SUE SCHULER: Okay, Brian.

BRIAN CIMBOLIC: Thanks, Sue. Hi, everyone. Welcome to the Registry Stakeholder Group DNS Abuse Working Group. Today we have a couple of things to talk about. The majority of which is just the updates on the separate work streams that are happening outside of our weekly meetings, but also there is interesting conversation that Jim and I had that we want to tee up for you for ICANN70 as well.

First, an outreach update. I see Keith is on the call. Actually, Keith—you just came on camera—if you don't mind, do you want to give us an update?

KEITH DRAZEK: Yeah. Thanks very much, Brian. Hi, everybody. Last week on Friday, as we had discussed last week, I sent the initial tranche of e-mails initiating the outreach effort to the NCSG, to the SSAC, and to ALAC. We included the list of questions, two or three questions, that we had posed and I have received feedback or a response from NCSG and from ALAC. I have not yet received a response from SSAC. I'll follow up with Rod probably later today or tomorrow, just to ping him. But the initial response from NCSG and ALAC was positive. We actually got some substantive response from ALAC in their e-mail back, actually, to the questions that we posed. So I think we're now on track to start having conversations with external groups over the course of the coming weeks and months.

Once we get this one scheduled, these three will move to a next round of some of the other groups.

So that's essentially the summary. Good positive feedback so far. I think we're on track to have the meetings. I'll be continuing to work with them to schedule those appropriately and to make sure that they're prepped and we're prepped, and that we're keeping this thing moving. So that's essentially the update, Brian.

BRIAN CIMBOLIC: Thanks, Keith. You inspired me to come on camera, too. So anyone else, feel free to join us. The water's fine.

The only thing I would add to that, Keith—oh hi, Alan, there you go—is that the ALAC one in particular I found interesting because, as you noted, there was quite a bit of substance in there and laid out some of the areas of disagreement. And it was very fine cordial e-mail and everything, but the reality with ALAC is that they think that there is either not enough tools for contractual compliance with regards to DNS abuse for registries and registrars or if those tools exist, Compliance is choosing not to exercise them.

So I think it's something that we should keep in mind as we go into these discussions. And that's fine. That's a perfectly valid position to take. We knew that that was going to be it but it sort of bolstered exactly what I think we should expect with those conversations.

KEITH DRAZEK: Yeah. I think that's right, Brian. I'll forward that e-mail in particular because it does contain substance to the distro so everybody has a chance to review it and understand what we're heading into. Thank you.

BRIAN CIMBOLIC: Sounds great. Thanks, Keith. The whole point is I think this all good. I think it's great that we're starting this process. Thank you again, Keith, for doing the outreach. Even if we can't squeeze them all in in advance of ICANN, I think that we've got this process started in earnest is really helpful.

KEITH DRAZEK: Yes. Agreed. Thanks, Brian.

BRIAN CIMBOLIC: Thank you, Keith. Anyone any questions on that before we move on to the other working group updates? I'm not seeing any. Okay. Next up is an update on the work with the PSWG.

A few days ago, Craig Schwartz, Jim, and I reached out to Gabe Andrews, who, as many of you know, is the FBI PSWG contact. Gabe also brought on Ryan [Lashinski] who many of you who've received DGA orders or large-scale botnet or malware orders, typically, recently they at least come in through Ryan. And just sort of bounced ideas off of each other as far as what can we do together. There seems to be some areas of real low-hanging fruit and one of which is around DGA (Domain Generation Algorithms). But that is the topic de jour and that's really more a subset of malware and botnets.

So there's a number of processes and procedures that we talked through on what registries can do to be helpful when it comes to these types of issues. Full disclosure, what the FBI is interested in—and I think PSWG more broadly—is the notion that law enforcement could at some form act as a trusted notifier on things like a DGA. So it's something that I'm certainly open to, but what we discussed was—and I'm very glad Alan is on camera for this—sort of bringing the band back together on the security framework, who many of you remembered and many of you participated in. A few years ago it was jointly drafted by the PSWG and the Registries, and it was so ably chaired by Alan Woods. It addressed what can a registry do, what is a security threat. We think that there's a lot of just agreement that when it comes to how we deal with DGAs, botnets, and malware at scale, that it's not really that controversial and it could be really helpful for both law enforcement to know how to approach a registry about a DGA or a botnet or malware that have hundreds, potentially thousands of domains affected at once. And on the flipside, educating registries, if you've never received one of these orders or these sets of domains, it's very intimidating. The first time you're like, "What the hell do I do with this? There's 1700 domains and you want them all sinkholed at 17:00 UTC on January 28." It's a bit of a thing. And so it could be a real resource for Registries and the PSWG at the same time, and I think it would be a very important step to show that cooperation from the Registries with the PSWG.

Before I take questions or solicit feedback on the notion that we would put out a new document on this in the vein of security framework, and we even just said framework to address malware and botnets at scale—it's sort of a mouthful but we can get there but that's the gist of it. The reason that this one is different from the other outreach we're doing is that, generally speaking, law enforcement doesn't go to registrars to deal with DGAs and malware and botnets at scale. They go to the registries because it can be obviously so spread out across a number of registrars that that's just not what they do. They come to the registries to create, to reserve, to do this stuff. Jim raised his hand probably to correct something that I just got wrong. Jim, go ahead.

JAMES GALVIN: I would never presume to correct you, Brian. I wanted to add something to the discussion. You said DGA a number of times. You keep saying DGA. Maxim says in the chat room, he talks about, "What if bad guys start using a dictionary instead of a DGA?" I wanted to clarify one of the other reasons why we're calling this "Framework on malware and botnets at scale" is to allow for us to have an open discussion about DGA versus large lists of names. Sometimes these kinds of mechanisms, they have a predetermined set of a large set of names that they're using. They're not generated by an algorithm but whatever the list is, it is. So that's where we got the "at scale" on the end of the title. Yeah. We keep saying DGA but we really mean conceptually lists at scale for these particular types of abuse. Thanks.

BRIAN CIMBOLIC: Thank you, Jim. That's a good clarification. I also want to make a clarification. In describing that, it sort of sounded much more like, what can we do for them? This is really an opportunity for them to be helpful with us, too. What we specifically talked about, I referred to it as referral hygiene or abuse hygiene, in that we would say like—Alan, I see your hand's up, just one sec—if there's a large number of domains that they'd say, "Reserve these names for two years," and so that would be one of the tenets that we would say, is that a good and sort of healthy relationship between LEA and registries, recognizes that we're not just going to either create and sinkhole or reserve names in perpetuity, that these things and in particularly for subsets of DGAs and recognizing that there's malware, botnets at scale, that once you pass that certain time that the algorithm would have hit then the threat has passed and it can be unreserved. So being mindful of the burden that it places on registries and so being very up front about the fact that it does create a burden on registries—administrative, logistic, whatever—so that when those come from law enforcement, we can then get on paper what is helpful to us to make it as painless administering it moving forward. Alan, go ahead.

ALAN WOODS: Thanks, Brian. Everything you're saying, I'm completely agreeing with you. I was thinking more of like the link that you're drawing with that on the security framework. To be honest, reaching back into the mind of the security framework, the DGA part of the security framework was probably the least developed. I assume that's what you're talking about. We can scoop in there and say this was something we kind of put a pin in because we didn't understand properly. I was reading the framework there. I think there's a definite springboard. It might even like grab a bit [inaudible] ICANN impetus from this and say we can actually build something out of that as well because it's well opened and to add a little bit more detail to that. So fully important because I think it’s a great idea.

BRIAN CIMBOLIC: Excellent. Thank you, Alan. Sean, go ahead.

SEAN BASERI: Great. Thanks. It sounds very interesting. I don’t know if you guys had a chance but has the issue of things like timing of actions, notification period before actions come up and also details on domains? For example, LEA might come in and say, “These are [inaudible] DGA domains provide information on—” I think you touched on this a little bit before Brian, but like threat windows of the domain and any details of what the variance of a malware, in addition to just “These are the DGA domains.”

BRIAN CIMBOLIC: Yes. The particulars of it I think it’s something that we can spell out in this proposed framework, and so that both parties are very clear as the expectations of timing of action and duration of action. We have the discretion and ability to reserve things much easier than say sometimes to properly mitigate or at least to allow for identifying victims, we would have to create the domain and sinkhole them at a minimum then once you create it. We’re talking of term of a year but being very up front as far as what the expectation is for the duration of the action.

I see in Donna’s question—I’ll be up front. Yes, we are seeing more of these come in. As Crystal alluded to and the FBI would be pretty clear, there is an ongoing DGA that recurs every November, and so there's typically a big batch that occurs in November. But we have now seen a few individual private parties identify DGAs in a security researcher type of way and get a court order requiring us to act on. This one was tens of thousands of names at once. We've also seen smaller DGAs come to us from other security researchers all within the scope of the last ten months. So I'd say we—and presumably the other big legacy type TLDs—have seen four or five of these come in in the last calendar year, in the last 365 days. And when they do come in, the numbers are typically in the thousands per instance. So it is four or five times, it doesn't sound like much except for when you're saying each of those times it can be potentially 10,000 domains at a time. Donna, go ahead.

DONNA AUSTIN: Thanks, Brian. What's the impact of these notices on the business? Are these nonsensical names or are these potentially good names for the registry? I'm just trying to understand. If you're going to take a number of names out of circulation, are they names that have value to the business? I guess that's what I'm trying to understand.

BRIAN CIMBOLIC: It's a good question. I think Jim is probably better suited to respond to it. But I will say just from experience, when you're talking about the names at scale, the ones that the instances where there's 10,000 at a time, it is gobbledygook. It's XYZ123, etc. Like, 12 characters long of just random letters and numbers. But that is not to say that no DGA couldn't use dictionary terms, and that has happened. Jim, I'm going to put you on the spot. You can probably better explain this.

JAMES GALVIN: I think what I would say, Donna, is you're asking a really good question and even Sean's comment earlier, too. These are the kinds of detailed issues that we'd really want to get into and having a discussion about this document and its output. What does it really mean to us? How do we respond?

It's also another reason why this framework would be optional. It's just proposal for how to do these things because not everyone is going to want to deal with them in the same way. There's a very real business impact sometimes in reserving names, even if it is for a law enforcement reason. So it's a valid question for a registry to ask itself, "Gee, am I in the business of doing this kind of stuff or am I not? Where are the lines in terms of what I will set aside and what I don't in terms of my policy with respect to abuse?" So, yeah, those kinds of issues can come up and we should probably speak two options in this framework. We obviously wouldn't want to say exactly what everyone should do because I think different people will do things differently. Thanks.

BRIAN CIMBOLIC: Thank you, Jim. Alan, go ahead, please.

ALAN WOODS: Thanks. My apologies, I got totally sidetracked there for a second so I missed what Sean was saying. So apologies, Sean, if you find me repeating or asking a question that's already been answered. But I'm assuming as well that the FBI will have the underlying kind of infrastructure aspects, that they will be able to identify infrastructure that creates the generated domain, turning into something that's going to be utilized in a botnet.

For the option of not reserving a domain name, is there an option that we could just be listing it for certain infrastructure, hence, from a backend provider of sorts? Because that could be a softer approach. You don't have to reserve because as soon as it goes up with that infrastructure, it just an auto system to take that down or sinkhole it straight away. There are other softer, more approaches as opposed to 10,000 domains in sinkhole or reserves. There is some technical jiggery-pokery, as we call it here, type of work.

BRIAN CIMBOLIC: That's a new favorite term of mine. Thank you, Alan. A couple of things. One, Donna asking, "Is this international LEAs that seek it, or just the FBI?" The answer is yes. So using avalanche is an example. My understanding it was either Dutch or German law enforcement that really the impetus behind figuring out the algorithm and coordinating the response. But just jurisdictional issues being what they are, FBI recognizing that Verisign, Afilias, Neustar, and PIR are all U.S. companies and that accounts for 90%+ of the DGA so, ultimately, it was the FBI that interfaced with us on those. Because of the location of the biggest gTLD registries, the FBI is typically the point organization, but certainly other LEAs are involved in the process.

The other thing I want to say is that this is a real opportunity in the sense that these referrals will happen. If we do a document, if we don't do a document, nothing is going to change as far as the frequency with which we get these requests. So this is an opportunity for us to inform what makes things better on our end that makes things, sure, it might make it easier—no, no, no, Donna. I see "Sorry about these questions." This is not an intuitive area so I totally get this. I get that it's hard to get. To the extent we're going to get these requests anyways. We're going to get these out. These DGAs are going to continue to be an issue. And I know that it's also an issue that ICANN is certainly looking at and the impact of DGAs at scale. The more that we can get out in front of it and inform the conversation, the referrals that are going to come to us anyway, we have an opportunity potentially to make them better and make the requests better suited to what we can do in a way that doesn't harm us in the end.

There's a lot of chat. I think I've lost where I jumped off from the thread. If anyone in the chat would like to jump in and say something, please do.

Kurt, I see you say, "Are there legitimate users of DGAs?" I think the answer I heard best summarizes this as academically, yes; practically, no. That there were some research, education things that, yes, in theory, there is some. But overwhelmingly it's no, they're not very useful or legitimate. "Could you gin up a legitimate DGA?" Of course, you could. It's only if the DGA is put to bad purposes like malware or botnets.

I see Jim, then Kurt, then Maxim. Jim?

JAMES GALVIN: Thanks. I actually wanted to call out a little bit of what Maxim had going on in the chat room there and maybe he'll want to say more after this. From my point of view, what we're proposing here is a framework where you have to opt in. So you have to decide for yourself if you're part of it. So the notion here is creating some guidelines for if law enforcement—and this would be any law enforcement—could opt in and we have to say something about what it means for law enforcement to opt in so that it's known, then they become a trusted notifier. In that sense, if you're opting in to the system then for registries, the same kind of thing. If you're opting in to the system in all this then it means that you are going to believe those law enforcement that are a trusted notifier to you, and you'll take that action. If you're not going to do this then it has no effect on you. Maxim was noting things in the chat room like, "Well, local law enforcement already have a lot of powers." Sure. This isn't really going to change any of that. This is just a mechanism by which you might allow other law enforcement from other areas, have a role in which they can help you in your abuse mitigation efforts. So we're just going to put some guidelines together for how that could work and then people could take that up and do it. The details of all these, it's certainly stuff to be worked out. These are important questions. They're really good questions. As you would expect, this part of putting together a policy or procedure, we had to figure out how much we want to say and the context in which it fits. Thanks.

BRIAN CIMBOLIC: Thank you, Jim. Maxim, go ahead.

MAXIM ALZOBA: Do you hear me?

BRIAN CIMBOLIC: Loud and clear. Thanks, Maxim.

MAXIM ALZOBA: Two items. First, as I understand, it was more than three or four years ago when bad guys started using an English dictionary for generation of domain names for their purposes. For example, they have name of some seashell and then some color or something. Potentially, those might be reasonable names and we will not be able to predict that and to distinguish those. Because DGAs, they obtain it two ways. First, they analyze the code. For example, some law enforcement or cybersecurity company managed to get hands on some piece of code. They decrypt it. They understand the method they used for generation or recognition of domains from which they took orders or sent information basically through those engineers.

The second way is the analysis of data. When you see what's been registered from the particular area, in particular time of day, or maybe from some specific IP addresses which were not far from IP addresses used in some other bad things. So basically, it's just the bottom. The issue is—if it's small, it's doable. Even if it's a lot and it's full of rubbish, some seems to be random generated characters, it doesn't have to follow it. But what law enforcement will ask you for is fast reaction. And nothing faster than automated acceptance of the list they pass you will not be sufficient.

Here we come to a situation where we will have to add to add to our recommendations words that if you receive something or establish channel of communication with some law enforcement and it is not against your local law. Because I see this working more or less for clusters. For example, I think that some of the Five Eyes countries like New Zealand sending PIR a request for help, most probably will be helped after your consultation with appropriate agency in your country. The same sent to us most probably will go nowhere. But the request from Moscow or Beijing, most probably will go to spam. So we will have to say that you will have to act in accordance to your applicable laws. That's what I can say. Because the only thing about international law enforcement, it's Interpol—there is no global law enforcement—and it works quite badly. Thanks.

BRIAN CIMBOLIC: Thank you, Maxim. Sean, go ahead.

SEAN BASERI: Great. I just wanted to mention a couple of quick items that came up as I listened to everyone speak. I think what Donna mentioned about a guideline, actually, I like that term as well. I think especially if we're going to include action items—and as you guys know, I worked on a lot of the DGA-related botnet takedowns on our side—there are different actions that can be taken at different times for different groups of domains some of you guys already mentioned.

I think there's also the international nature. Oftentimes what I've seen is there'll be international coordination not just because it's multiple law enforcement agencies working on it, it's because at times a botnet operator may choose to use a DGA that spans multiple TLDs to make it more difficult to after the infrastructure and that may include a ccTLD. And of course, they inherently are going to be involved with folks in the ccTLD space, the law potentially.

Then finally, what may happen at times too is DGAs may not use dictionaries. Sometimes they may use shorter strings. So instead of being 12 random, they might use 8 or smaller. There's kind of a little bit of complexity to it.

BRIAN CIMBOLIC: Thank you, Sean. Maxim, is that an old hand? Old, okay. That's all helpful context. I think Jim sort of nailed it on the head as far as bringing things back to the security framework in the sense that that was voluntary on its face, that the introductory paragraph it says, "This is a voluntary framework that helps to inform registry action on security threats." I think that's what we're talking about here. We're not talking about any sort of binding commitment on any of us. We're saying that, to Sean's point, I think it would allow for sort of an explanation as far as what can a registry do when confronted with a DGA? Technically, we can reserve the names. We can create and sinkhole. We can create and suspend. But just like we did with security framework, we list those out and say when there's a request to reserve the name, it should be time-bound and it should not to exceed the life of the potential threat. Same thing with creation and sinkholing and all that. Again, these things are going to happen. These DGAs will continue to be an issue, so the more that we can get out in front of it and inform the conversation in a constructive way and not let it get away from us, and do so in a way that's not contractually binding and is strictly a voluntary framework, I think the better off we are.

Is there anyone else that has any other questions? Correct me if I'm wrong, maybe I'm not reading them right, but I think I sort of get to the sense that the devil is always in the details but this is a good thing worth pursuing for us. As a matter of fact—yes, Craig, everyone. Okay. Yes, I think that there's the sense that this is a good idea.

Okay. So then I think our next steps would be to go back to the PSWG, let them know that that was our takeaway. Then with the security framework, Dennis Chang at ICANN served as staff liaison. Yes, I agree, Donna. Donna says it would be great if we could develop something in short order rather than drag us out in the same way the security framework dragged out. I think we can and I think we will in the sense that in the security framework we were talking past each other for like 14 months, and then something clicked. I always credit that to Jim and his explanation of what a registry and registrar actually can technically do. I think we're starting out roughly speaking the same language. Jim or Craig, you guys correct me if you think I'm wrong on this. But I think we're starting out much closer to the same page on this. I think what we could do is let the PSWG know. I think we could ask for ICANN staff support on this and that could really help facilitate setting up the meetings and having sort of that neutral party in the middle. But Alan being the alumni chair of that framework, I would love for you to help have us a primary seat at the table to help facilitate this, but we can figure those details out after this.

ALAN WOODS: If I could just jump in there.

BRIAN CIMBOLIC: Go ahead. Yeah, Alan, please.

ALAN WOODS: Just to say happy to do so. Thank you.

BRIAN CIMBOLIC: That's excellent. Thank you. There's a lot going on on the chat still. The other thing I want to say is—Donna, you said that maybe not having staff involved. This is a unique one in that ICANN probably needs to have some seat at the table because one of the primary means to address the DGA would require ICANN approval for the ability for a registry to directly create a name without having fees. So in one sense, we want ICANN there at least tangentially. And I thought Dennis did a great job as ICANN staff last time, so if we could get him, I think that would be great. Donna, I see you raise your hand. Go ahead.

DONNA AUSTIN: Thanks, Brian. I understand that there is an element here that impacts ICANN with the waivers but perhaps we can get to a point where we get everything done, and then bring ICANN when we need to. I'm very reticent given some of the efforts we have going on at the moment that are dragging up because of what I personally perceive as ICANN having a different game plan to us. So if we want to move this quickly, let's get done what we can get done and bring ICANN in when we need to on the waiver issue. But I'd be [careful] to bring them in early. It has a potential to stall us down.

BRIAN CIMBOLIC: Understood. I think there's something to be said for that, that maybe then we bake the cake a little first and present it to them only in time for the frosting rather than when we're starting with the recipe. But at some point, we will have to loop them in, but a point very well taken.

Anyone else? Any questions or thoughts before we move on? No. Okay. In that case, the next one, the output group and this is going to be a quick update for a very quick call. Thank you, those of you who joined the other day.

What we settled on as a potential good idea for outputs from our group is taking a step back there was a question, "Would we just endorse something that exist? Would we create something new? Would we have some sort of framing and then pull from both sort of a hybrid approach?" That's where we ended up. We think that it would be helpful for our group to put out one to two pagers on a number of different topics, explaining what the problem is, what the issue is that we're trying to address with each topic, each paper, and then pulling from existing resources and/or adding some of our own commentary as well.

So where we agreed to start was pulling from the security framework, which is an existing already identified ICANN document drafted by the PSWG and us on choice of action. So what can a registry do? Technically, when it comes across DNS abuse and bolster that with some of the Internet and Jurisdiction work as well. But to Donna's point, I&J has been sort of prolific in getting stuff out there. We don't want to just keep citing to I&J. There's going to be some times where I think that it's certainly going to be, if not the only resource, the primary resource. So when we can point to something else, we should. I think our plan there is to look to the security framework menu of what a registry can do and bolstering it with the I&J docs. Donna, I see your hand. Go ahead.

DONNA AUSTIN: Thanks, Brian. Well, actually, I had to drop off that call. I had Internet issues yesterday so I didn't get to the end of that call. But one of the things that strikes me as well, is that every registry has their own acceptable use for how they deal with DNS abuse. Most of that is probably on a homepage that they have associated with their website. So when we think about—Craig, it won't be you, I guess—but when we think about reorganizing our website and if we have a DNS abuse page, maybe we can capture some of that as well. And one of the things that I thought about is, if we have a members page—when I say members page, a page that identifies who the members of the Registry Stakeholder Group is, and there's the link to information about their TLDs or their organization—then that could be a way that makes it easy for people to find if they're looking for what the acceptable use policy or something is for a registry. Because I think people don't understand that registries do have their own internal policies and that guides what action they will take, generic stuff that covers most of what registries do, like the framework and the I&J stuff. But I think there's another avenue available to us as well, in that our members already do stuff in accordance with their acceptable use policy. So if we can find a way to make that readily available, if somebody's talking on their website, I think that might be helpful as well. Thanks.

BRIAN CIMBOLIC: Excellent. Thank you very much, Donna. Anyone else? Any thoughts on the form of what we sort of described? If not, then Keith pointed out that he supports the approach and discussed having Internet and Jurisdiction join one of our calls. Yes. So that is something I meant to bring up. So Liz Behsudi who's the director of the Domains and Jurisdiction track reached out. Internet and Jurisdiction is putting out toolkits, which I get the sense are going to be sort of taking on the existing work they've done with expanding in a way to make it much more operationalized. And they would like to come to our group as well as the Registrar Group and present what these toolkits are at a high level. I think it'd be great. I let her know that we're working on an outputs group that we're going to pull liberally from I&J, so I think the timing is good. I think they're aiming for mid-March for that. Hopefully, we can get a little bit of a sneak preview, and maybe one of our meetings in early March, a couple weeks before the ICANN meeting, that might be a good time for Liz or Bertrand or Ajith, but someone from Internet & Jurisdiction to come present. I will reach out to them.

There's some chatter that I haven't been able to monitor. Anyone else? A question on the output plan? By the way, that's just the first document, obviously, and it's sort of a non-controversial one, because the menu of what a registry can do, it's defined already. There's basically five technical choices and that's it. So anyone else? Anything on that before we move on? Okay. I see there's chatter again. I'm sorry, I haven't been able to quite monitor it. So please just jump in the queue with your hand if you're interested in raising any of these points.

Moving on to Section 2, this is something that Jim and I had discussed, and Sue as well, to an extent too. We sort of have a session, I think, reserved at ICANN70. And part of that was there was a thinking, should we maybe give a report on what our outreach has looked like? And my original thought to that was like, "I don't know if we want to do that because the whole point of these..." Sue says, "I have not reserved the session yet." Okay. So this might help inform that. But my original thought to that was like, "I don't know, because the whole idea is that we're supposed to have these frank conversations that are almost Chatham House Rules, if not more off the record, so then doing a readout of that doesn't quite feel right."

What Jim and I had talked about was what about having a Registry Abuse Group open house on that day? Almost like a mini public forum. Like, "Here's our Registry Abuse Group, maybe it's the CPH Abuse Group, come discuss what's on your mind about DNS abuse." Yes, there's going to be some people that are there and come to be trolls. But it's not just lip service at that point that we want to hear from people, that we can potentially even give a little presentation on what we're doing, on what DNS abuse is to us, but then open things up. Anyone can come and have a Q&A with us about DNS abuse-related questions.

What do you guys think? Sue says her deadline is tomorrow. With that, what does the group think? Jim, if you think I missed anything or mischaracterized something, please jump in.

JAMES GALVIN: I guess I wanted to ask you, Brian. I'm just trying to decide whether I prefer the way that you just described it here, or one of the things we talked about was this idea that in the same way that we're doing outreach to particular groups, we could set it up as an outreach to the community at large, "Come tell us what's on your mind." And we can frame it in the context of the three questions that we're sending to all the other groups. So it's an opportunity for anyone simply to come and say something. We're just acknowledging that we're there to take in the input and we would give it some consideration. I know that sometimes that can be awkward to not promise anything. So I'm sure that that's what's on people's mind.

I mean, I don't think that we have to decide specifically all the details of how we would have the session but the notion of having a public session is interesting to me, I think. Given Sue's deadline, we should think about, let's select it, and maybe we just have to have more discussion about exactly what we would do with it. So I hope that helps. Thanks.

BRIAN CIMBOLIC: It does. And you're right about framing things around those three questions. That gives it some framing and not be so loosey-goosey. If that's what people are coming in expecting to discuss, then maybe we can keep it on the rails a little bit more. Jim, go ahead. I see you raised your hand.

JIM PRENDERGAST: Thanks, Brian. I do like the idea as well. One thing I think you may want to consider as far as the format is concerned and how the meeting is actually conducted is to make it as casual as you possibly can. I don't think you've recorded, you're not up on a day, I think it's sitting around the table. You want to try and disarm that combative nature that sometimes the room sets up just by default. You don't want people at a queue and things like that. So I think if it's framed as, like you said, an open house or just to come have a conversation or depending on the time of day, come have a drink. It can be something like that. I think it's a good idea worth exploring.

BRIAN CIMBOLIC: I like that. An unintentional, casual approach to it I think is good. Especially this topic, it used to be GDPR, it feels like everyone was trying to dunk on each other. It feels like, right now, abuse is one in which people are trying to dunk on us, and it's not fun. I think the more that we can have this be approachable, sensible conversation, the better off we'll be. Crystal Ondo just Skyped me, saying she can't figure out how to raise her hand. Crystal, go ahead.

CRYSTAL ONDO: It's not my fault. It's Zoom on a Chromebook that Google manages, which is illegal against whatever all the company rules. So I don't have—

BRIAN CIMBOLIC: Always the tool in every carpenter, right?

CRYSTAL ONDO: Exactly. I totally agree. I think it's a good idea. I agree with Jim's comment about keeping it casual. The one thing I do want to point out is that for registrars, when registries take action on abuse—and we're talking about doing it more and more—there's no good way to communicate that to a registrar and each registry does it very differently. Is it an e-mail? Is it a poll message? Why did they do it? What's happening? So I think one thing that we should add to our specific Registry Abuse Working Group is, is there a way that we can standardize across the registries engaged, which is probably the vast majority of them at this point, how registries communicate to their registrars when they take action on a domain? Because right now registrars have no idea. All of a sudden the domain is down and how do they tell customers who come back asking? So it is something to think about that we could also tackle and would maybe want to touch on in any communication with the outside community, is that anything we do, we have to consider our own customers because obviously those actions impact people downstream.

BRIAN CIMBOLIC: Well said. Jim Galvin and Pendergrast, I think you both came off mute. Do one of you want to talk? No? Okay. You're just hanging out.

I think that's a good plan, Crystal. I'm seeing in the chat, everyone seems to think this is a good idea. And as Jim alluded to, the devil will be in the details. But we think it's generally a good idea to have some sort of open house, some discussion, open discussion on abuse.

Sue, if it's okay, I think we should go ahead and request that slot. What I don't know is it whether or not that is a Registry-only slot or a Registrar, Registry, or CPH slot. I sort of feel like the Registrars might think it odd if it was just us since we've been doing these joint meetings, so maybe that's something that Jim and I can chat with Graeme or Ashley and figure out if we want to do a CPH session. If the Registrars don't have an interest in doing this, great. It sounds like we're going to do it anyway, I think is the takeaway message. But if they want to make it a joint CPH message, does anyone have an issue with that? Or would you all prefer it to be Registries only? I don't think that would be a good look, in my opinion, by the way.

KEITH DRAZEK: Brian, just a thought. I'd like the idea of a joint session. But the abilities or the capabilities of registries and registrars are different. There is a distinction between what a registry can do and what a registrar can do. And if we're going to have a joint session, it might make sense to actually have it divided into two separate parts. But I'm just throwing this out there. Because it's sort of my reaction, as we're working on our registry-specific focus in terms of the guidelines and the two pagers that we're talking to put out, those could differ from what the registrars might come up with on their own. I'm just throwing that out there for food for thought. I'd like the idea of a joint session, but if we're going to be wanting to highlight things specific to registries and our capabilities and our engagement, there might be some value in having registries go first then registrars or vice versa. Thanks.

BRIAN CIMBOLIC: Of course. Thank you, Keith. That was a great point. And I almost wonder too, maybe it's sort of last-minute for them to make this decision. But registrars want to request their own and we can go back to back. Or we have one session, as you note, and we just split it up. That the registrars get 45 minutes, we get 45 minutes. We'll figure that out. But ultimately, I think, Sue, let's go ahead and request it. And then Jim and I will reach out to Graeme and Ashley on the registrar side and figure out what they want to do, whether or not it's they're going to request their own meeting or whether or not we should split one meeting up half and half. Because point very well taken, Keith, that the issues are even different, the issues are clearly related. But at the end of the day, too, I think we should all recognize that it's primarily the registrars' responsibility to address DNS abuse. They are ultimately their customers. But the registries, we're still stewards of our own zones. So we always have the right to take action if a registrar does not. We can reach out and take that offline, but we'll go ahead and request the slot. I think we can close out the ICANN70 one unless anyone has anything else. There's a lot of chat. Go ahead, Sue.

SUE SCHULER: This is just a real quick question. Do you think you want 60 or 90 minutes?

BRIAN CIMBOLIC: That's a good question. Can I tell you in a couple hours if we get the chance to talk with Graeme and Ashley?

SUE SCHULER: Sure. Yes.

BRIAN CIMBOLIC: Sam says she'd go 90 regardless. Let's go 90. There it is. Let's go nuts. 90 it is.

SAM DEMETRIOU: Sorry, Brian. You can always have a 90-minute time slot and only use 60 minutes of it. In this way, if you do decide to do joint, it's there, it's all set.

BRIAN CIMBOLIC: There you go. I like it. 90 it is.

SUE SCHULER: Okay.

BRIAN CIMBOLIC: Okay, that is it for today unless I'm happy to open it up if anyone has any AOB. I'm not seeing anything. I think we can end a couple of minutes early. Thanks, everyone. This was a really good one. I think we've got some good things to work on. Thank you very much, Donna.

KEITH DRAZEK: Thanks all.

BRIAN CIMBOLIC: Catch you guys later.

SUE SCHULER: Thanks, Brian. Andrea, we can end the recording.

[END OF TRANSCRIPTION]