THE WHITE HOUSE

Background Press Call on the Virtual Counter-Ransomware Initiative Meeting

OCTOBER 13, 2021•PRESS BRIEFINGS

Via Teleconference

(October 12, 2021)

12:31 P.M. EDT

MODERATOR: Thank you. And thanks, everyone, for joining. We're going to be discussing today the virtual Counter-Ransomware Initiative meetings that are being facilitated by the White House National Security Council this Wednesday and Thursday.

The call will be on background, attributable to "senior administration officials," and the contents will be embargoed until tomorrow, Wednesday, October 13th, 5:00 a.m. Eastern.

For your awareness and not for reporting, joining us is [senior administration official]. [Senior administration official] will give some brief remarks at the top, and then we're going to turn it over to your questions.

With that, I'll turn it over to [senior administration official].

SENIOR ADMINISTRATION OFFICIAL: Thank you so much. Good afternoon, everybody. Thank you for joining us today.

So, I wanted to give a brief preview of the virtual Counter-Ransomware Initiative meeting

taking place at the White House tomorrow and Thursday.

The initiative builds on President Biden's leadership to rally allies and partners to counter the shared threat of ransomware. It builds on our own domestic efforts as well — significant efforts, as you saw, on the recent Treasury designation and other efforts we have underway.

But focusing on President Biden's international efforts: In June, the President and G7 leaders agreed on the importance of the international community working together to ensure that critical infrastructure is resilient against this threat, that malicious cyberactivity is investigated and prosecuted, and that we bolster our collective cyber defenses. In addition, noting that states address the criminal activity taking place from within their borders.

At NATO, President Biden and leaders endorsed a new cyber defense policy to ensure the NATO Alliance is resilient against malicious cyberactivity perpetrated by state and non-state actors, including disruptive ransomware attacks against critical infrastructure.

And finally, as you know, we've worked with allies and partners to hold nation-states accountable for malicious cyberactivity as evidenced by, really, the broadest international support we had ever in our attributions for Russia and China's malicious cyber activities in the last few months.

So, now onto tomorrow and Thursday's meeting specifically. So, we're hosting — we're facilitating a virtual meeting. It'll be joined by ministers and senior officials from over 30 countries and the European Union to accelerate cooperation to counter ransomware.

The Counter-Ransomware Initiative will meet over two days, and participants will cover everything from efforts to improve national resilience, to experiences addressing the misuse of virtual currency to launder ransom payments, our respective efforts to disrupt and prosecute ransomware criminals, and diplomacy as a tool to counter ransomware.

The work is organized in six sessions. The first meeting is a plenary and is open to press and observers. All the subsequent discussions are restricted to invited participants to allow for frank, open dialogue.

We expect participants will speak to four areas in greater detail. And those are, as I mentioned, national resilience, countering illicit finance, disruption and other law enforcement efforts, and diplomacy.

I should note two things: While the United States is facilitating this meeting, we don't view this solely as a U.S. initiative. Indeed, we're leading internationally — bringing other countries together.

Many governments have been indispensable in organizing the meeting, and four countries in particular have volunteered to lead and organize specific thematic discussions: India for resilience, Australia for disruption, the UK for virtual currency, and Germany for diplomacy.

In addition, I want to note that we see this meeting as the first of many conversations among the international partners participating this week and beyond.

We'll have more to say on Thursday regarding takeaways from the discussions, but I want to give a brief laydown of U.S. ransomware efforts — a four-part strategy that we have here, run by the White House, to coordinate a whole-of-government effort.

First: disrupt ransomware infrastructure and actors. We're bringing the full weight of U.S. government capabilities to disrupt ransomware actors, networks, financial infrastructure, and other facilitators. Some examples that I can share publicly were, as I noted, DOJ recovering colonial ransom and Treasury's SUEX designation recently.

The second part of our strategy: bolstering resilience to withstand ransomware attacks. Even as we work to disrupt criminal ransomware networks, we also have to address our own vulnerabilities so we're not easy targets. Some examples of what the government has done: the ICS initiative focusing on control systems and TSA's recent security directives mandating cybersecurity across pipelines and other transportation networks.

You also recall [our] letter, where [we] called on the private sector to step up and do their part independently to modernize their defenses and invest to ensure the resilience of their networks

is adequate to meet the threat.

Third, we're addressing the abuse of virtual currency to launder ransom payments. We're leveraging existing and acquiring new capabilities to trace and interdict ransomware proceeds.

Finally, leveraging international cooperation to disrupt the ransomware ecosystem and address safe harbors for ransomware criminals.

And really, this event over the next two days is exhibit A of how we're working with international partners to disrupt ransomware networks, to improve partner capacity for detecting and responding to such activity within their own borders, including imposing consequences on the perpetrators, and holding accountable states that allow criminals to operate from within their jurisdictions.

So, with that, I'll take your questions.

Q Thank you for hosting this call. Can you tell us what the 30 countries are and also what you are hoping to get out of this two-day meeting by the end of Thursday? Any particular agreement or deliverable? Anything specific or concrete?

SENIOR ADMINISTRATION OFFICIAL: Absolutely. So, first, we'll be joined by ministers and representatives from the following countries: Australia, Brazil, Bulgaria, Canada, Czech Republic, Dominican Republic, Estonia, the EU, France, Germany, India, Ireland, Israel, Italy, Japan, Kenya, Lithuania, Mexico, the Netherlands, New Zealand, Nigeria, Poland, the Republic of Korea, Romania, Singapore, South Africa, Sweden, Switzerland, Ukraine, the UAE, and the UK.

And I think that list of countries highlights just how pernicious and transnational and global the ransomware threat has been in the different countries from all different parts of the world who will be participating.

And to your point regarding concrete: Absolutely, I won't preview it at this time. There's been a lot of very good preparatory discussions, particularly around the four panels I

mentioned to you. I'll be hosting the final plenary, which is when we'll summarize the discussions in the four panels and outline very key next steps. And we'll be happy to discuss that more on Thursday, following the event.

Q Hi, thanks for doing the call. One question I had was that Victoria Nuland, the senior State Department official, is in Russia this week to meet with her Russian counterparts, and I'm wondering if cybersecurity, and particularly the administration's message on cracking down on ransomware groups within Russia, is a message that she's delivered and has been received by the Russians.

And then, secondly, I wonder if you can address the elephant in the room in that Russia not being part of these talks, for a number of reasons — but how are you going to lean on U.S. allies and countries that are more in Russia's neighborhood to try to crack down on cyber criminals that may be in that region? Thanks.

SENIOR ADMINISTRATION OFFICIAL: Sure. So, yes, Toria is traveling, and cybersecurity is always one of the topics we engage with internationally. I won't go into more details regarding our discussions, as, you know, diplomacy is always best done in private.

With regard to the countries who are participating, there's a host of reasons that, you know, particular countries were invited to participate, including scheduling restrictions, availability of partners, and logistical considerations.

But most importantly, this is not our first international engagement; it won't be our last. And the countries that are participating are not our only valued partners. We look forward to future engagements and collaboration with these and other countries as we expand and accelerate cooperation on this important topic.

We will continue to lead in this area, and we will continue to lead internationally in this area.

And then, with regard to Russia: So, I think, as you know, the U.S.-Kremlin Experts Group, which is led by the White House, was established by President Biden and President Putin, so the U.S. engages directly with Russia on this — on the issue of ransomware. The President

has been very clear about marshaling the resources of all the departments and agencies to counter ransomware and address the four-part strategy I talked about.

We do look to the Russian government to address ransomware criminal activity coming from actors within Russia. I can report that we've had, in the Experts Group, frank and professional exchanges in which we've communicated those expectations. We've also shared information with Russia regarding criminal ransomware activity being conducted from its territory.

We've seen some steps by the Russian government and are looking to see follow-up actions. And broader international cooperation is an important line of effort because these are transnational criminal organizations and they leverage global infrastructure money laundering networks to carry out their attacks.

So, working with our international partners is also something we are doing in parallel to our diplomatic efforts to ensure we can disrupt the ransomware ecosystem, the actors, and the, frankly, illicit use of virtual currency that really drives this — drives the growth of ransomware.

Q Hey, thanks for doing this. One simple logistical one and then one follow-up one on (inaudible).

First of all, what's the format for the call? You know, is it Zoom? Is it Microsoft Teams? Is there a special, you know, international government tool that we've never heard of?

And then, secondly, I just want to clarify the invitation process here. You're saying Russia was not invited to be part of the U.S.'s — this initial summit because there's this other kind of channel open with Russia — do I understand that correctly?

SENIOR ADMINISTRATION OFFICIAL: So, first, I won't speak — I'm not going to speak to the logistical way we're going do it. It's a routine commercial technology that's bringing individuals together.

And as I said, a host of factors went into the planning of a virtual, international meeting of

this size to include scheduling restrictions, availability of partners, and logistical considerations. And there will be opportunities for other groups of partners to join us as well.

The headline, folks, should really be around U.S. government leading and bringing countries together to fight ransomware effectively.

And as you can imagine, with as many time zones and the complexity of bringing this many countries together, some could, some couldn't play. The important part is that we're starting on this journey, really building on the work that the President previously did in the G7 and at NATO.

Q Hi. Thank you for doing the call. So, first, just as a clarification, you said, "We've seen some steps by the Russian government. We're looking to see follow-up actions." Can you just identify what those steps were that you're referring to?

And then, secondly, we've talked about Russia, but North Korea is obviously a big player in ransomware just to support the operations of their government. And if Russia is at least nominally, you know, susceptible to various geopolitical pressure as part of the international economic system, North Korea is really, really much less susceptible — I think most people would agree. So, can you talk about how this meeting fits into your strategy for applying pressure on North Korea, which obviously has different incentives and motivations here than Russia?

SENIOR ADMINISTRATION OFFICIAL: Thanks. On the first part, I won't go into more detail on the initial steps that we've seen taken. I noted that we've had very candid and direct discussions. And in the context of those discussions, we've seen those steps by the Russian government, and we're looking to see follow-up actions.

With regard to North Korea, you're making a really excellent — and I also just, you know, would note, to the point on that, that we initially — sorry, I just — there was a key point I wanted to note to you — that, you know, ransomware focuses on our citizens and businesses, and as a result, the best insights regarding ransomware attacks often comes from private sector entities who monitor public and private networks.

So, I just want to flag, you know, a recent kind of note and tweet that a respected private sector entity — Kevin Mandia of FireEye — did, where he noted a lull from several high-profile actors and a reduction in activities in some of the most impactful ransomware groups they've responded to in the last — you know, in the last few months.

We won't speculate from here why that is, but I just did want to flag that as we're watching that closely as we continue to execute the administration's counter-ransomware strategy.

And to your question on North Korea, that is why we're putting such a focus on the four-part strategy I talked about, right? Because while we can work to try to shape actors — you know, as you've said, North Korea is famously difficult in that way — what we do control is ourselves.

So, that is why we have, A, called on the private sector to make the investments to improve cybersecurity. The President announced in his executive order that the federal government will actually start practicing what we preach in making significant improvements in our own cybersecurity. We've put a real focus on disrupting ransomware actors and networks, whether that's the work coming out of DOJ, whether that's the work of Treasury with the first-ever designation.

A huge amount of work went into that first-ever designation because virtual currency is a new area, and the very strong anti-money laundering and other rules that we have in place globally on fiat currencies are not yet in place all around the world.

So, we really are in our own way both saying we're going to enforce these and work with partners around the world on that, as well as, as I noted, you know, leverage international cooperation to disrupt the ransomware ecosystem, as in this case — right? — facilitating a meeting with 32 other countries to discuss these four areas to really coordinate our fight against ransomware.

Q Thank you so much [senior administration official]. So — sorry, did you say that Russia was indeed invited at least, but they just were not able to make it this time?

SENIOR ADMINISTRATION OFFICIAL: Russia is not participating at this time, but we have a separate channel in which we're actively discussing ransomware with Russia.

Q Hey, good afternoon. Sorry, [senior administration official], just to clarify: I understand that Russia isn't participating, but can you definitively say whether they're invited or not to participate?

SENIOR ADMINISTRATION OFFICIAL: In this first round of discussions, we did not invite the Russians to participate for a host of reasons, including various constraints. However, as I noted, we are having active discussions with the Russians. But in this particular forum, they were not invited to participate, but that doesn't preclude future opportunities for them to participate as we do further sessions like these.

Q Sure. One quick follow-up, if I may. Do you see a long-term successful strategy to combat ransomware coming out of these sessions if the Russian government doesn't participate in the future, or does it require their involvement, do you think?

SENIOR ADMINISTRATION OFFICIAL: So, two-part. One is: I am very hopeful and really excited about this international coalition work.

I can honestly say, as we started extending invitations and as we've talked to — as I've talked with my counterparts around the world; as my amazing team, who pulled this event together, has talked to their counterparts around the world, the eagerness to participate, the eagerness to learn, the eagerness to help other countries build capacity in areas like virtual currency tracing and areas like disruption to share information around law enforcement, intelligence, financial facilitators has just been huge.

Everybody has been suffering from ransomware, and I just — I'm really excited about what this will kick off. And I'm really excited about, as I noted — right? — the four countries who raised their hand and said, "We want to lead panels."

It's often that you have — you know, people have good ideas; it's less often that folks raise

their hand and say, “I really believe in this; I want to lead.”

So, truly exciting, and I look forward to sharing with you all on Thursday, you know, more details on, as Ellen asked early on, next steps.

To your point: Clearly, you know, there are — Russia plays a role because of a number of criminal actors who are, you know, operating from Russia. And that is the reason that President Biden established with his counterpart — with President Putin — a dedicated channel for us to have very focused and candid discussions. And that’s why I noted to you that we’ve had several and they continue.

And we’ve shared information regarding specific criminal actors within Russia, and Russia has taken initial steps. So, we are seeing and we will look to see follow-on in that area as well.

MODERATOR: All right. Thank you. With that, that was our last question. If we did not get to your question, please feel free to reach out to me directly, and we’ll make sure to get back to you.

As a reminder, this call was on background, attributable to “senior administration officials.” And the contents of the call are embargoed until tomorrow, Wednesday, October 13th, 5:00 a.m. Eastern.

Thanks, everyone, for your time. Bye.

12:50 P.M. EDT