SUE SCHULER: Okay, Brian.

BRIAN CIMBOLIC: Thank you, Sue. Hi, everyone. Welcome to the Registry Stakeholder Group Abuse Working Group Call. This is our last call for the year. We are not having one next week on Christmas Eve, and I just want to jump right in. You see the agenda.

So first, we had our call with the registrars which, for those of you that weren't able to make it, I think went pretty well. The real outputs from that are that we're going to work with them, potentially, on our outreach path.

We had said that we would like to talk to each constituency in advance of ICANN as the Registry Stakeholder Abuse Group, but it probably made some sense for that to be a CPH type of approach since we're essentially aligned on 95% of the issues that come up with the registrars.

And Graeme is the chair of that group and certainly the most vocal on those calls and seemed to be very receptive to that idea. I think that seems to be the plan moving forward.

Also, for those of you that missed it, there's the four work paths that the registrars had identified that Graeme sent to the CPH abuse list. And we provided some feedback and, ultimately, I think they're open to our feedback on that as well as Alan's suggestion of a separate interoperability track for registries and registrars.

The interoperability question segues nicely into our second agenda item unless anyone else had any question about the registrar/registry meeting or had anything else they would like to add of significance to that.

Not seeing anything. And Alan says, “Interoperability track makes it sounds fancy.” That’s because it is fancy. It was a very fancy and excellent idea, Alan. Way to go.

Today, we are starting our work as far as outputs. One of the things that Jim and I and the whole group has identified is that for us to show value and that we’re taking the question of DNS abuse seriously and trying to actually help create solutions for the problem is the notion that we would generate some sort of outputs.

And that may be alone in the Registry Stakeholder Abuse Group or with the registrars as well, but the first agenda item on outputs is sort of an open question. We’ll get into the I&J docs and the other documents that are listed there, but does anyone have any thoughts as far as what a RySG abuse-endorsed output looks like? Or a CPH abuse group-endorsed output looks like?

We’ll turn to the I&J documents in a moment. It could be something as simple as we think that this looks good, we think this makes sense. It could be that we modify it, tweak things for our own purposes—of course with proper accreditation—and say, “Hey, community. Here is a potentially helpful paper for notifiers out there when you’re curious about how you make a notification on DNS abuse that is likely to get the attention of the registry and registrar and get action taken. Here’s some helpful information.”

So, I didn't know if anyone had any thoughts on 1) the format of our outputs, and 2) potential dissemination to other constituencies.

Jim, I see your hand. Go ahead.

JIM GALVIN: Thanks, Brian. I'm going to stay away from form of the output for the moment, myself. I had two suggestions for actual work products that we might think about, at least in my mind, as the two things that are top of mind in terms of things we can do here.

The registrars have put together a form for suggesting how to report abuse. I think that's really a good thing to have, too, and I think that, as registries, there would be a benefit in having such a thing. And part of having that form or a standardized look at what those things are is we could also be very explicit about what the content should really look like.

In particular, I'm imagining an expanded section on what evidence really looks like and what it means. And I think that would be a useful thing to have. Now, what it means for that to be a standard and what form that should take and best practice and how it's published? Yeah, we're going to have to get to that. But that's sort of the substance. So, that's one.

The second thing is, similarly, I think that the way in which we interact with registrars … Our security framework that we have already talks about the fact that there are steps along the way and you interact with the registrars. I think having a standardized form for what we pass on to registrars and what that looks like, and then also probably a standardized from for a response that we

would expect, is a valuable thing to the extent that we can make all of that look in a very standardized way.

One of the observations I make is, it allows for integration with greater automation and less touch points. As registries, you're dealing with your own set of volume, as are registrars. But if you can standardize these interactions, then you can set things up in a way that you can deliver them and receive them and respond to them.

Those interactions can have a bit more automation in them and less touch points. And I think that speed is a good thing here to the extent that we can provide the technology to make that happen. Then the next step would be to talk about the policies that make that happen, but that can be a whole separate discussion.

Let's at least make it possible to do things more efficiently, and then get some [value] out of that. Thanks.

BRIAN CIMBOLIC: Thanks, Jim. Very well said, and all excellent points all around.

Anyone else? Any other questions on the framing of this?

It's not a question, to Jim's point, that we have to answer today. It is something that I would like us to start thinking about and, eventually, to be on to mapping things out in the future. I would love, to the extent we have some hard outputs that we can put our seal of approval on, to have regular clips. That if we have three or four or five different, specific topic output, I would love to not just dump them all at once but rather, every other month or so, putting

out documents to show our continuing value to the community, our continuing education of the community as far as dealing with DNS abuse issues.

Donna, I see your hand up. Go ahead.

DONNA AUSTIN: Thanks, Brian. Just a couple things. On the call that we had with the registrars this week—last week?—there was a little bit of discussion about the I&J documents, and I think Ashley made a good point that maybe it's best to keep documents from a reputable external source as something we can point to.

So, I think that's a valid thing that we could consider because I think it's helpful to have external documents that we can point to, so to say, "Look. It's not just us. There's other work going on in this area and they support our thinking on it."

In terms of developing documents for endorsement or support, I think whether we endorse something or whether we simply support it—we say that there are some members of the Registry Stakeholder Group that support this document—that's a process that we would go through, through the Registry Stakeholder Group. Right?

So, with the DAAR Working Group report that went to ICANN. That was developed by our internal group and it went to the full stakeholder group for a couple of iterations, and ultimately it was endorsed and sent on. And then the letter that we did to the community about abuse, that was a pretty testy conversation, I

suppose, that we had within the stakeholder group, but ultimately led to endorsement.

So, I think endorsement has a different connotation for me rather than supporting. I think there's a good product that we can develop, as Jim says, that goes to standardization. But the level of support, perhaps, or whether we endorse it as a stakeholder group, that's probably a secondary issue.

If we feel strongly about something and think an endorsement by the full stakeholder group is worthwhile, like we did with the definition on DNS abuse, then we take it to the full stakeholder group. But I don't think that should complicate any thought about documents that we think are valuable[, though,] getting our message out about abuse and what we're doing. Thanks.

BRIAN CIMBOLIC: Thanks, Donna. That's a point taken about the consideration of the working group work versus the full stakeholder group.

In the end, totally, point taken. But I would hope and expect that if our group recommends something, that we can bring it to the stakeholder group with a full endorsement of our work, not to sway what happens once it gets there.

I see Keith mentioning that he would be happy to (in the chat) coordinate the community outreach planning for our group or the CPH group. I think that would be excellent. I think that having someone be the coordinator and tip of the spear on that would be really helpful, and I think Keith is very well situated to do that.

So, Keith, I would welcome that. We can formalize something. Give the group a chance to respond. But I think that you would be excellent at that.

So, back to the topics here. Understood and point taken, Donna, on Ashley's point on I&J. I, too, think that being able to point to an expert third party in some ways—what I&J is; comprised of different stakeholders other than just Contracted Parties. [Manal] is one of the prime government members involved in the contact group. There is really pretty broad representation there.

So, for us to be able to point to a third-party expert document as informing our approach on DNS abuse, I think, would be nothing but helpful.

With that, I had sent, again, the seven I&J documents. For today, we're not going to go through all seven, but there were three in particular that I thought would be helpful.

Sue, can we start with the Guide for Notifiers document? Not that one. Sorry, I know I sent a lot. Excellent. This is great. And if you could scroll down a little bit, Sue.

This is some of the work that I find very helpful. There are three documents in particular, and the fourth I want to just preview with you guys.

There is a Guide for Notifiers. So, if you're going to make a complaint about DNS abuse, what do you need to consider?

There is a Guide for DNS Operators. So, if you were a registry or registrar that has received a complaint regarding DNS abuse, what do you need to consider?

And then finally, the Effects of Action. So, discussing what happens once an operator has taken action to suspend or otherwise act upon a domain name for DNS abuse.

So, I think that's a pretty good universe of documents to start looking at because it provides actual, practical guidance to registries and registrars. But it also provides guidance to people that want to complain about DNS abuse. And I say "complain" not in a pejorative way, but just to provide notifications regarding DNS abuse.

So, I&J has things broken down into identification, evaluation, and I believe remediation or action. So, these are questions that a notifier should ask itself prior to making a referral for DNS abuse.

And it's important to remember that not all I&J documents are laser-focused on DNS abuse. There are times that conflate website content abuse, DNS abuse. That is not the case in any of the documents we are about to discuss. They are bread-and-butter DNS abuse issues, so all of these questions should be looked at in light of potential DNS abuse questions.

So, obviously, here are the questions that a notifier should ask with regards to identifying DNS abuse.

Sue, if you could scroll down to the next page.

This, to me, I think is a bit more interesting. This is regarding evaluation of DNS abuse. So, what questions should a notifier ask in assessing the DNS abuse prior to sending a notification to a DNS actor.

And it's important to note that the I&J documents sort of apply the principle of subsidiarity in some ways, which is to say that when you identify action, that you should make the notification first to the level that has the most direct control.

And so, if there is a third-level domain, then you should talk to the site operator rather than the registrar or registry because of the collateral damage that can occur when you take action via the DNS.

You can scroll down, Sue. We don't need to walk through all the questions.

Same thing. Who do you notify when …? And, really, that's it. Each of these documents are really one-to-two-page, digestible chunks tackling topics that provide, in my opinion, pretty helpful information for notifiers in the event that they're going to send DNS abuse on to a registry or registrar.

So, that's the first of the three documents. I know I sort of whipped through it because I want to get to all three. They are also in your inbox. Are there any questions about this document?

And by the way, I bring this document to the group's attention not to say that, "Oh, yeah. We should endorse this or recommend this approach." But I think that it contains useful information that we may be able to extract and put our own name on.

But I think us educating those parties in our community that wan to provide notifications as far as what a good notification is, is in all of our best interests. Not just theirs but ours as well.

Okay. If no questions on that one, Sue, could we go to the DNS Operator's Guide on DNS Abuse?

So, this is the same sort of approach. If you could scroll down just a smidge.

So, the four categories: Identification of Abuse, Evaluation and the Scope of Abuse, Determination on the Choice of Appropriate Action, and Technical Actions to Ensure Recourse and Remediation.

This guide in particular, I find, is pretty helpful especially for those small registries or small registrars that really have no idea where to start when it comes to DNS abuse questions.

It's not quite a flow chart, but it is breaking down, at a fundamental level, what questions an operator needs to ask itself when it is confronted with plausible claims of DNS abuse.

So, if you could scroll down a little, Sue.

I'll just take a minute here. I'm not going to walk through all these questions.

If you could scroll down just a smidge more, Sue. There you go.

Take a look at these questions. I'll pause just a few seconds.

Identification and Evaluation of Abuse. Identifying it, seeing what the scope of the technical abuse is. Consideration of whether or not the domain has been compromised such that a registrant should be contacted.

Donna, I see your hand and I will get to you in just one sec.

That's something that, in our outputs and all our conversations, I don't think enough attention is paid to compromised domains with regards to DNS abuse. Yes, DNS abuse is bad, but suspended a domain name when you have a compromised domain—which is not an insignificant chunk of domains engaged in DNS abuse, particularly for legacy extensions—it's not something that should be overlooked.

Donna, with that I'll turn to you.

DONNA AUSTIN: Thanks, Brian. Just a question and excuse my ignorance.

When I&J developed these documents which, I agree, they're good documents and they're helpful for education—but what is their promotion or PR of these? Does it sit static on the website? Or how do they promote these documents?

BRIAN CIMBOLIC: It's a good question, and admittedly they're not super great at promoting them. Actually, they would like, at some point, to come and speak to this group. They have already spoken to the registrar DNS abuse group.

So, yeah, they just sort of sit static on their website. I don't think they have plans to revisit them, nor do they have any sort of big promotional blast going out. They do post it on the LinkedIn now and again.

DONNA AUSTIN: So just a follow up if I may, Brian. So, we could potentially help in that regard if we were—I don't know how to call it—a third-party promoter. I don't know, but it seems that these are really helpful documents, but if they're sitting static on a website somewhere, then a lot of the value is probably lost.

So, to the extent that we can use them rather than reinventing the wheel, then I think that's beneficial as well. Thanks.

BRIAN CIMBOLIC: Thanks, Donna. I agree. I think that we're their best possible way to amplify what they're doing. And I think the best way to do that is to really get this information, in whatever form we eventually deem appropriate, into the hands of registries and registrars.

The people that especially—and, you know, it's the old ICANN idiom we hear time and time again, the people not here. The people that aren't sitting in the DNS Abuse Working Group. Getting this information into the hands of people that …

Some of these questions may seem fundamental, but there are some parties out there that don't really even know where to start with the fundamental questions. So, I agree. It's good information that we as a stakeholder group are in a good position to amplify

and help educate our friends both in Registry Stakeholder Group and in the registrars as well.

Sue, if you could scroll down to the next page, please. That's great right there. Thank you.

So, the next questions: Choice of Action. What should a registry or registrar do? If you've confirmed phishing—you've confirmed that the domain is not compromised—what steps should be taken?

I&J has a separate paper on this. It's another one-or-two-pager that I sent around that we won't touch on today. But in the end, we all sort of know that, typically, the most appropriate step is to suspend or apply server hold on the domain rather than deletion.

And then, Recourse and Remediation. This is something that is along the lines of something that the Registrar Stakeholder Group was working for registrant rights. In the end, what happens if a registry or registrar suspended a domain or otherwise acted upon a domain and it turns out that the domain was compromised or that the registry or registrar screwed up?

So, consideration for what mechanisms does an actor have in place to take a second look, sort of reconsider the action that the registry or registrar has taken.

And if you can scroll down. I don't think there's much more on this document. Yes.

Okay. Finally, could you … Actually, not quite finally. Could you go to Effects of Action next?

Sorry. I'm seeing Donna's comment that, "[inaudible] ICANN and I&J, but GDS has the rolodex of contacts for all registries."

I think that's a great idea, Donna. As far as leveraging our relationship with ICANN to get information into the hands of registries that we might not otherwise see or work with. That's a great idea.

So, this is a document—if you could scroll down a smidge, Sue—that really is nice because we've all talked about, in DNS abuse conversations, what happens when a registry or registrar takes action on a domain? What happens when we transfer? What happens when we suspend?

And if you can just sort of slowly scroll to the bottom of the document, Sue, so people can just sense … We're not going to go graphic by graphic. But just to give you a sense as far as the visuals as far as what happens when a registry locks.

It's information that also gets to the question of collateral damage—that the entire domain name goes down. I think that these sorts of visuals, while maybe seeming basic to us—and you can have your qualms about the actual design of things—are really helpful especially when we have people yelling and screaming at us about DNS abuse when they're really talking about content. They've had no thought as to what that actually means from a technical perspective.

So, a document like this—or pulling, if not the graphics, the concept from what happens when a registry or registrar takes action—I think is really helpful to inform the conversation.

Any question on this document? There's one more document I wanted to touch on before we move on.

No? Okay. Then could you bring up the flow chart. Yeah, there we go. Thank you.

So, of all the documents, this is a really in-the-weeds, nitty gritty (in a good way) flow chart as far as what happens when a registry or registrar gets …

Actually, it's even broader than that. It's sort of cradle-to-grave from a notifier's perspective. What does it do when it has identified phishing or malware? A registrar—what happens when it receives such a complaint. And a registry—what happens when it receives a complaint if the registrar doesn't take action?

So, if you could scroll down a little, Sue.

This document, of all of the work of the I&J contact group, was … It wasn't controversial, but it had the most iterations. And the reason why is the first blue box directly below "Notifier." Actually, if you could scroll up just a smidge. Sorry. The smaller blue box. There you go.

This contemplates a notifier providing notification at the same time to the registrar and to the registry. Now it does that with the explicit acknowledgment that the registrar is the more appropriate actor to remediate DNS abuse. That because of its relationship with the registrant, it's in a much better position to identify potential compromised domains. It's certainly in a much better position to remediate a compromised domain.

The registrar should be the entity that takes action if it's determined that there is phishing, and that the domain was maliciously registered. It does, of course, reserve the right …

Now if you can scroll down until the green box is all the way on the screen. Thank you.

It contemplates that if the registrar hasn't taken action either in a set amount or time or the registrar informs the registry that it is not going to take action, then the registry conducts its own analysis pretty promptly thereafter.

So, the reason this was a little controversial is because the registrars involved didn't really think that the registries needed to be provided that notice at the outset. The problem is that all of the registrars that were contributing to this document were necessarily those that are engaged and act on DNS abuse in good faith.

Several of the registries that are involved pointed out that not all registrars really can say the same about their abuse practices. I'm sure we all know of registrars that brush off DNS abuse questions very easily, and don't have any problem just sort of ignoring abuse that gets alleged.

So, the registries sort of insisted that, "Listen. It doesn't make sense if you're going to send something to a registrar, wait 96 hours for them to do nothing, and then start the clock again in sending it to the registry."

But if you send notification to both parties at the same time, then the registry can conduct its own investigation if the registrar

doesn't take action and the registry is still satisfied that there has been abuse. Then it's in a position to immediately take action.

And that might be suspending the domain. It might actually be having a conversation with the registrar informing them, "Hey. This really looks like a compromise case. You should take a closer look at it." Or ultimately saying, "No. This isn't abuse."

With that, that's sort of this document in a nutshell. And I wanted to point out that it is specific to malware and phishing.

So, botnets. The contact group anticipates putting out a very similar flow chart for botnets that may actually involve ICANN at some level because there are some times that we registries have to get ERSR waivers. So, just keeping in mind that this is flow chart that is specific to phishing and malware.

Alan, I see your hand. Go ahead.

ALAN WOODS: Yeah. Thank you, Brian. I just want to say at this point, and it's a quick segue into the interoperability track—I couldn't remember what we called it—because I think this is one of those really, really good points that we can bring up to them and actually bring in the I&J by osmosis, almost into those registries and registrars who are those people who do have a great relationship.

And we can bring in that idea of, "Look. If we both get an escalation at the same time and nothing happens within a certain period of time, how would you like us to respond to that? Would

you mind if, after a certain amount of hours and we felt strong enough for us to intervene…?"

You know, set those expectations and those boundaries. So, that's one of the ways we can get the I&J work into our day to day as well, as I said, just by osmosis. So, I found this really helpful.

BRIAN CIMBOLIC: That's excellent. Thanks, Alan.

And I think Graeme has done an excellent job, sort of by threat of expulsion, having an atmosphere that really allows for candid conversations. And having those awkward conversations about—and just using examples—"Well, listen. Yeah. For every GoDaddy or Tucows or other registrars that are really active and engaged in dealing with abuse questions, there is a small registrar with a small team that has no interest in dealing with abuse."

And that's just a reality that we're not going to scream from the rooftops elsewhere, but with our friends in that group, we can't be working under the assumption that all registries are good and taking serious action on abuse—or that all registrars are. We need to set up systems that allow for good faith actors to pick up the slack where need.

But no. Point totally taken. This is a great kickoff to that interoperability track.

But I also think is a very good, helpful flow chart for those that are uninitiated into abuse, and especially for members of our community that would be the ones providing the notification. From

their perspective, they provide the notification and either the domain goes down, or the abuse is mitigated, or they don't hear anything, or they hear a "no."

So, showing them what questions are asked—what processes we have to work through in order to get to either remediation, fixing a compromise, or taking no action—I think is really helpful educations materials for the community.

So with that, any other questions or comments on this document tor any of the three other I&J documents or the ones that we didn't touch on?

If not, then Sue, I think we can go back to the agenda. Thank you very much, and thank you for navigating that, Sue.

I think that gives you a flavor as far as the level of detail, the potential helpfulness and education that can be provided by somehow working in the content of an I&J; of relying on a third-party expert group that is comprised of much more than just registries and registrars as far as really helping us advance conversations around DNS abuse in a thoughtful way.

So, with that, obviously I&J is just one set of potential documents that we can rely on. We don't have them on the screen, but of course there is also the Security Framework which Jim has already mentioned, which is not to be confused with the Framework to Address Abuse.

For those of you that may or may not remember, the security framework was something developed hand-in-hand by registries and the PSWG, and was so very ably chaired by Alan Woods.

Alan, kudos again. It uses the terminology “security threats” which are largely synonymous with some forms of DNS abuse.

It's something that we may want to revisit with the PSWG. It may be that there are updates to be provided there. We can explicitly use the terminology “DNS abuse” potentially, now that we’re all sort of using that same terminology.

I think that is a real low-hanging fruit and a potential to show how cooperative we are, especially if we’re the ones that come to the table and say, “We think it might be worthwhile taking another look at the Security Framework.”

Before I move on, I see Sam’s hand. Sam, go ahead.

SAM DEMETRIOU: Thanks, Brian. I put my hand up to plus one the things that you were saying, but also to respond to some of the things I've seen in chat which is this idea of using ICANN as the vehicle to get this material in front of more registries and registrars who could benefit from it.

And so, I’m actually wondering if this idea of enhancing the existing ICANN-level security framework, maybe this is a place where we can direct some of the efforts that you guys have described about incorporating material from I&J or concepts from those documents.

And if we’re maybe, as a group, willing to try to work with ICANN staff as needed, or the PSWG as needed, to have these outputs

live on the ICANN site. And I think that has the potential of getting a bigger reach like you've described.

But also adding some—I don't want to say additional legitimacy as if the Registry Stakeholder Group lacks legitimacy. But ICANN is just a more, I think, recognized organization especially for Contracted Parties who aren't super-involved in the ins and outs and the day-to-day of the ICANN community work.

Yeah, exactly, Brian. Like getting that ICANN-level street cred.

I'm glad you put it on here because I think this is something for us to consider exploring as a group, whether that can be the channel for a lot of the output documents, and whether that is something that also will resonate well with the broader community because, look, this is the ICANN effort that's going on to address DNS abuse.

BRIAN CIMBOLIC: Thank you, Sam. And Donna, too.

I think that they sort of go hand-in-hand. If ICANN's willing to do that, I think that would be great. I'm not positive they would, but I think it's certainly …

They should, for one. But I'm not positive they would, but I think it's certainly a great conversation to have. And I think would really go to show the lengths that we're going to educate our fellow registries and registrars as well as the community.

So of course, also, there's the Framework to Address Abuse. So, keeping in mind that the Framework to Address Abuse goes beyond just DNS abuse. There's the portion of that that is specific to DNS abuse that we have pulled the CPH definition from. The other stuff about certain categories of website content abuse, I don't think our group should go anywhere near because we're here to talk about DNS abuse.

But also, and this is sort of a question that we don't have to answer now. But if anyone has any additional sources that they would like for us to consider off the top of their head, please go ahead and raise your hand. But I do think that we should think about what other resources are out there beyond just I&J, Security Framework, Framework to Address Abuse.

So with that does, anyone have any other questions or comments before we move to AOB? We might get out of here a few minutes early.

I know Jim Galvin has an item, and I have an item that I wanted to tease up to. But Jim, if you are ready, willing, and able, I will hand over to you.

JIM GALVIN: Sure. Thanks, Brian. I wanted to offer to folks. I had occasion to be chatting with John Crane and Samaneh just recently. And those who are in the DAAR Working Group will remember that we were having discussions about persistence. And then, of course, there was a question that Samaneh at the time. She wanted to talk about incorporate ccTLDs into the DAAR reporting, and I've come to learn that there's actually a bit more going on there than we were aware of at the time.

In fact, ICANN has been creating the equivalent of DAAR reports for ccTLDs where they are just that ccTLD, and the DAAR report has only their data in it. And in fact, they've been moving towards putting the data available in MoSAPI so that it's just generally out there for anybody who wants it to look at for your own TLDs.

So, John in particular was asking again about interest in getting together with us to move that work along and progress that idea. They really do want to have discussions with us. They want to talk about how to make data more generally available so that registries and others can do things with it.

And of course, in addition to incorporating ccTLDs into the DAAR report and make that data available, there is still the discussion about how to bring registrars into that fold and whether or not that's possible.

There are technical limitations to bringing in the registrars, but that's a discussion that we can have, and we can talk about potential ways to deal with that once we have our larger group.

So, my point is this is really just kind of a teaser at the moment. I know there was a group of us who were doing a lot of this beforehand, but I think this is just another track of work as we get into the new year. We can look at creating a track here, see if we can get some interested parties together and move forward with this and take a hard look at this and take advantage of this opportunity and their willingness to work with us.

So, that's it. Thanks.

BRIAN CIMBOLIC: Thanks, Jim. That's great. That's really great news. John Crane's team and Samaneh have always been pretty straight shooters on this. And that's excellent. I think that would be very helpful.

So, my other piece of AOB was just to re-emphasize what Keith put in the discussion earlier. You know, we talked about different tracks as far as what we're hoping to do as a group, both as far as the long-term planning outputs and then outreach.

And Keith has tossed his hat in the ring to serve as sort of the coordinator for that community outreach. I think that Keith is extremely well-positioned to do that. Jim and I briefly chatted before this. I really appreciate the offer, and I think that Keith would be excellent to doing that.

Unless anyone has any issues with it, we should move forward accordingly. And Keith, congratulations. We dub thee coordinator for outreach. So, with that, I see you have raised your hand.

KEITH DRAZEK: Thanks, Brian. Thanks a lot for that. And, yeah, I volunteered to *help* coordinate so it doesn't have to be me alone, certainly. But I am absolutely more than willing to engage on behalf of the registry group and to coordinate with the registrars to try to help identify an action plan that this group would approve. It's not a runoff and start talking to people.

It's more about let's put a plan together that we can then start executing it against, once we have the outputs that are ready to be socialized externally. So, I'm happy to help there, and I expect it will be a team effort anyway. But happy to help coordinate that.

But I think, Brian, to your point, the outputs are probably the most important thing for us to be focusing on right now and trying to move that forward so we can start even one at a time or sort of in an ongoing way—and I think you spoke to this earlier—start demonstrating that there's action and activity taking place.

So, yeah. I'm looking forward to helping coordinate and to help contribute to that effort. So, thanks.

BRIAN CIMBOLIC: That's excellent. Thank you, Keith.

The only thing I want to add to that other than our thanks—and yes, of course it is going to be a group effort, but I think having you as the face of it certainly is a good thing for all of us (certainly better than my face)—the one thing I would say, though, is that I wouldn't want us to …

I agree that outputs are important and we should start focusing on that soon, and I can even take a crack at putting initial thoughts just for our group as far as what an initial output might look like. We can create a Google Doc that I'll share. I know so many of you love Google Docs. Like Crystal Ondo, I know does.

But we shouldn't let outputs get in the way of the outreach, is the one thing I would say. Yeah. And so, Keith, the outputs and outreach plan should be developed in parallel. I completely agree. So, we're on the same page.

My point is that we don't want to necessarily have everything ready to launch on the outputs before we start having these

conversations because there are a lot of folks that we want to talk to ahead of the next ICANN. So, we want to get that moving, too.

Keith, go ahead.

KEITH DRAZEK: Yep. Old hand. Just going to say I agree completely. So, running it in parallel. Have the action plan pulled together, approved by this group in time for the outputs.

BRIAN CIMBOLIC: That's excellent. Thank you, Keith.

KEITH DRAZEK: Okay, thanks.

BRIAN CIMBOLIC: All right. Anyone else? Any other AOB before we break for the year? Not seeing any.

Happy holidays. Happy new year, all. We've just gotten this up and running. I think we're on the right path, and I think it's going to be a good 2021 for us.

So, thank you, everyone. Looking forward to getting a lot of work done. Happy new year. Happy holidays.

[END OF TRANSCRIPTION]