, in at least one or two instances the effort was successful at an intrusion.

So there was a growing list, and we saw the scope of this activity expanding as time progressed. And then eventually, in January, we were in a position to say that this activity itself was also the Russian Government.

Now, I too have seen the more recent reports. I have not had access to classified information for 5 months, so I am not in a position to tell you whether it's right or wrong. But very definitely, as fall progressed, we saw a progression of scanning and probing activities around voter registration databases, which concerned me, which is why I kept

encouraging State officials to come and seek our help.

Mr. Schiff. Did that involve a majority of the States?

Mr. Johnson. Yes. And I was very pleased about that. Eventually --

Mr. Schiff. I'm sorry. I don't mean -- I don't mean the -- that they took you up on the help. But did the Russians probe a majority of the States' voter databases?

Mr. Johnson. I don't know the final count, because I haven't had access to the intel for the last 5 months. I know what I see open source, and I'm not in a position to agree or disagree. I've seen open source, I think, 39 States, and I'm not in a position to agree or disagree.

Mr. Schiff. Thank you, Mr. Chairman.

Mr. Conaway. The gentleman's time has expired.

Mr. Gowdy, 5 minutes.

Mr. Gowdy. Good morning, Mr. Johnson.

Mr. Johnson. Good morning, sir.

Mr. Gowdy. I want to start by thanking you for your service to our country, which includes a very successful stint as an AUSA. So you will recognize some my questions as being leading questions. They are not leading from the standpoint of I'm trying to trick you as more in the interest of time. So if I say something you disagree with, interrupt me, stop me. It's just in the interest of time, I want to see if we can get some things out of the way that we all agree on.

Russia has a history of cyber attacks against our country. Is that true?

Mr. Johnson. Yes.

Mr. Gowdy. In the parlance of our former jobs, Russia would be considered a career offender as it comes to seeking to undermine the foundations of our Republic. They are constantly trying to attack the foundations and firmament of our Republic. Is

that fair?

Mr. Johnson. I think that's a fair statement.

Mr. Gowdy. All right. So they are a career offender. They have a history of cyber attacks on our country. We suspected before the November elections --

Mr. Johnson. As do others, by the way.

Mr. Gowdy. Sir?

Mr. Johnson. As do others, by the way.

Mr. Gowdy. Yes, sir. It's not just them, but for purposes of this morning, I want to focus on Russia.

We suspected before the November elections that they might attack our voting infrastructure. Is that fair to say?

Mr. Johnson. Yes.

Mr. Gowdy. In fact, you warned that they were going to do so.

Mr. Johnson. I was very concerned that they would do so, which is why I kept issuing all these public statements. Yes, sir.

Mr. Gowdy. All right. At the time you separated from service in January of 2017, you have seen no evidence that the Russians were successful at changing voter tallies or voter totals.

Mr. Johnson. Correct.

Mr. Gowdy. At the time you separated from service in January of 2017, had you seen any evidence that Donald Trump or any member of his campaign colluded, conspired, or coordinated with the Russians or anyone else to infiltrate or impact our voter infrastructure?

Mr. Johnson. Not beyond what has been out there open source and not beyond anything that I'm sure this committee has already seen and heard before directly from

the Intelligence Community. So the only thing I'd have on that is the derivative of what the Intelligence Community has and the law enforcement community.

Mr. Gowdy. Speaking of the Intelligence Community, it strikes me that most of the information currently available was available in the fall of 2016. Most of the intelligence products that are relied upon to form certain assessments, that underlying data was available in 2016, some of it before the election.

Mr. Johnson. I'm not in a position to agree or disagree with that, because I don't have access anymore to intelligence over the last 5 months.

Mr. Gowdy. Well, looking at this a different way, before the election in November of 2016 you had already seen evidence of Russian efforts to impact our election. In fact, you testified --

Mr. Johnson. Yes.

Mr. Gowdy. -- they had a preference for a candidate, they were aggressive, and I think you used the phrase "plain and simple."

Mr. Johnson. Yes. With respect to efforts to hack into the DNC and other political organizations, yes, very clearly.

Mr. Gowdy. All right.

Mr. Johnson. Correct.

Mr. Gowdy. This is, I guess, what I'm getting at. They are a career offender when it comes to attacking the foundations of our Republic. They have a history of cyber attacks on our country. You warned before the elections that they may attack our voting infrastructure. After the election, President Obama took steps to target Russia and you took steps to consider our voting apparatus to be critical infrastructure.

Given what we knew before the election, what more could we have done and should we have done? We weren't surprised that Russia was doing this to us. They

always do it to us. So what more could we have done, should we have done, before the election?

Mr. Johnson. Well, hindsight is brilliant. Hindsight is 20/20. I'll preface my answer by saying, I think it was unprecedented, the scale and the scope of what we saw them doing, and there have very clearly been intrusions before by a number of State actors, as I'm sure you're aware.

You know, in retrospect, it would be easy for me to say that I should have brought a sleeping bag and camped out in front of the DNC in late summer, with the benefit of hindsight. I can tell you for certain that in the late summer, fall, I was very concerned about what I was seeing, and this was on my front burner all throughout the pre-election period in August, September, October, and early November, to encourage the States to come in and seek our assistance. And I'm glad that most of them, red and blue, did.

Hindsight is perfect, 20/20. But I'm satisfied that this had my attention. It had the attention of my people, because I pushed them at every step of the way to make sure we were doing everything we could do. But, obviously, there are lessons learned from this experience, and for the future there is probably more we can and should do.

Mr. Gowdy. For the States, if I remember correctly, you had a conference call or otherwise communicated with the States to offer them your assistance prior to the election.

Mr. Johnson. Correct.

Mr. Gowdy. And if I remember your testimony correctly, their response vacillated between neutral and opposed.

Mr. Johnson. Correct. It was to the issue of designating them as critical infrastructure.

Mr. Gowdy. Okay.

Mr. Johnson. Correct.

Mr. Gowdy. Do you know, without naming the States, whether any of the States most vocally opposed to that designation were, in fact, impacted by Russian efforts?

Mr. Johnson. I'd have to look at both lists. If you're saying impacted, were they -- were those States, States that had their voter registration databases scanned and perhaps infiltrated, I'd have to look at both lists, sir. I don't have the information off the top of my head.

Mr. Gowdy. What I'm wondering is if any of the States most vocal in rejecting your help actually needed it the most.

Mr. Johnson. Well, again, they didn't reject our help. Thirty-six of them accepted our help, but they were resisting the idea of a designation to be critical infrastructure, which I went ahead and did anyway.

Mr. Gowdy. What would that designation have done in November or in October? What would that designation have accomplished had you done it in the fall of 2016 instead of January?

Mr. Johnson. Well, as I outlined, I outlined earlier the advantages of that declaration. But in the short term, my assessment was that we needed to get them in. We needed to bring the horses to water to seek our cybersecurity help. And so making the designation would have, in my assessment, driven them in the opposite direction. And my number one priority pre-election was to get them to seek our cybersecurity help, and for the most part they did.

Mr. Gowdy. Thank you, Mr. Secretary.

Mr. Conaway. The gentleman's time has expired.

Mr. Himes, 7 minutes.

Mr. Himes. Thank you, Mr. Chairman.

I'll begin by yielding a moment to the ranking member.

Mr. Schiff. Thank you, Mr. Himes.

Just a quick follow-up. You've been asked, Mr. Secretary, about whether the vote tallies were impacted. Some have suggested that because the actual counting of the votes by the machines wasn't impacted that, therefore, you're testifying and others have testified there was no effect on the election. These are two quite different things.

In your written statement, you state, "I am not in a position to know whether the successful Russian Government-directed hacks of the DNC and elsewhere did in fact alter public opinion and thereby alter the outcome of the Presidential election."

Mr. Johnson. Correct.

Mr. Schiff. Do you stand by that?

Mr. Johnson. Yes. And thank you for the clarification.

Mr. Schiff. And it's not really the job of the intelligence agencies to determine whether the information that was dumped had a determinative effect on the outcome, only whether machines were impacted, not people.

Mr. Johnson. Correct. You'd need a social scientist or a pollster to do that.

Mr. Schiff. I also wanted to ask you about the information concerning potential coordination with the Russians. Are you aware of the basis, because we've heard testimony that the FBI investigation was somewhat compartmentalized and even Director Clapper wasn't fully aware of what went into the FBI counterintelligence investigation, are you aware of the information that formed the basis for Director Comey opening a counterintelligence investigation, as you testified in July of last year?

Mr. Johnson. No, not as I sit here. And if I did, I'm not sure I could talk about it in open session. But I do not.

Mr. Schiff. And I'm not going to ask you to. But do you believe that Director

Comey would have opened a counterintelligence investigation on a Presidential campaign lightly or on mere hunch?

Mr. Johnson. No.

Mr. Schiff. He would need some evidentiary or information basis to do so.

Mr. Johnson. Based on everything I know about Jim Comey and the FBI, yes.

Mr. Schiff. I yield back to Mr. Himes.

Mr. Himes. Thank you.

And good morning, Mr. Johnson.

I want to start by asking you, Mr. Gowdy's questions and your responses established that this is not a new thing, this sort of meddling in our election. We've seen it before. And I want to come back to that. But you also stated and we've heard from others that the meddling in the 2016 election was unprecedented in its scope and reach.

So I wonder if you might take a minute or 2 and just help us better understand why it was unprecedented? What was different about this particular array of meddling versus what we've seen in the past.

Mr. Johnson. Well, we've seen a history of various different types of bad cyber actors intruding into, infiltrating political organizations, political campaigns, and that's what I was referring to.

When I say that this effort was unprecedented, what I mean is that we not only saw infiltrations, but we saw efforts to dump information into the public space for the purpose of influencing the ongoing political campaign. And it was widespread. And in that respect -- and we knew it was happening. So in that respect, it was very much unprecedented.

Mr. Himes. So can I, just distilling your testimony, we had seen scanning,

queries, what we might sort of generally considered espionage --

Mr. Johnson. Correct.

Mr. Himes. -- trying to gathering information.

Mr. Johnson. Correct.

Mr. Himes. But we had never seen what the Russians call active measures, that is to say, actually the insertion of information designed to alter an outcome. That's what makes this unprecedented?

Mr. Johnson. Yes.

Mr. Himes. Thank you.

So let's step back a little bit away from how this is unprecedented. We have seen this before. In 2008, Chinese hackers targeted then candidate Barack Obama and John McCain. We saw it again in 2012.

So my question is, as you assumed your duties at Homeland Security, how were we thinking about this? Were we thinking about this issue in a constructive way prior to the last election?

Mr. Johnson. Good question. It became a front burner item for me in summer 2016, and I began discussions with my staff about what should we be proactively doing to help the State election officials prepare. I was pleasantly surprised to know that there was an Election Assistance Commission and that DHS had collaborated with that and that there had been an ongoing dialogue through the EAC, through State Secretaries of State, going back to election cycles past.

But this had -- this was now becoming a matter for me as the Secretary of Homeland Security, so it was becoming front burner for me in the summer of 2016. But there had been that ongoing dialogue.

Mr. Himes. So summer 2016 this becomes front burner, implying that prior to

2016, this had been back burner. What was the catalyzing event that moved it from back burner to front burner?

Mr. Johnson. For me, personally, it was the reports we were receiving about efforts to intrude into the DNC and the emerging intelligence picture.

Mr. Himes. Okay. Let's get a little more granular here. Becomes a front burner issue. Were there certain parts of the process at the time, the voting machines, the political party databases, the politically associated organizations that we understand may have been probed, that you thought were particularly vulnerable at the time?

Mr. Johnson. Voter registration databases. In the course of learning about this issue myself, I took a look, along with my staff, at the practices in the different States. They tend to vary. But for the most part, there are redundancies in the system, and most of it exists off the internet in terms of collecting votes, reporting votes. There are a few States where it does not.

But the States, with some DOJ, Election Assistance Commission help, have been engaging in some best practices, but they tend to vary all over the lot. But what we were most concerned about and what we were seeing were efforts at compromising voter registration databases.

Mr. Himes. Okay. You said something that in my very limited time I don't want to let drop. You said you thought there is more that we could and should do to address this issue.

Mr. Johnson. Yes.

Mr. Himes. Can you just elaborate on, if you were still Secretary of Homeland Security, what would your recommendations be at this time?

Mr. Johnson. A number of things. One, I would, as a Congress, think about whether -- I would think about grants to State election officials to help them harden their

cybersecurity. I would raise awareness among State election officials as well as, you know, public in general, employees of State governments, raise awareness about the evils and the hazards of spear-phishing.

I think at a national level there should be, in this current administration, somebody who really does take the mantle of cybersecurity on full time to highlight this issue, to lead the charge on this issue. My preference would be somebody within DHS. But we really need a national leader to take charge of this issue.

But first and foremost on the ground, we need to encourage State government, State election officials to engage in best practices when it comes to vote tallies and so forth, and through grants, we ought to consider grants. I hear that from State election officials themselves.

Mr. Himes. Thank you.

Thank you, Mr. Chairman. I yield back.

Mr. Conaway. The gentleman's time has expired.

Mr. King, 7 minutes.

Mr. King. Thank you, Mr. Chairman.

Mr. Secretary, it's good to see you again. I've had privilege of working with you closely on the Homeland Security Committee when you were Secretary, and I commend you for your service, truly an outstanding job, and your career in public service, Defense Department, assistant U.S. attorney, and now as a successful lawyer, I'm sure.

Just a few points before I yield to Mr. Gowdy.

Can you elaborate more on what the DHS' connection with the DNC was or consultation with the DNC was after you became aware of the hacking, they became aware of the hacking, as to what was offered them, what they accepted? Was there any level of cooperation at all?

Mr. Johnson. To my disappointment, not to my knowledge, sir. And this is a question I asked repeatedly when I first learned of it. What are we doing? Are we in there? Are we helping them discover the vulnerabilities?

Because this is fresh off the OPM experience. And there was a point at which DHS cybersecurity experts did get into OPM and actually help them discover the bad actors and patch some of the exfiltrations or at least minimize some of the damage.

And so I was anxious to know whether our folks were in there. And the response I got was: FBI had spoken to them, they don't want our help, they have CrowdStrike, the cybersecurity firm. And that was the answer I got after I asked the question a number of times over the progression of time.

Mr. King. And that was, I assume, totally different from the reaction you got from OPM?

Mr. Johnson. The OPM efforts, we were actually in there, onsite, helping them find the bad actors.

Mr. King. Do you know who it was at the DNC who made that decision or who was making the decisions?

Mr. Johnson. I don't, no.

Mr. King. Do you know if the FBI continued to try to help, try to assist?

Mr. Johnson. I have -- I've read in The New York Times about those efforts sometime earlier this year.

Mr. King. I move to strike all references to The New York Times.

I would just say, maybe it's editorializing on my part, that really is to me an unusual response by the DNC. I mean, if you are talking about a Presidential election, you have an unprecedented amount of cyber hacking by a foreign power, an adversary, from my point of view, and that they would not accept all the help that could possibly be

given, especially, I mean, it's not as if -- not that you would be partisan or anyone else -- but it's not even like it was a Republican administration trying to intrude into the DNC. This is an impartial governmental entity, FBI, DHS, and they didn't accept that. I just find it very hard to, you know, to comprehend.

Mr. Johnson. Well, my interest in helping them was definitely a nonpartisan interest.

Mr. King. Yeah. I know that, yeah.

Mr. Johnson. And I recall very clearly that I was not pleased that we were not in there helping them patch this vulnerability. The nature of -- the nature of -- when you're dealing with private actors and even political organizations, we don't have -- we, DHS, does not have the power to issue a search warrant or get a search warrant and go in and patch their vulnerabilities over their objections.

Mr. King. I understand.

Moving ahead, was there any significant intelligence or information that came about after the election that was not available before the election? In other words, if there was so much out there, if the administration was so concerned, why was it that suddenly after the election it seemed, you know, somewhat serious action was taken, sanctions -- well, sanctions in particular. And also the public statements by the President, by the Intelligence Community, coming out, really coming on strong, and yet I didn't see what was present after the election that wasn't there before the election.

Mr. Johnson. Well, I'm going to disagree with your premise, sir. We did before the election, 1 month before the election, formally and very publicly accuse the Russian Government of doing this in pretty blunt terms uncommon for the Intelligence Community. That statement was pretty blunt, in saying we know the Russian Government is doing this based on the picture we saw at the time.

The picture continued to build upon itself as time progressed. There was more we knew about the Russian Government's efforts at scanning voter registration databases.

You'll recall the October 7th statement say we were not then in a position to attribute that to the Russian Government, but the picture got clearer as time progressed. But on October 7th, we issued a very clear declaration, based upon what we knew at the time, that the Russian Government was behind the hacks of the DNC.

Mr. King. I'm not at all being critical of you. I'm just saying that it seemed if the administration --

Mr. Johnson. It just didn't get the attention that I would have preferred it get, because we're in the midst of a campaign, we're -- the press and the voters are focused on lots of other things, like 11-year-old videos.

Mr. King. I'm thinking more about the administration, with all the power they have. Because in December we had this drumbeat of stories coming out, one after the other, some open, some being leaked. And then you had sanctions being issued.

It seemed that all the power and mobilization of the administration to get that story out came after the election, into December and early January, and between October 7th and election day there was very little. As you say, the October 7th statement was overshadowed by the other incidents that were occurring at the time.

So I think you did what you had to do, but I'm just saying, I'm just so concerned -- not concerned, but --

Mr. Johnson. Well, very definitely, the October 7th statement was an administration statement. That was the result of an Intelligence Community assessment. The President approved the statement. I know he wanted us to make the statement. So that was very definitely a statement by the United States Government,

not just Jim Clapper and me.

Mr. King. No, but in reality, though, most of the American people were not fully aware of it. In view of all else that was going on, I just would have thought during that 32 days -- if they had done as much during the 32 days from October 7th to November 8th as they did in December and January, I think the American people would have been a lot better informed when they went to the polls. And I'm just wondering why they didn't do it.

Mr. Johnson. Well, I can tell you I issued statements on September 16th, October 1, October 7, and October 10 about what we saw, specifically directed to State election officials.

Mr. King. You did your job. I'm not questioning you in any way about that. I'm really asking about the administration overall.

And with 30 seconds, Trey.

Mr. Gowdy. Just real quickly, if I could get you to put on your old hat for a second.

Hacking into one's server strikes me as a crime.

Mr. Johnson. Yes.

Mr. Gowdy. So the DNC was the victim of a crime. I'm trying to understand why the victim of a crime would not turn over evidence to you and Jim Comey, who were both apolitical and come from apolitical backgrounds.

Mr. Johnson. Well, I'm quite sure that at some point in the timeline they did do that. My point earlier was that in the initial period I was not satisfied that we were able to get in there ourselves, DHS, to help them identify the bad actor and patch the vulnerabilities. I'm quite sure that at some point the FBI and the DNC had a dialogue, but you'd have to ask them.

Mr. Conaway. The gentlemen's time has expired.

Ms. Sewell, 5 minutes.

Ms. Sewell. Thank you, Mr. Chairman.

I would like to yield a minute to the ranking member to ask a question.

Mr. Schiff. I thank the gentlewoman.

I just want to follow up on Mr. King's comments and question, because I really agree quite completely with Mr. King. And I'm not saying this as a matter of hindsight. Senator Feinstein and I were saying this in real time as it was going on.

Why didn't the President of the United States -- and, Mr. Secretary, you did what you could do -- but why didn't the President of the United States, at the time you were making your attribution or thereafter, speak to the American people and say, "A foreign power is interfering in our affairs?" This isn't a Democratic thing, this isn't a Republican thing, this is an American thing, and they need to be rejected and they need to stop.

Why wasn't that done? Was there thought given to that? Why was that course rejected?

Mr. Johnson. Well, again, Congressman Schiff, we did make the statement. And we were very concerned that we not be perceived as taking sides in the election, injecting ourself into a very heated campaign. And so -- or taking steps to themselves delegitimize the election process and undermine the integrity of the election process.

And so we considered those things, and the decision was made that the Director of National Intelligence and the Secretary of Homeland Security should together make this statement. And there were public statements made by various administration officials, including myself, all through the campaign season, pre-election, to the same effect.

Mr. Schiff. I yield back to Ms. Sewell.

Ms. Sewell. Secretary Johnson, welcome. Again, thank you for your years of service to this great Nation.

I'd like to talk about attribution. And by now it's well known that the Russians hacked, stole, and then strategically dumped emails from the DNC in order to affect the outcome of the 2016 election.

What I'd like to understand better is how the United States Government came to reach that conclusion and how DHS and the rest of the government were able to attribute it directly to the Russians.

So according to the declassified Intelligence Community assessment released in January of 2017, we noted that Russian intelligence accessed, quote, "accessed elements of multiple State and local electoral boards," and that seems pretty clear.

How do you -- how does one go about attributing that to the Russians? What kinds of information signatures or cyber activity would you be looking for in order to make that attribution? And how do you go about validating that information?

Mr. Johnson. Congresswoman, you'd probably have to have that discussion in closed session, because it's sources and methods, and it's probably better to have that discussion with someone in the Intelligence Community.

I do recall that, looking at the intelligence, it was a pretty clear case -- perhaps beyond a reasonable doubt, Mr. Gowdy -- that the Russian Government was behind the hacks into the DNC based on everything I was seeing.

In terms of attribution, there are normal considerations about when one makes public attribution to a State actor who is engaged in some type of cyber attack. My personal opinion was that and is that those normal considerations were out the window and that we had an independent, overriding need to inform the voting public of what we saw going on.

And the way I looked at it as a corporate lawyer was, if I'm the issuer of a public stock and I see a very powerful actor in the market trying to manipulate the price of my public stock, I have a duty to tell the investing public what I know.

Ms. Sewell. Now, how did you go about alerting the States -- DHS go about alerting the States and local communities about what was going on? And I know that you did the designation for critical infrastructure. What I'm trying to get at is, given your background and your recommendation that we do something more now to really alert the State and local governments, how do we do it now? And what would you suggest would be a better way to go about alerting them of something?

Mr. Johnson. Well, we did have an ongoing dialogue all throughout the fall with State election officials. At the law enforcement level, with DHS, there was of course the public October 7th statement, but the conversation didn't stop there. I continued to issue public statements, and we continued to have a dialogue with State officials as they came in to seek our cyber assistance at the staff level.

In answer to your question --

Ms. Sewell. But only if they came to get your assistance would DHS be more helpful in that sense? So you really left it up to the States and the local governments to actually request help?

Mr. Johnson. I think it's the case that we had a dialogue with just about every single of the 50 States. Eventually, ultimately, we had a dialogue with, I think, all but maybe one or two of the States. And they actually signed up for our cybersecurity assistance. There were 36, along with a whole lot of counties and cities, that actually signed up for our assistance. But we were pushing information out the door to everybody as often as we could.

But in answer your to your question, I think that -- the States are -- one thing I

discovered in this conversation, State election officials are very sensitive about what they perceived to be Federal intrusion into their process. I heard that firsthand over and over: This is our process. It's our sovereign responsibility. We're not interested in the Federal takeover. And they were very --

Ms. Sewell. But doesn't the Federal Government have an interest in the integrity of these elections?

Mr. Johnson. I think the American public, the Nation, has an interest in the integrity of the election, and I think you federally elected officials have an interest in the integrity of the elections that result in you sitting here, yes.

But I think that we need to continue, now that the campaign is over, maybe in odd years, if we could find a way, to raise awareness, when the temperature is down, maybe through grants, encourage best practices at the State level, and maybe encourage a uniform set of minimum standards for cybersecurity when it comes to State election systems and voter registration databases.

Ms. Sewell. Thank you.

Mr. Conaway. The gentlelady's time has expired.

Mr. LoBiondo, 5 minutes.

Mr. LoBiondo. Thank you, Mr. Chairman.

Mr. Secretary, thank you for being here. Thank you for your service.

Some of this may be a little bit redundant, but I'm trying to really better understand how all the different entities have come together. Can you briefly summarize DHS' role in cyber defense?

Mr. Johnson. To summarize it, we are the agency of the U.S. Government responsible for asset response. So responsible for working with other Federal agencies and the private sector in identifying vulnerabilities, patching vulnerabilities, raising

awareness. And because of the help we got from Congress, we are the principal portal through which information from the private sector should pass to the U.S. Government. So that's it in a summary.

Mr. LoBiondo. And with that in mind, can you briefly tell us DHS' role in sharing cyber threat indicators, how that works?

Mr. Johnson. On my watch, it was the -- and this is an acronym -- the NCCIC, the National Cyber Communications Integration Center, is the place designated to receive cyber threat indicators and report them.

Mr. LoBiondo. Okay. Switching gears a little bit, based on what you know now, what would you have done more or differently in response to the Russian cyber attack of the 2016 election?

Mr. Johnson. Well, with the benefit of hindsight, there is always more things you can say to yourself I should have done. Like I said earlier, you know, with the benefit of hindsight, perhaps I should have camped out at the front doors of the headquarters of the DNC.

But at the time, knowing what we knew and wrestling with all the considerations we had, I can tell you that this was very much a top priority for me, because none of us knew how this was going to come out and how far the Russians were going to go in their efforts.

And so I can tell you with the benefit of hindsight, that this was a top priority for me. And virtually every day during the campaign season, I was questioning my own staff about: Are we mobilized? Are we energized enough to do what we need to do? Have we set up a crisis response center on election night? Which we did.

At one point, and I said this in my prepared statement, I picked up the phone and called the CEO of Associated Press, that has and has had for years the responsibility for

election night reporting, to make sure that their systems were satisfactory, and I was satisfied that they have enough redundancies in their system as well.

So this was something that was, you know, very much uppermost in our minds in the runup to the election.

Mr. LoBiondo. Okay. So thinking ahead to 2018 and 2020, what scenarios -- two-part question -- what scenarios most concern you? And what recommendations do you have for us that we should do that maybe is something that's not in place now?

Mr. Johnson. Well, the scenarios that most concern me about the integrity of elections are not necessarily cybersecurity related. But in the cybersecurity realm, what I do worry about are the vulnerabilities around State voter registration databases, and we saw those vulnerabilities last fall. And so I think there needs to be more done to secure voter registration databases so that that information doesn't get out in the open.

Mr. LoBiondo. So from a congressional approach, somehow grants to the States for databases, or anything specific you recommend?

Mr. Johnson. I know that the States -- State election officials are very sensitive to and would oppose, likely, Federal standards for how they should run their elections. It's very hard to bring about. I remember the debate about HAVA in 2002. So I would use the carrot approach instead of the stick approach and encourage them through grants to bolster their own cybersecurity.

[11:00 a.m.]

Mr. LoBiondo. And what specific policy changes, if any, would you recommend to your successor, Secretary Kelly?

Mr. Johnson. In addition, to all the things we just discussed, I think it's important that Secretary Kelly or the Under Secretary for NPPD really take this on as a front burner issue. When I came into office in 2013, I viewed counterterrorism as the cornerstone mission of DHS. And then, after a time, when I got sense of the threat environment, I realized that cybersecurity needed to be the other cornerstone, needed to be the other top priority of our Department's mission. It's going to get worse before it gets better and bad cyber actors all the time are more and more ingenious, more tenacious and more aggressive. And so I would urge Secretary Kelly to make this one of his top one or two priorities.

Mr. LoBiondo. Thank you.

I yield the balance of my time to Mr. Gowdy.

Mr. Gowdy. I thank the gentleman.

Director Johnson, I don't want to beat a dead horse, but I do think it's important, the last time you and I talked, I wasn't 100 percent sure, but I have since had it confirmed: The DNC never turned the server over to law enforcement. So twice now you have said that you could have camped out in front of DNC, and I would say, in defense of you, it wouldn't have made any difference if you had because they weren't going to give you the server. So, if you're investigating, either from a law enforcement or from an intelligence standpoint, the hacking by a foreign hostile government, wouldn't you want the server? Wouldn't that help you, number one, identify who the attacker was? And if memory serves me, this was early in the summer of 2016 when we learned of the DNC hack. So, if they had turned the server over to either you or Director Comey, maybe we would have

known more and maybe there would have been more for you to report.

So I guess what I'm asking you is, why would the victim of a crime not turn over a server to the intelligence community or to law enforcement?

Mr. Johnson. I'm not going to argue with you, sir. That was a leading question, and I'll agree to be led.

Mr. Conaway. The gentleman's time has expired.

Mr. Carson for 7 minutes -- oh, excuse me.

My general counsel has informed me that our unanimous consent order to extend the conversation for 7 minutes per member is only good for an hour. So I ask unanimous consent that each member has 7 minutes to question the witness. And, hearing no objections, we will continue down that path.

Mr. Carson, 7 minutes.

Mr. Carson. Thank you, Chairman.

Thank you, Mr. Johnson, for your service to our country.

We've heard since last year about Russian bots that were released on the internet, generating and disseminating fake news on social media platforms. As far as you understand, sir, how do these bots work? And how did we come to discover them? And how effective were they in basically shaping opinions? And how did they interact with social media to make their campaign most effective?

Mr. Johnson. Congressman, you're really testing me here.

Mr. Carson. You're a brilliant man.

Mr. Johnson. -- to a technical level that I'm -- there are others that could sit here and give you a much better answer. It's hard to know. I mean, the activity you cited I know is prevalent.

Mr. Carson. Sure.

Mr. Johnson. It is hard to know to what extent it influences public opinion. Like I said earlier about the election result, it is hard to know -- it is not for me to know to what extent the Russian hacks influenced public opinion and thereby influenced the outcome of the election.

Mr. Carson. Sir, do you think, as I do, that the Kremlin on some level managed to stoke uncertainty about our electoral institutions and thus their operation was successful? And, secondly, do you think with the Russian influence or interference operation, all of which Americans were victims, even if their votes weren't effective, offers us any had lessons learned, sir, that we should carry on with us as we prepare for 2018?

Mr. Johnson. Well, certainly, if the Russian aim of what they did was to distract us and divert us from the business of government, whether it's healthcare or something else, yes. I mean, as evidenced by what we are doing here today.

Again, I think the answer has to be greater workforce awareness among those who use, whether it is the DNC or, you know, House.gov or the private sector, raising awareness among those who use the system about unrecognizable emails and attachments. You know, this apparently started with an email somebody shouldn't have opened. And I can tell you from experience, the most devastating attacks -- and forgot the Russians for a moment here -- the most devastating attacks by the most sophisticated actors very often start simply because somebody opens an email that they shouldn't open. So raising awareness about spear phishing can go a long way and, as I said earlier, encouraging those who are responsible for our democracy in ensuring that their cybersecurity is protected and they've done what they need to do.

Mr. Carson. Thank you, sir. Keep up the great work.

Mr. Chairman, I yield back.

I yield to the ranking member at this time.

Mr. Schiff. I thank the gentleman.

Just to follow it up on the DNC and I know my colleague, Ms. Speier, will have some questions with that too, but I take it whatever criticism you might have of the DNC for how they responded or whether they were willing to turn over the server or not, you're not maintaining that that somehow justifies the Russian hacking of our institutions?

Mr. Johnson. No, of course not.

Mr. Schiff. Because I think there's a tendency, as in many cases, to blame the victim.

Mr. Johnson. No.

Mr. Schiff. Over their victimization. The DNC was a victim here, were they not?

Mr. Johnson. Correct. Yes.

Mr. Schiff. And there's a lot we're going to have to probe in terms of the government response as well as the DNC's. The primary actor that interfaced with the DNC, would it have been DHS, or would it have been the FBI?

Mr. Johnson. Well, in a perfect world, it would be both of us. It would be law enforcement and asset response. So it would be DHS, law enforcement, and, when necessary, the intelligence community. And there have been cases where we have worked well hand in hand together, law enforcement and Homeland Security, addressing a situation.

Mr. Schiff. One of the reasons I raise this issue is and one of the reasons I think the public nature of these hearings is so important is the Russians are among the most capable cyber adversaries in the world. Are they not?

Mr. Johnson. Yes.

Mr. Schiff. And for the most part, if the Russians want to get into it the DNC or the RNC, they are going to find a way to get in. Would you agree with that?

Mr. Johnson. I tend to be not that fatalistic, especially in my old role, but it's -- you know, it's like saying, you know, sooner or later, there's going to be another act of violence in this country. But you can minimize the vulnerabilities and the opportunities through a number of steps that can be taken.

Mr. Schiff. Without question. But, nonetheless, it is a fairly asymmetric battlefield in which it is much harder to defend than it is to be on offense.

Mr. Johnson. Correct. I think I said that in my opening statement. Yes.

Mr. Schiff. And for that reason, would you agree that among the most important things we can do in addition to improving whatever our cyber defenses are or how we respond to an intrusion is to inform the public and in a sense inoculate ourselves against further foreign interference by developing a consensus that, whoever it helps or whoever it hurts, we will all reject it. Isn't that ultimately the best defense and better than any cyber defense?

Mr. Johnson. That is certainly a critical part of a needed response, which is one of the reasons why I felt strongly we should issue the October 7th statement.

Mr. Schiff. I think this is something that President Obama alluded to when he did speak to this after the election, that what in fact made this hack so successful for the Russians was that they were able to play on the deep divisions within our own politics and exploit that division to sow discord within the United States. Would you agree?

Mr. Johnson. I would -- yeah, I don't disagree with that statement. You know, certainly, the rhetoric of the campaign contributed to that as well.

Mr. Schiff. I thank you, Mr. Chairman. I yield back.

Mr. Conaway. The gentleman yields back.

Dr. Wenstrup, 7 minutes.

Dr. Wenstrup. Thank you, Mr. Chairman.

Thank you, Mr. Johnson, for being here. I appreciate it.

Mr. Johnson. Good morning.

Dr. Wenstrup. We are here to get some lessons learned and a path forward. And, hopefully, we can do that on a united front. And I appreciate your insights here today.

When you came in, in 2013, that's obviously after an election, were you given information on previous attempts in previous elections, say in 2012, 2008, or 2004, and the kinds of things that take place? Because it's been said many, many times, Russia, for example, that they have been trying to do this type of stuff in any way they could since the Soviet Union. So were you given any kind of background to maybe help you in your --

Mr. Johnson. Well, I was certainly aware, not just from my experience at DHS but from my experience as the general counsel at the Defense Department, that there had been nation-state efforts at espionage for the most part into various political organizations and campaigns.

Dr. Wenstrup. I am pleased to see that you have agreed with Secretary Kelly to make cyber a top priority, and that's probably very good advice.

During this process, was it ever reported, were there attempts on the RNC, for example, with phishing expeditions, spear phishing, was any of that reported anywhere else or any other agencies that are involved with elections?

Mr. Johnson. Yeah. So I remember there was a lot of back and forth around the RNC. Sitting here now, my head hasn't been in this for a while.

Dr. Wenstrup. Sure.

Mr. Johnson. But sitting here now, I remember there was something about the RNC. Somebody could give you chapter and verse on that. But I remember there was something around the RNC too, but I'm not sure what it is --

Dr. Wenstrup. Some attempts at least.

Mr. Johnson. My recollection here is going to be faulty, and so I just don't -- it's a knowable question.

Dr. Wenstrup. Thank you. So we're talking about hacking from an external, a foreign source and clearly an illegal activity. You look at something like -- and trying to influence an election -- and you look at something like "Access Hollywood"; I assume that was legally obtained, but trying to influence an election. I'm not trying to compare the two in any way, shape, or form. What I am going to is we talk about Russia -- we are talking about Russia today, but we're also talking about other countries. As you mentioned before, they are not alone in this process. But do we have domestic concerns as well? We're talking a lot about foreign entities trying to influence our elections through nefarious behavior. Do we have concerns domestically as well that we should be alerted to?

Mr. Johnson. Absolutely. Domestically, there are bad cyber actors that would probably have a motive in trying to affect the outcome of an election as well as, you know, theft, ransomware, a host of other things that I think we all know about.

Dr. Wenstrup. Sure. Have we seen any of that from the domestic front? I mean, I know we are talking about foreign entities today. But have we seen attempts, any successful attempts domestically to try and invade --

Mr. Johnson. Cyber attacks for a political motive, I have to believe, yes, yeah. Sitting here, I can't list them, but I'm sure there have been.

Dr. Wenstrup. I don't really want you to list them.

Mr. Johnson. You all may have been the victims of such things.

Dr. Wenstrup. I'm sure there's been attempts. That's all I have, and I thank you for being here today.

Mr. Chairman, I yield back.

Mr. Conaway. The gentleman yields back.

Ms. Speier, 7 minutes.

Ms. Speier. Thank you, Mr. Chairman.

Mr. Johnson, thank you so much for your extraordinary dedication to public service for many, many decades. So anything that I ask you now is not an effort to undermine.

Mr. Johnson. By the way, I'm billing this by the hour. Just kidding, just kidding.

Ms. Speier. So one thing that we do know is that hindsight is 20/20, and when we look back, oftentimes, we say, you know, I would have done things slightly differently. So, back on August 15, 2016 -- and this is a year later from the DNC hack -- you had a call with State officials about cybersecurity and elections infrastructure in which you said you were, quote, "not aware of any specific or credible cybersecurity threats relating to the upcoming general election systems," unquote, and then offered support by DHS. Why didn't you at that time say to the State elections officials, "Russia is intent on hacking into our systems"?

Mr. Johnson. Because I was not in a position to say that at that point. The state of my and our awareness was progressing, and I was not in a position to reveal or know exactly what we saw the Russian Government doing at that point. So it was an emerging picture. And so but, within a very short period of time, and it could have been just before, but within a very short period of time, right around that time, we began to see these intrusions scanning and probing into voter registration databases. And if you

look at my public statements, you will see that I informed State election officials of what we saw at the time.

Ms. Speier. So -- but 2 months later is when you said to them, along with James Clapper, that the Russian Government was in fact attempting to. But back in October, you encouraged jurisdictions to seek assistance. So 2 months had passed; early voting had already begun. And there is a part of me that feels that we should have been able to have sounded the alarm earlier. But at the time, on October 10th, you encouraged jurisdictions to seek assistance: 33 States used DHS tools; 17 did not. Now, if we know that there's something vicious, a viral attack is happening, why would we not want to inoculate everyone? And in this situation, because it's being left up to the States, 17 States didn't even take you up on it. Did you have a concern about that, did you reach out to them again, encouraging them to use the tools.

Mr. Johnson. We had an ongoing dialogue. And on September 16th, I said publicly: In recent months, we have seen suspicious cyber intrusions involving political institutions and personal communications. We have also seen some efforts at cyber intrusions of voter registration data maintained in State election systems.

On October 1, I said: In recent months, malicious cyber actors have been scanning a large number of State systems, which could be a preamble to attempted intrusions. In a few cases, we have determined that malicious actors gained access to State voting-related systems.

Six days later, I said the same thing again.

Ms. Speier. Okay.

Mr. Johnson. We were not in a position to attribute it to the Russian Government at that time.

And then 3 days later, I made another statement. So I was beating this drum

constantly.

Ms. Speier. I guess what I want to ask you is: In my mind, this was, this cyber attack on our country was an act of war. It was unprecedented. The Russian intentions were not just to hack into a couple of party servers, but to do a full on effort to undermine our election. So do you believe, looking back at it, that we should have or should in the future standardize election systems? We have so many different systems around the country. Some have paper trails; some do not. Is there value in going back to paper voting?

Mr. Johnson. Well, I would say too this Congress, if you want to try to federalize elections in this country, good luck. I think you probably all know better than I do the reaction you'll get from your State election official constituents.

Ms. Speier. Well, how about the equipment, though?

Mr. Johnson. Again, there was an effort at this with HAVA right after the 2000 election. We made some progress, but this is something where I think a carrot over stick approach is best warranted. And so, through grants and other means you might have at your disposal, I would encourage State election officials to adopt certain minimum cybersecurity standards.

Ms. Speier. Voter registration lists were infiltrated. We have heard over and over again that we don't believe any of the votes were altered. I want to know how we can be confident that none of votes were altered, first of all.

And the second question is having -- if in fact that's the case, I don't think any of us should be sanguine in thinking that the Russians won't attempt to alter votes in subsequent elections. Do you agree with that?

Mr. Johnson. Well, I have said, based upon what I know, I know of no evidence that votes were altered as a result of cyber attacks. But, again, I have not had access to

classified information in 5 months. And, at this point, you all are in a better position to know the answer to that question than I am.

Ms. Speier. So, during -- after the election, did DHS take any steps to determine whether or not the vote had been impacted by Russians? What kind of steps could or would have been taken?

Mr. Johnson. No, and I'm not sure I had the authority to do that. I don't -- the Department of Homeland Security does not engage in vote recounts, election recounts. There are others that have that responsibility.

Ms. Speier. So what methods would you like to send to State and local election officials regarding just how vulnerable their systems are to compromise?

Mr. Johnson. I would say that your voter registration databases are very vulnerable to exfiltration, exposure, and that all State election officials, local election officials should undertake an effort to harden their cybersecurity, minimize the exposure of the process to the internet, and that this is serious and we're not just -- this is not just an academic exercise; it is a very real threat, and we know because of what happened last year.

Ms. Speier. Thank you.

I yield back.

Mr. Conaway. The gentlelady's time has expired.

Mr. Stewart, 7 minutes.

Mr. Stewart. Thank you, Mr. Chairman.

And, Mr. Secretary, thank you. I join with others in thanking you for your service. We had a chance to sit down together last week at the dinner. I enjoyed that, and I walked away impressed as I think many people obviously would be.

I'm going to ask you a series of questions if I could. I have to tell you I don't think

you're going to like them, and I think they are going to be difficult to answer.

But, before I get to them, I want to set the table, if I could. I was in Moscow last summer. I came home from Russia, and I said: They are going to mess with our elections. And that wasn't based on any particular specific piece of intelligence, it was just based on commonsense and history and the things that we know, some of them we have been discussing here today.

I think we have to agree that this mission, they were overwhelming successful. I mean, some KGB captain just got promoted to four-star general on this mission because it was a resounding success from their point of view. They have to be thrilled with the outcome. And if success breeds success, and it does, then we have to anticipate that they are going to try and do it again, not just here in the United States, but, as we have seen, throughout other Western democracies, because democracies are vulnerable. And I think I want to emphasize this point: Politically divided democracies are particularly vulnerable. And I think that's where we find ourselves.

So we ask this question: What do we do? And that's what we've been discussing with you here today. That's the point of this hearing. Frankly, I think that's the primary point of the intelligence process here in this question, is, what do we now do?

Now, some of that has been diverted from, I think, our primary goal, and some of it has been diverted unfortunately by what I think is political grandstanding. So I want to come back to it. What do we do?

Now, Mr. Secretary, it leads me to my questions. Yeah, so we can defend against email hacks. And that's an obvious thing to do. I think we can train people not to be victims of phishing, which some of the DNC officials were. You can product voter registration machines. You can protect the voter machines and the registration

databases. But this is the difficult part: How do you protect against propaganda? How do you protect against false news stories? How do you protect against internet trolls who we know are paid Russian employees? And the last question, this is a tough one: How do you encourage a gullible press to be more mature in their judgement, more defined in their judgements, rather than play into Russian hands. I think those are the real challenges we have. And if you have views on that, I would love to hear them because I think that's where we are going to go crossways in the future.

Mr. Johnson. All I can say is wow. Where do I begin?

Mr. Stewart. Well, I appreciate that response because that indicates your agreement that this is a real challenge for us. Is that true?

Mr. Johnson. I would encourage you to look at a speech I delivered at Westminster College in Missouri in September 2015, where I said that I believed it was the responsibility of those who hold public office and seek public office to be responsible in their rhetoric, those who command a microphone. Well, that's for starters, because overheated rhetoric can hurt innocent people. You know, God bless the First Amendment. You know, anybody with a keyboard now and access to the internet can say virtually anything they want about any public official in this room and you have little or no recourse because of the First Amendment and the way it is interpreted. That's the age in which we've evolved.

I grew up when we had gatekeepers to news, and I suspect you did too: Walter Cronkite and others. In the 1970s, if a big event happened in the course of the day, in my house it didn't really happen until Walter Cronkite told me it happened at 7 o'clock. And that's when I in my own mind accepted it.

Now, with the 24/7 news cycle and the internet and so many people out there who call themselves journalists, who can say virtually anything without fact-checking,

make virtually any accusation, and there are a whole lot of people who rely on that information, it's a new frontier.

Mr. Stewart. And if I could, sir, interject quickly. It is not just those who call themselves journalists. In too many cases, they are actual journalists. And some of the institutions -- and I won't name them -- but some of these reliable or formerly reliable media outlets that we know now have just, as I said, have completely played into Russian hands in some of the reporting that they've provided us.

Mr. Johnson. That's a whole separate subject.

Mr. Stewart. Yeah. And I interrupted you. I don't know if you --

Mr. Johnson. No, no, I think my views on this subject are probably shared by lots of members of the committee.

Mr. Stewart. Well, thank you.

And, again, just to conclude, democracies are vulnerable. And it is easier to protect your email account. It's hopefully achievable that we can protect voting machines. But Russian active measures are relentless. They are pervasive. They are everywhere, and we don't recognize it, or, as we have said, too often we play into their hands and make it altogether too easy for them. And we do that to ourselves, and I just think we have to have a conversation with our fellow Americans about, how do we discern what's real and not real? And how do we discern what's manipulated and what's not manipulated? And it will be interesting to see what happens in some European democracies as their elections come up and in our own over the next few years if we are better at dealing with this.

And, finally, sir, once again, thank you for your many years of service. We are grateful for that.

Mr. Johnson. Let me just add to that in the time remaining. Every time I have

an opportunity to sit down with a group of young people, like the interns over here, I always ask the same question: How do you get your news?

Because I'm interested to know how young people receive news. And it's not the way you and I grew up receiving news. When I do my daily commute into New York City, I'm probably the only person in the train in that car with a hardcopy of a newspaper anymore. That's how I still get my news or at least on the second or third pass anyway. When I was at DHS, I got my news through the daily intelligence briefing, and then I'd read the newspaper to see how they were covering the news. But it's fascinating to me that more and more people are getting their news in more and more different ways.

Mr. Stewart. No doubt about it.

Mr. Johnson. Less discerning ways.

Mr. Stewart. You know, and Americans have gotten so that, if I see it in the news, unless it is a sports score, I'm not sure I believe it. And even the sports scores I'm going to check twice.

So thank you.

Mr. Chairman, I yield back.

Mr. Conaway. The gentleman's time has expired.

Mr. Quigley, 7 minutes.

Mr. Quigley. I yield 1 minute to the ranking member.

Mr. Schiff. I thank the gentleman.

Mr. Secretary, I just want to follow up on one of Jackie Speier's questions. You mentioned that a message you would have for the States would be that their voter registration databases are vulnerable to exfiltration. If they are vulnerable to exfiltration, are they also vulnerable to the manipulation of data within the voter registration database such that there could be uncertainty created about whether

someone was eligible to vote? And what's more, even though there wasn't evidence of tampering with the vote-counting machines, if those machines are WiFi compatible, if those machines are periodically updated in terms of their software by thumb drives or through WiFi accessibility, are the machines themselves potentially vulnerable next time?

Mr. Johnson. Yes and yes to both your questions.

Mr. Schiff. Thank you.

And I yield to Mr. Quigley.

Mr. Quigley. Thank you. Thanks again for your service, sir, and thanks for being here.

Help me understand: Last August, to the question that Ms. Speier had touched upon, DHS provided last August a readout of the a call you had with the National Association of Secretaries of State and other election officials, and, quote, "You were not aware of any specific or credible cybersecurity threats relating to the upcoming general election systems." At the almost exact same time, the State of Illinois Board of Elections announced that it had been hacked or some variation thereof. Was this one of the reasons for your calls? I mean, what prompted the call if you believed what you said; they are not aware of any specific or credible threats?

Mr. Johnson. Well, the state of my awareness was evolving constantly. And the statement I made on August 15th I'm sure was a very careful statement based upon what I knew at the time. What prompted the call was the general increasing threat environment that we were concerned about. And so I wanted to engage State election officials to encourage them to seek our cybersecurity help and to raise this issue of designating them critical infrastructure. I wasn't going to do that without engaging them first.

Mr. Quigley. Let me reference Vice Chairman Senator Warner's letter to

Mr. Kelly. And he references: We know that DHS and FBI confirmed two intrusions into voter registration databases in Arizona and Illinois by foreign-based hackers. There was suspicious activity aimed at the election databases of multiple other States, he references, as have others.

Could you comment on his request and what your reaction would be? He urges them to work closely with State and local elected officials to disclose publicly which States were targeted to ensure that they are fully aware of the threat and to make certain sure their cyber defenses are able to neutralize this danger. We are not made safer by keeping the scope and breadth of these attacks secret.

Mr. Johnson. I've seen that letter. I don't have it in front of me. I think that what Senator Warner requests is probably a good request. I'm not sure whether DHS itself could provide all the information, but more awareness around this to raise concern about it, I definitely endorse.

Mr. Quigley. The question is, why would you ever not want to make that public? We are briefed constantly on public sector and private sector attacks, cyber attacks. And one of the things that is generally known is, most of the time, in either sector, the entity doesn't even know it has been hacked. Is that correct?

Mr. Johnson. That is very often true, but --

Mr. Quigley. Somebody else finds out for them, correct?

Mr. Johnson. -- any time you ask somebody to maybe a public disclosure of this type, you have to balance against that, are you revealing a vulnerability that compromises --

Mr. Quigley. I think that has gotten out of the barn and is running around the farm right now, the fact that there are vulnerabilities.

Mr. Johnson. There may be others out there.

Mr. Quigley. How many states would be left, given the numbers you talked about earlier?

Mr. Johnson. Well, the number we've talked about earlier is 39, but that was based on open-source reporting. I don't know the exact number. But my -- I'm in general agreeing with what you're asking, whether there should be more public awareness and disclosure around this. And, in general, I don't have an issue with that.

Mr. Quigley. To finish the thought: Most entities don't know they've been hacked. They've been hacked a long time before they are made aware, and they are made aware by someone else.

Mr. Johnson. True, that can be true, yes.

Mr. Quigley. What's your knowledge of how long it takes before they find out that they've been hacked?

Mr. Johnson. It varies. It could be a very long time. The actor could get into the system, be latent, lie in wait, given how some of these groups function.

Mr. Quigley. So we've been informed -- I think they said something like 9,000 entities run a Federal election. The degrees of sophistication, obviously, vary widely. It just reinforces the point I think you're agreeing to here is they need additional resources. But if they don't even know that they've been hacked, how can they possibly know that they need to come to you for assistance?

Mr. Johnson. All the more reason why and I preach this now in my private life, a pre-incident examination of your cybersecurity is definitely worthwhile, because you'll very often discover that you have been hacked, and you didn't know it.

Mr. Quigley. And I know what you're thinking: This is a guy from Chicago talking to me about election reform. We have a long and colorful history there, but we sure don't want the Russians playing a role. So we appreciate --

Mr. Johnson. No, no. Cybersecurity is just one aspect of election integrity, very clearly.

Mr. Quigley. Obviously, this is the one that worked.

Anyway, my time is about up, but I thank you again for your service.

Mr. Johnson. Thank you.

Mr. Conaway. The gentleman yields back.

Mr. Crawford for 7 minutes.

Mr. Crawford. Thank you, Mr. Chairman.

And thank you, Mr. Johnson, for being here.

So you designated our voting network essentially -- "network" is not the appropriate term, but it is critical infrastructure.

Mr. Johnson. Yes.

Mr. Crawford. So there are 50 States out there and territories included that all probably have that many different versions, variations of methods, and so on of voting. So that must be very difficult to be able to synchronize that or harmonize all that and to implement comprehensive type of security strategies, cybersecurity strategies, correct?

Mr. Johnson. Well, that's not quite the nature of a critical infrastructure designation. That's not what it does. It prioritizes our assistance when they ask. It guarantees a certain level of confidentiality in their communications with us. And it gives them the protection of domestic and international cyber norms -- not any type of Federal takeover.

Mr. Crawford. Sure. No, I understand that completely, and I wouldn't want that to be the case.

To your knowledge, are there any States who have their actual voting terminals, are they online?

Mr. Johnson. There are States that have aspects of their systems online. There are States, for example, I believe that use the internet for absentee voting.

Mr. Crawford. Okay. And that could be compromised. Is that possible?

Mr. Johnson. That's -- it is a potential vulnerability, yes.

Mr. Crawford. But the actual -- when you walk in to vote, whether that be in early voting or whether it be on election day, you walk in there and either you've got a paper ballot or a screen that looks like what you see in front of me here, that's not online, would not be subject to a --

Mr. Johnson. Correct. In just about every State so far as I know, yes.

Mr. Crawford. All right. And so kind of following on to what Mr. Schiff said, then if there was an attempt made to compromise that, in other words to affect the tally of the vote count, there would have to be a human component there, correct?

Mr. Johnson. Well, there's a human component behind every cyber attack.

Mr. Crawford. I get that. But what I mean is -- I'm talking about somebody within the realm of that election and that particular State and that particular precinct or whatever to be able to affect the outcome of that particular tally from that play. Do you follow my question?

Mr. Johnson. I think I do.

Mr. Crawford. For example, if there was a malware or something placed on the computer in the county courthouse or whatever, and they took a thumb drive, inserted that into a terminal, again, you can't directly hack into this.

Mr. Johnson. Well, if your question is, is it impossible for somebody offshore to manipulate an election result, I'm not sure I would agree with you.

Mr. Crawford. Tell me why.

Mr. Johnson. Well, First of all, I -- you never know the limits of the human

ingenuity.

Mr. Crawford. Right.

Mr. Johnson. But to the extent any part of this system or the reporting of a result exists on the internet, we have to be concerned about the vulnerability of that, whether it's from an actor domestic or international.

Mr. Crawford. Okay. And I wasn't --

Mr. Johnson. And I think it was Congressman Schiff who talked about ways in which malware can be implanted, so --

Mr. Crawford. Malware, obviously, is, generally speaking, is done or effected by unwitting actors that may open up an email or may do any number of things that could then subject them to that malware.

Mr. Johnson. Well, if what you're asking me is whether it can only be the case that somebody could affect an election if they are domestic based, I'm not sure I would agree with that.

Mr. Crawford. And that's kind of gist of where I'm going here, is all the offshore stuff -- I mean, obviously, we have hackers from around the world, Russia most notably in the context of what we are talking about today, but there have been others that have played a role in trying to take active measures in elections. But my point is for them to fully affect the outcome of the election in terms of manipulating numbers, would they not need to have some sort of complicit individual physically present to effect that?

Mr. Johnson. I don't think I'm prepared to agree with that, just because cyber bad actors are extraordinarily clever, aggressive, tenacious so I don't think I could categorically agree with that.

Mr. Crawford. Without having access to this terminal through a network and only being able to update that software on this terminal through a thumb drive or some

other connection, then somebody would physically have to connect it to do that is what I'm saying. So --

Mr. Johnson. I'm not sure -- I'm not a cyber expert. I learned a lot about this topic over the last 3 years. And I think that's a conversation you should have with people who really understand these capabilities.

Mr. Crawford. Thank you.

I'm going to yield the balance of my time to Mr. Gowdy.

Mr. Gowdy. I thank my friend from Arkansas.

Director Johnson, this will probably be the last time I get to talk with you so I want to finish the same way I started which is to thank you it for your service to our country: DOJ, DOD, and DHS.

Our committee has been asked to do four things: What did the Russians do? With whom, if anyone, did they do it? What was the U.S. Government's response? And then the issue of leaks. You're a member of the Intelligence Community. You're a former Federal prosecutor. Can you speak to what a negative impact -- let me rephrase it. How important are our surveillance programs and to the extent that the felonious dissemination of classified material endangers the reauthorization of those surveillance programs, how important and critical are they to our national security?

Mr. Johnson. Based on my experience, reading intelligence every working day in the front of my working day, I would say that intelligence, our intelligence collection capabilities are vital to the ability of national security officials to do their job, to keep the American public safe.

I agree with your question in that the compromise of that type of intelligence endangers our ability to -- endangers our ability to continue this activity, compromising foreign partnerships, endangers those foreign partnerships. I cannot overstate for you

how important it is that we have good intel, access to good sources to do our jobs. Otherwise, you're flying blind.

Mr. Gowdy. Thank you, Director.

Mr. Conaway. The gentleman's time is expired.

Mr. Swalwell, 5 minutes -- 7 minutes.

Mr. Swalwell. Thank you, Chair.

May I yield to the ranking member?

Mr. Schiff. I thank the gentleman. I will be very quick, just on the point that my colleague, Mr. Gowdy, raised.

I fully concur, Mr. Secretary, these intelligence programs like 702 are critically important. There have been a number of leaks. We don't know where they've come from. Some may have come from agencies; some may have come from the President's own staff. I just want to make sure that we don't jeopardize these programs by attributing leaks to sources when we don't know what the sources of those leaks are. We would ill suit sort of the country if we do away with vital tools as a part of a political attack, rather than based on the merits of those programs and any reforms that are necessary. That's just some commentary, rather than ask you for response.

But I yield back to Mr. Swalwell.

Mr. Swalwell. Thank you, to the ranking member.

Mr. Secretary, was our democracy attacked this past election?

Mr. Johnson. Yes.

Mr. Swalwell. By who?

Mr. Johnson. The Russian Government.

Mr. Swalwell. And it sounds like, based on your experience, this attack that occurred could have easily been carried out not just by Russia but by other foreign

adversaries. Is that right?

Mr. Johnson. Yes. There are certain nation-state actors, several, that have those kinds of capabilities.

Mr. Swalwell. And it also could have been carried out by non-nation-state actors, like terrorist groups. Is that right?

Mr. Johnson. The level of sophistication that we saw last year, I'm not sure the terrorist organizations that I'm familiar with would have that level of sophistication and capability, but it is an emerging threat.

Mr. Swalwell. And certainly by cybercriminals?

Mr. Johnson. Yes.

Mr. Swalwell. And you've described that the cost of this attack is the chaos that we find ourselves here today, that we're holding hearings and, as you described, we're not working on issues like healthcare?

Mr. Johnson. The people's business, correct. I think that's one of them, yes.

Mr. Swalwell. And would you agree that the first step to solving a problem, have you heard of this quote or this idea, is to acknowledge that a problem exists?

Mr. Johnson. Sure, yes.

Mr. Swalwell. Why do you think that President Trump will not state that Russia meddled in our elections?

Mr. Johnson. You'd have to ask him, sir. I've seen various different statements from him on this topic.

Mr. Swalwell. Does that concern you?

Mr. Johnson. Well, I think that a President, a Secretary of Defense, a Secretary of Homeland Security, a Secretary of State, it depends upon the Intelligence Community. And, otherwise, if you don't, you can't effectively do your job; you're flying blind. Your

Intelligence Community are your eyes and ears to do your job.

Mr. Swalwell. Now, Mr. Secretary, you have talked about what we need to do going forward. I'm glad you brought that up because this committee, as Mr. Gowdy referenced, one of our duties is to get to the bottom of whether any U.S. persons worked with Russia, and then it is the FBI and the Department of Justice's job, if they did, to hold them accountable.

But I think we all agree that if we are back here in 2019 or 2021, after the midterm and the next Presidential election, talking about a new hack and a new meddling, we have failed the people that we represent. And you talked about in your statement that you came to the determination that election infrastructure should be designated as critical infrastructure subsector. Can you explain what this designation means legally and practically?

Mr. Johnson. Essentially three things: One, it means that when the sector seeks our cybersecurity assistance, we prioritize providing it; that's number one. Number two, it means that the certain communications that we have with critical infrastructure are confidential and protected from public disclosure so as to avoid discussion about vulnerabilities. And, number three, if you're critical infrastructure, you have the protection of the international cyber norm that says nation-states should not attack critical infrastructure of other nation-states?

Mr. Swalwell. Would you agree that conducting stress tests as we now do post 2008 with our financial institutions on voter information and voter balloting systems would be helpful?

Mr. Johnson. Yes.

Mr. Swalwell. Mr. Secretary, in addition to structural reforms to our election systems, do you also agree that just a general broader awareness would benefit the

American people as far as social media trolls, fake news, the dissemination of hacked information, and how that can affect outcomes?

Mr. Johnson. Yes.

Mr. Swalwell. Mr. Secretary, you said that, in January, you designated our election systems as critical infrastructure. And I want you to comment on a claim that candidate Trump made during the campaign season. He said, "Remember, we are competing in a rigged election," to a Wisconsin rally. "They want to try and rig the election at the polling booths where so many cities are corrupt and voter fraud is all too common." Did you find that any polling booths were rigged?

Mr. Johnson. Well, as I said, I know of no evidence that, as a result of any cyber attack, ballots were altered or reporting was altered. That comment goes to cyber attacks. I cannot comment on the integrity of every voting machine in Chicago or San Francisco or South Carolina.

Mr. Swalwell. After the election, President-elect Trump said that 3- to 5 million people cast illegal votes. In your position as Homeland Security Secretary, did you find that that occurred?

Mr. Johnson. I'm not in a position to comment on that. I heard the same claim. I'm just not in a position to comment on that.

Mr. Swalwell. And can you judge the credibility just based on your experience and interaction with James Comey? Do you find him to be a highly credible individual?

Mr. Johnson. Yes.

Mr. Swalwell. Do you find John Brennan to be a highly credible individual?

Mr. Johnson. Yes.

Mr. Swalwell. And, Mr. Secretary, can you just talk a little bit about you talked about the importance of a carrot rather than a stick with our local election systems. I

don't think any of us want to see a Federal takeover, but we don't want to find ourselves in a position like this again. What can we walk away from today and tell our local election officials that we can do to make sure that they are better prepared the next time Americans go to the polls?

Mr. Johnson. The process is vulnerable to future cyber attacks by those who are becoming increasingly aggressive, ingenious, and capable. So that's number one.

Number two, it's in everyone's interest at the local, State, and national level to ensure the cybersecurity integrity of the process, which is vulnerable and exposed in certain respects. We had the experience we had last year, and from that, we have to learn. And if we do not grapple with this, we're failing as a democracy and those of us in public office are failing the people we serve.

Mr. Swalwell. Thank you, Mr. Secretary, for your service and wish you well in the private sector.

Mr. Conaway. Ms. Stefanik, 7 minutes.

Ms. Stefanik. Thank you, Mr. Chairman.

Thank you, Mr. Secretary, for voluntarily being here today and for your service to our country. My line of questioning will focus on the January 6th Intelligence Community assessment.

According to the unclassified assessment released on January 6, quote, "DHS assesses that the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying." Can you outline what are the key factors that allowed DHS to make this assessment that we successfully protected the integrity of our vote tallying system?

Mr. Johnson. It was the result of spending a lot of time examining State by State what the practices are and were. And that assertion was based upon our best available

intel that we had at the time.

Ms. Stefanik. Can you speak a bit more about the process evaluating State By State? I assume that began after the election. How long did that take?

Mr. Johnson. After and before.

Ms. Stefanik. After and before.

Mr. Johnson. When I got into this myself in the summer of 2016, I was pleased to see that a lot of that analysis had already been done within DHS and in the interagency, so it didn't begin post-election. And one of the takeaways was that voter registration databases are vulnerable because they can be infiltrated online, but the way the tallying and voting and reporting of voting process works, it is largely offline and it is redundant in many ways, so, if one avenue fails, there's another avenue, but that some of it does exist over the internet by way of absentee ballots, absentee voting, and the like. And so that was the basis for that statement at the time.

Ms. Stefanik. Thank you.

Mr. Johnson. Based upon the absence of anything to suggest that the tallying had been compromised.

Ms. Stefanik. Thank you for that clarification.

Other than providing an assessment regarding vote tallying systems, what was DHS' role in any -- if any -- preparing the Intelligence Community assessment?

Mr. Johnson. There were a number of recommendations that we made that I believe are in a nonpublic document. And in terms of the actual intelligence assessment, I believe we had a role in what you just stated -- we had a role in making that assessment. But for the most part, what the Russians were doing, sources and methods was the role of the Intelligence Community, CIA, et cetera.

Ms. Stefanik. Was there a reason why DHS' role was so limited?

Mr. Johnson. I wouldn't characterize it as limited. Going back to October, the statement that was issued in October was a joint statement of DNI and DHS. And our people were very definitely involved in the report that was issued on January 6th, as well as some of the documentation for the actions we took on December 29th.

Ms. Stefanik. Let me ask you about the October 2016 joint statement you just referenced. The quote that was included in that statement, it says, you were, quote, not in a position to attribute scanning and probing of State election-related systems to the Russian Government.

And yet in the January --

Mr. Johnson. I wrote that sentence.

Ms. Stefanik. You did?

Mr. Johnson. Yes.

Ms. Stefanik. Well, you're the correct person to ask then because, according to the January 2017 assessment, the quote was Russian intelligence accessed elements of multiple State or local electoral boards. What new information enabled attribution of this activity?

Mr. Johnson. I couldn't say in this session.

Ms. Stefanik. We will follow up with you in closed session.

Mr. Johnson. It is a documented -- there is a documented answer to that that will be reflected in intelligence reports, I'm sure. But the statement that I made on October 7th was accurate at the time based on the state of awareness at the time.

Ms. Stefanik. We will follow up in a classified setting. Thank you very much for the answers.

I yield back.

Mr. Conaway. The gentlelady yields back.

Mr. Castro, 7 minutes.

Mr. Castro. Thank you, Chairman.

Thank you, Secretary for your testimony here today.

The American people understandably are very concerned about the integrity of our democratic processes and our voting systems. So, just so that we can frame it very clearly, let me ask you: Do you know of any law that requires even minimum basic cybersecurity protections for our voting systems?

Mr. Johnson. No.

Mr. Castro. Any State law that requires it?

Mr. Johnson. Sitting here now, I don't know the answer to that question. There may be.

Mr. Castro. And you described extensive efforts that you and the others in the government took to work with the States on protecting the integrity of their voting systems. And you noted that most States complied and came forward and worked with the Federal Government. But it's also fair to stay that some States did not come forward. Is that right?

Mr. Johnson. Correct.

Mr. Castro. For those States that did come forward and work with the government, the Federal Government, we don't know what they did with that information that we provided to them or that advice?

Mr. Johnson. Well, we do know there were a number of vulnerabilities identified and reported to the States. And I have to believe that they took steps to --

Mr. Castro. But were acting on good faith if they did.

Mr. Johnson. Well, it was in their interest to act on what we told them so --

Mr. Castro. True. But you can't say conclusively that they took the advice that

we gave them.

Mr. Johnson. I cannot say conclusively. There are problems others at the staff level at DHS who can give you more details about what we knew they did do.

Mr. Castro. Okay. Thank you.

So we've talked today a great deal about elections systems and databases that State and local governments oversee and operate, but I want to ask you about our major political parties. The declassified Intelligence Community assessment noted that Russian intelligence services conducted cyber operations associated with both major U.S. political parties. The ICA specifically discusses the systematic and relentless cyber attacks that the Russians perpetrated the DNC. But it does also note that the Russians collected on Republican affiliated targets. What's interesting is that they did not conduct a comparable disclosure or dumping of campaign material against the RNC.

Just this week, the private security firm UpGuard reported its discovery that an RNC contractor left an immense amount of voter data, in fact 1.1 terabytes, according to the report, exposed and unsecured in publicly accessible online databases. The report says the data included information on roughly 200 million Americans.

Clearly, neither political party is immune to the pitfalls of online data vulnerability or invincible to malicious hackers hunting for security lapses to exploit. So, in light of the preceding discussion about election systems as critical infrastructure, which you've advocated for, do the political parties themselves, their networks, databases, financial, and donor information, merit inclusion as well?

Mr. Johnson. Well, that's an interesting question. The danger with going down that road is you start to lose clarity about what's critical infrastructure and what's not. The definition that I wrote on January 6th very clearly was confined to election infrastructure and not political organizations, because I thought we needed that clarity so

everyone knows what is critical infrastructure and what is not.

But I'm not disagreeing with the premise of your question. I think there needs to be greater awareness around the cybersecurity of political institutions in general and political campaigns.

Mr. Castro. And let me -- the next few questions are about consultations or how accessible essentially the resources would be to political parties. So, when you were you at DHS, was there any discussion in the government about whether campaigns should receive counterintelligence briefings or briefings about the threats to our elections or cyber threats to campaigns? And is there something you would think is wise to do?

Mr. Johnson. Providing it is done so on a bipartisan, nonpartisan basis, I think that there -- I think that information sharing of the threats is a good idea.

Mr. Castro. And do political campaigns or the major political parties have the ability to work or contact DHS to obtain cybersecurity assistance or expertise? In other words, can they go forward to you all and work with you on this stuff?

Mr. Johnson. Yes.

Mr. Castro. Okay.

Do you have concerns about the security integrity of primary election voting systems or databases?

Mr. Johnson. To the same extent I would for general elections, yes.

Mr. Castro. And how should we approach the security of the primary elections as integral components or our general elections and the overall electoral process?

Mr. Johnson. I think the same vulnerabilities that exist with respect to general elections exist with respect to primary elections because, to my knowledge, States run primaries mechanically the same way they run general elections, with the same voting machines and the same reporting mechanisms.

Mr. Castro. All right. Thank you.

I yield back.

Mr. Conaway. The gentleman yields back.

Our Unanimous consent order to extend questioning to 7 minutes has expired. I ask unanimous consent that we allow each member to use 7 minutes instead of 5.

Hearing none, I recognize Mr. Hurd for 7 minutes.

[11:59 a.m.]

Mr. Hurd. Thank you, Mr. Chairman. And I would also like to associate myself with all of my colleagues that have thanked Secretary Johnson for his years of service to our country.

Mr. Secretary, I have two sets of questions I'd love to chat with you about. The first sets are what-ifs, and I ask these what-ifs under context of we are trying to figure out what could we have done differently and what should we do in the future. And I know one of the things that you were trying to do during your time as the Secretary of the Department of Homeland Security was the reorganization of the NPPD.

Mr. Johnson. Right.

Mr. Hurd. If the NPPD had been reorganized the way you had envisioned it, and let's say that had happened in early 2016, how would that have helped in dealing with this issue that we dealt with in our elections?

Mr. Johnson. Well, it's difficult to say had something been done the outcome would have been different.

I'll say two things. One, I do think that there is strong advantage to reorganizing NPPD into a leaner and meaner organization that focuses solely on cybersecurity and infrastructure protection, because the two are so interrelated.

That's something that we would need Congress to do. I know that there are a number of people in Congress who support that idea. I continue to believe it is a good idea.

When it comes to the efforts we made to engage State election systems, I was impressed with the apparatus we did have within NPPD to do so and to address all of the States that came in and sought our assistance, and that mechanism would exist whether NPPD was in its old form or its new form.

But in general, I think that we need to reorganize NPPD into a cyber and infrastructure protection agency, just simply because there ought to be an agency of the Federal Government dedicated to cybersecurity.

Mr. Hurd. Thank you, sir. And, again, the next what-if -- and I recognize the difficulty of answering what-if questions, but the goal is to try to understand how we could do things differently.

Had the electoral systems or infrastructure been identified as critical infrastructure by DHS in early 2016, how would that have impacted the situation we just went through.

Mr. Johnson. I can't say. It's something that when I first addressed this issue with my staff and they first suggested it to me, I thought this is something that we should have done a long time ago. Why isn't it? And one of the things they said to me is you could view it as already critical infrastructure, because government infrastructure is already critical infrastructure.

My view was we needed to publicly declare it to, you know, make a big deal over the fact that we're going down this road for the domestic and international audience.

Mr. Hurd. Copy.

And my next set of questions is really just in the interest of standardizing terminology and make sure that we're all singing off the same page. And our utility system, a grid, that's identified as a critical infrastructure, correct?

Mr. Johnson. Correct.

Mr. Hurd. Has DHS ever taken over a grid or a utility municipal company?

Mr. Johnson. Not to my knowledge.

Mr. Hurd. Okay.

Our telecommunication --

Mr. Johnson. I'm not sure we have the authority to do that either.

Mr. Hurd. Our telecommunications infrastructure is considered a critical infrastructure, correct?

Mr. Johnson. Correct.

Mr. Hurd. And has DHS ever taken the system over?

Mr. Johnson. No. No. Nor do we have the authority to do so.

Mr. Hurd. Good copy. Just helping to, you know, baseline what a designation of critical infrastructure actually means. And you've said that many, many times today, and I'm not going to ask you to do it again. But this is a conversation I've engaged in many times as well.

Scanning and probing, could you maybe give us a quick explanation what that is?

Mr. Johnson. You know, when I started addressing this publicly somebody said to me, well, you know, Jim Comey made a statement publicly that there was scanning and probing of voter registration systems. And I said, that's a good phrase, so let's use that phrase, because I thought it captured what we saw.

And eventually what we saw was success in infiltrating voter registration databases, which I reported publicly. But scanning and probing is basically looking into a locked box to see what's inside.

Mr. Hurd. It's a passive tool that happens millions of times across the United States every single day. Would you agree with that?

Mr. Johnson. It can, yes. I don't know if I'd describe it as passive, but, yes.

Mr. Hurd. The voter registration databases that we've talked about, isn't the information that's contained within voter registration databases publicly available information?

Mr. Johnson. Not necessarily. It may depend on each State.

Mr. Hurd. Because in Texas you can go down to the county office and get that information. And I'm curious as to why our hostile actors were -- and I definitely know that the financial systems, you know, whether it's on the Federal level that is through FEC websites, every State has this information made available. Why would you think a hostile actor like the Russians would be trying to hack systems where the information is publicly available through a portal available to the public?

Mr. Johnson. Well, I don't know that in every case in every State the information that was examined was publicly available. My concern was that if a bad actor is doing this it might be a prelude to wiping out or eliminating voter rolls or altering them in some way.

Mr. Hurd. Good copy.

Mr. Chairman, I yield back the time I do not have.

Mr. Conaway. The gentleman yields back.

Mr. Heck, 7 minutes.

Mr. Heck. Thank you, Mr. Chair. I'll begin by yielding a minute to the ranking member.

Mr. Schiff. I thank the gentleman for yielding.

Mr. Secretary, I just want to thank you, as we come towards the end of the hearing, for your testimony today and for your profound service to the country.

And I also wanted to acknowledge and thank my colleagues, Mike Conaway and Brad Wenstrup, for the aid they gave to our colleague who was injured during the shooting last week. And we're glad that they're safe and with us, and grateful to have them, and thinking about our colleague and wishing him a very speedy recovery.

I yield back.

Mr. Heck. Mr. Secretary, thanks for being here.

I want to talk to you about the future. The IC has assessed, and we regularly hear it from both former and current government officials, that the Russians will be back. They'll be back to disseminate fake news. They'll be back to hack and steal and dump this information intended to harm good people. They'll be back to find their way into the very infrastructure we trust to help us choose our elected officials, the very infrastructure we choose or trust to uphold our democracy. And I think more than anything, that puts this entire question into very vivid and stark relief, and it is namely as follows.

I'm from the school that says America is exceptional. We're going on nearly a quarter millennium of the longest running democracy in the history of our planet. But it's not just the longevity that distinguishes us. It's our rule by law. It's our free, fair, open elections conducted with integrity. And most importantly, quintessentially, it is the peaceful transfer of power.

Nobody else has ever managed this, regularly transfer power in a peaceful manner. And the winners and the losers accept the outcomes. Why? Because we are ruled by law. Because we do have free, fair, open elections. And that is what is at stake here, that which defines us. This goes to the very core of who we are.

But my question for you, sir, just to be abundantly clear, will the Russians be back?

Mr. Johnson. I think we have to assume, for all the reasons that have been discussed here, that the Russians will be back, and possibly other State actors, and possibly other bad cyber actors.

Mr. Heck. Fair to assume you were concerned, if not worried, about the '16 and '18 elections and all others going forward?

Mr. Johnson. Yes.

Mr. Heck. So you did an excellent job in the preceding 2 hours of highlighting

what you consider to be the greatest vulnerability, namely, the voter registration database. I just want to make sure that people understand that the harm here, the risk here, can be insidious, because I think when people hear that, their reaction is, oh, the addition or deletion of names.

But it's more than that, is it not, sir? Could it not, as an example, include changing the spelling wholesale of a bunch of names such that when those voters showed up at the polling places they were turned away or denied? Is that not yet one of many examples of how infiltration and manipulation of voter registration databases could reap considerable harm?

Mr. Johnson. Yes, I think that's a fair question, and I think that's a fair comment.

One thing I do want to emphasize, though, we've talked a lot about voter registration databases. When I was at DHS, I always encourage my people, don't respond to the last attack, try to anticipate the next attack. So I think it's incumbent upon all of those who manage the system to look comprehensively at where there are vulnerabilities. We focused on voter registration databases, I focused on them, because that is a known exposure that we saw.

Mr. Heck. And, Mr. Secretary, is it also true, to clarify, this doesn't have to be done wholesale, voter registration databases, this can be done in select or targeted communities or municipalities, and the undermining of confidence in our system would be, however, wholesale?

Mr. Johnson. Correct. Yes.

Mr. Heck. I don't know how many times I lost count of the references to the adage that hindsight's 20/20. I don't want to talk about looking back last year. I want to talk about how we're going to look back at some point in the future.

I've always believed it's easy to judge those who miss the obvious or the

dangerous inflection points, those who miss that Chamberlain's appeasement at Munich would lead to world war, or those who miss that passage of the Gulf of Tonkin resolution would lead to a war that, arguably, was unwinnable in Vietnam.

But the truth is there were plenty of people at those times who did know and who were raising their voices and who were ringing alarm bells. It's just that the warnings weren't heeded.

My wish, my prayer, literally, is that someday we don't look back on today and this time and deeply regret that we didn't heed the warnings, that we didn't take seriously enough a foreign power's repeated efforts to undermine our democracy and make America weaker and to so wholesale lack of confidence in our elections such that we do not accept the outcome, such that we do not peaceably and peacefully transfer power as is our Nation's heritage and is that which distinguishes us in the history of this planet, because if we do, it'll be too late.

Thank you, sir.

I yield back the balance of my time.

Mr. Conaway. The gentleman yields back.

Mr. Rooney, 7 minutes.

Mr. Rooney. Thank you, Mr. Chairman. And I would like to associate myself with what Mr. Heck just said. I think that that was very well said and very eloquent. And I think that if there's any issue that's surrounding everything that's going on in Washington right now that should unite, especially this committee and what we're doing, is what we're doing here today with Secretary Johnson, talking about the integrity of our elections.

There's one thing that we -- there's a lot of questions out there that remain unanswered, but there's one thing that I don't think is ambiguous at all, and that is, if the

American people don't have confidence in the way that their vote was cast is actually true and real, whether our guy won or next time your guy wins, and there's a question out there as to whether or not Russia may have been able to mess with the numbers, then we really do cease being the country that we are.

Secretary Johnson, I've known you a long time. I think we first met when I first got elected in '08.

Mr. Johnson. We first met when you, I think, were in the House about 5 minutes, in Patrick Murphy's office.

Mr. Rooney. Right. So I appreciate your work as the attorney at the Pentagon and then as Secretary of Defense. I think that you are a true statesman and somebody that we're all very proud of regardless of party, and it's been an honor to get to know you over the years and to work with you.

I do think that it needs to be said that -- and I've said this before in this committee -- that if anybody out there in the countryside believes that Russia is not trying to influence our electoral process, this is your notice that they are and that they will continue to do so, whether that is just merely propaganda through things like the RT or whether that's actual cyber intrusion, like changing votes or deleting votes.

We've seen no evidence, in part thanks to you, of the latter, but the former and the latter may very well be a real thing moving forward. I certainly think propaganda will continue to do so.

I know that I can speak for the rest of the committee when I also say that your -- well, I'll speak for myself in saying this. You said earlier that your designating the election systems as critical infrastructure after the election because you were worried that it might drive people away, I think you're absolutely right in that assessment. That may be arguable, but, you know, certainly, I think that that's true.

I also would say this. I hope that you work with Secretary Kelly in whatever lessons that you've learned and also sharing with him whatever the key factors were that helped you successfully protect vote tallying. I know that, you know, some staff might still be there or what have you, but for the sake of our country and for the sake of his success, as I'm sure that you are wishing upon him, that we can move forward knowing that in the next election cycle that he has every tool that he needs to be able to be successful as well.

Being that I'm the last questioner on our side, my question is going to be very specific with regard to Florida.

Ironically, today, the county supervisors of elections is holding a gathering of all Florida State associations of election supervisors. And we called some of them today from my district and asked them about, you know, your designation. And there is a states' right versus Federal intrusion issue that they are concerned about. But mostly, there's a lot of lack of or just yearning for more information of, what does that mean, what are we supposed to do, how do we tell the people of Okeechobee County and Sarasota County and Charlotte County that your local supervisor of elections is in charge of counting your votes but that this designation that DHS has put out there is somehow this security blanket that's going to make sure that Russia, a foreign entity, isn't changing your votes?

If you were talking to the Okeechobee County supervisor of elections right now, what would you tell them that the designation that you made means for them and how their job and the local votes that are cast is safe, secure, and not being mandated by some Federal bureaucrat in Washington in any other way other than protection?

Mr. Johnson. By analogy, financial services is critical infrastructure, which includes all the big banks. And I do not run those banks. The CEOs of each of them are

responsible for their own networks and their own systems. And what it means, most fundamentally, is that we prioritize helping them when they ask, if they ask. And that's what the designation means. It doesn't mean I get to regulate. I don't have the authority to regulate standards for voting booths and for reporting mechanisms.

But there are lots of other critical infrastructure sectors where everybody is responsible for running their own business, not me. It's a matter of providing assistance to them when they ask. It's simply that.

Mr. Rooney. If there is a Palm Beach County situation, where I grew up, is there some kind of a fail-safe mechanism that would come in, because that was -- the Palm Beach County butterfly ballot thing, I don't even remember the year that was, but --

Mr. Johnson. Two thousand.

Mr. Rooney. Two thousand. Now that this designation has been made, would there be some kind of an automatic trigger that would happen if a situation like that would happen where we felt like it was not because of a faulty ballot but because of actual intrusion by a foreign entity?

Mr. Johnson. Well, the Secretary of Homeland Security would not have the authority to go in over the objection of a local official and do a ballot recount. But the nature of it is that when States ask, when counties ask, we will come and provide whatever cyber assistance they ask for. Assuming we have the resources to do it and the capability, we'll do whatever we can to help them with their cybersecurity. That's it.

Mr. Rooney. Okay. I appreciate your time and your service.

And thank you, Mr. Chairman. I yield back.

Mr. Johnson. And if I could say, Congressman, since the day we first met, I have very much been impressed with your service in Congress.

Mr. Rooney. Thank you.

Did everybody get that on the record? Thank you.

Mr. Johnson. Some of the things you've pushed through as legislation, I very much appreciated them.

Mr. Conaway. He's a Congressman, not a banker. He can't loan you any money.

I wasn't going to say anything about last Wednesday, but since Adam did, I want to thank you. But we also can't leave not acknowledging Officers Griner and Bailey that morning, the Capitol Hill police officers, professionals and heroic. And I was right beside them watching them work to do what they said they would do best, and that's get between a really bad person and the rest of us.

And I can't thank them enough for what they did, heroes in the absolute best tradition of what that really means. And so we thank them for that.

And I appreciate the Nation's prayers for Steve and Matt Mika. Griner was wounded, as well, and Bailey and Zack. I appreciate that also.

With respect to today's hearing, thank you very much for doing it. We appreciate that. The cyber threat is ongoing and will get tougher and harder. We got, maybe, lucky this time that it was not successful in causing any more problems for our systems than we have.

I would hope that the National Association of State Secretaries of State would take to heart your message this morning, and then they would form a working group, a task force, to build that best practice, build that system on their own that would allow themselves then to police it and create it, because there's no one better at doing that than the folks who are actually responsible for doing it.

So I'm would hopeful, if they don't already have that in place, that there is an aggressive campaign to build that best practices and/or standards by which they would

then hold themselves to that would give all of us a lot more comfort in making it happen.

Again, Secretary Johnson, thank you very much for being here this morning.

And we're adjourned.

Mr. Johnson. Thank you.

[Whereupon, at 12:22 p.m., the task force was adjourned.]