ICANN70 | Virtual Community Forum – GNSO - CPH DNS Abuse Work Group Community Outreach
Monday, March 22, 2021 – 10:30 to 12:00 EST

JULIE BISLAND: Hello and welcome to ICANN70 CPH DNS Abuse Working Group community outreach. Please note that this session is being recorded and follows the ICANN Expected Standards of Behavior. During this session, questions or comments submitted in chat will only be read aloud if put in the proper form as noted in the chat. Questions and comments will be read aloud during the time set aside by the chair or moderator of this session. If you would like to ask your question or make your comment verbally please raise your hand. When called upon, kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly at a reasonable pace. Mute your microphone when you are done speaking.

The session includes automated real-time transcription. Please note this transcript is not official or authoritative. To view the real-time transcription, click on the more button in the Zoom toolbar and select view full transcript. With that, I will hand the floor over to Keith Drazek. You may begin, Keith.

KEITH DRAZEK: Thank you very much, Julie, and hi, everybody. Good morning, good afternoon, good evening, wherever you may be. Welcome to ICANN70 and this is a session that has been coordinated by the Contracted Party

House and, more specifically, the Contracted Party House Work Groups on DNS Abuse.

The Registries Stakeholder Group and the Registrars Stakeholder Group. Each have their own working groups focused on DNS Abuse and the group actually has regular joint sessions. And throughout the course of 2021 and the end of 2020, we have been working quite regularly and quite diligently together, as the Contracted Party House, to try to be a little bit more organized and to really engage with other parts of the community to do some outreach and do some engagement to establish some important dialog.

We really view this session as a continuation of that effort to engage the community, to inform other parts of the community of what the Contracted Party House is doing, and to really make sure that we have an ongoing dialog on the topic and that's really the purpose of this session today. We really do want to make sure that this is an opportunity for engagement and for joint communication. If we could move to the next slide.

I am your moderator for today. I'm going to give an overview of our approach. We actually have relatively few slides, which I think is good. It'll give us an opportunity to provide some introductory remarks and an overview of what the Contracted Party House DNS Abuse Working Groups are doing and then really get into a conversation around some specific questions.

I'm in the process of giving a welcome and introduction, and I'll shortly get to an introduction of the Contracted Party House's definition of DNS Abuse. Then I will hand it off to Jim Galvin and Brian Cimbolic for a specific introduction on the Registries Stakeholder Group's DNS Abuse Working Group, then we'll hand it off to Reg Levy for an update on the Registrars Stakeholder Group's DNS Abuse Working Group.

Then, we will turn to a moderated session focused on questions. These are three specific questions that the Contracted Party House has developed to try to initiate and to encourage dialog and we'll get to those questions in a moment. And we're in a Zoom room today so we're not in a webinar format. So for those who want to ask questions and to engage in the dialog when we get to that, do feel free to put your questions into chat with the appropriate formatting and/or put up your hand and I will be calling on the folks who are interested in engaging. With that, next slide, please.

Just to tee things up and to frame the discussion today, the Contracted Party House definition of DNS Abuse is that DNS Abuse is composed of five broad categories of harmful activity insofar as they intersect with the DNS. That includes malware, botnets, phishing, farming, and spam, when spam serves as a delivery mechanism for the other forms of DNS Abuse listed above. You can find further details on both the Registrars Stakeholder Group website and the Registries Stakeholder Group website. But this is essentially the definition that Contracted Parties are using when we talk about DNS Abuse.

And I think it's clear that this is primarily focused on infrastructure abuse. And we certainly, as Contracted Parties recognize that there are other types of Internet abuse—abuse of the Internet on the Internet. Much of that is focused in the realm of content and website content. but from a Contracted Party perspective, the term DNS Abuse really does and should apply to the technical infrastructure and the abuse of the technical infrastructure that's captured in these categories that we've identified. Malware, botnets, phishing, farming, and spam, when spam is a delivery mechanism for those other types of abuse.

With that, I'm going to hand it off now to Jim Galvin and Brian Cimbolic for an introduction of the Registries Stakeholder Group engagement, and then we'll hand it off to Reg Levy for an update on the Registrars Stakeholder Group. Then we'll circle back to discussion and Q&A. So Jim if I could hand it over to you and Brian at this point. Thank you.

JIM GALVIN: Thanks, Keith. I'm Jim Galvin from Donuts. I will talk first with respect to the Registries Stakeholder Group, and if you could skip to the next slide, please. The Registries Stakeholder Group has a DNS Abuse Working Group co-chaired by myself and Brian. I want to first point out some things that we do have that are actively going on and I'll talk about the first couple of things here.

So the Registry DNS Abuse Working Group that we have actually started out as a DAAR Working Group that we started more than a year ago—almost two years ago now. And when OCTO first announced DAAR, we

reached out to them and joined to them to talk with them about making sure that DAAR would really inform the community and would be helpful to the community in representing what was really going on with respect to DNS Abuse.

So we've actually had a lot of success with them. I do want to give a shoutout and acknowledge them for being very collaborative and working with us. John Crain and Samaneh Tajali. We actually have some ongoing work with them. So the DAAR Working Group morphed into a much broader and bigger scope and now we have this DNS Abuse Working Group that we're doing.

One of the things we're still working on with OCTO is this concept of a TTL on listed domains. And what that means is how long is a domain alleged to have abuse?

What's important about that number is if you had something like that, then you'd be able to see that registries, and in the future probably registrars and DAAR, would actually be able to see the fact that we're taking action. DAAR presents some absolute numbers and percentages but a missing characteristic there is the 10 domains that it highlights one month are not necessarily the 10 same domains the next month. So being able to distinguish that and call out the fact that activity is going on is important. That's additional work item that's going on there

And as Keith said, this session is really an outreach session for us. We have already started, and working jointly with our Registrar colleagues, created an outreach program, we're calling it. We are reaching out to all

of the SOs and ACs and in this session here we're just opening that to the community at large, where we're asking them the same questions that you're going to see later and we're talking to them. We want to hear from them about their pain points and what they do with respect to DNS Abuse.

We've already met with NCSG and ALAC so we had a first meeting with them and that was very productive and helpful. We have a BC meeting scheduled and we're still pending some scheduled meetings with IPC, SSAC, and ccNSO. But we're hopeful that these will be ongoing interactions, just as this session might be. Depending on how this goes today and what comes out of it, maybe there'll be an opportunity for doing this again. But we certainly want to continue to meet with each of the organized groups in ICANN so thanks for that. If you don't get a chance to speak today, please do go back to your individual groups and make sure that you're part of the ongoing sessions that we have together.

With that, let me turn it over to my co-chair Brian to pick up the remaining two items.

BRIAN CIMBOLIC: Thank you very much, Jim. Hi everyone, I'm Brian Cimbolic with Public Interest Registry. Thank you very much for being here. As Jim and Keith have mentioned, outreach is one of our key initiatives in both groups, the Registries, and Registrars.

Another work track in the Registries is the outputs—not outreach, but outputs. And so we've begun an output series that's really meant to inform two audiences. One is recommended practices and options for registry operators when it comes to dealing with DNS Abuse but, two, the broader community—so a broader understanding of the capabilities, what a registry can and cannot do.

And to that end, we've put out our first output document which is called Registry Operator Available Actions. That's available on the Registries Stakeholder site and it details what are the technical capabilities of a registry operator once it's identified DNS Abuse—explaining the differences between potentially applying server hold to suspend the domain, transferring the domain, locking the domain, etc.

Again, this is just the first of what we anticipate to be a series of outputs to help inform community dialog around DNS Abuse. And as part of that, we're also currently working on a potential output document with the GAC Public Safety Working Group. So this builds on some of the work that the Registries Stakeholder Group and the PSWG did several years ago when we jointly drafted and put out the framework for registry operators to respond to security threats.

This new framework targets botnets and malware at scale. Really, we're thinking of things like domain generating and algorithms which, as our friends in the PSWG have noted previously, these are low-frequency high-impact incidents, where you might have a single domain generating algorithm that generates hundreds of thousands of domain names at once—so really helping to educate both registries on the

mitigation side, as far as recommended practices to address those DGAs and malware botnets, and also on the law enforcement side. What goes into a potential order or potential request from the law enforcement side to the registry that makes it the most easily implementable, the results most easily achievable on both sides?

It's an area—one of many areas—where there's certainly joint interest in making that process run smoother on both sides and we're excited to really get to work in earnest on that. With that, that's it for this slide. We can hand things over to Reg on the Registrars Stakeholder side.

REG LEVY: Thanks, Brian. May I have the next slide, please? Thanks. So the Registrars Stakeholder Group has also been meeting, along with the Registries Stakeholder Group sections on DNS Abuse, with stakeholders to get their input on what their pain points are. I'm not going to repeat what Jim and Brian just went over.

Some of the white papers that we have published so far are linked here and I believe these slides will be available later. We have a guide to reporting abuse to a registrar. This includes all of the information that we consider to be necessary in order to appropriately investigate an allegation of DNS Abuse. Often registrars will just get a domain name and so this gives more information to potential reporters about what it is that they should be providing to us so that we can appropriately investigate.

We also have a report on some of the work that we did during the early part of quarantine, since we are definitely still in it. Hopefully, there is an end on the horizon, though. A bunch of us put some effort into doing manual reviews of domain names that had COVID or corona in the domain name itself and whether or not the domains were being used abusively or not, so the report discusses that. Basically what we've found matches what others will indicate is the case that the domain name itself often bears little resemblance to any abuse that might be present on it. The worst abusers of the COVID-19 crisis did not use any domain name that had a keyword and there was a lot of good being done.

We also have a minimum required information for WHOIS data request sheet, it's a list of seven questions that if you submit to a registrar, they can use that to evaluate whether or not previously private WHOIS information can be disclosed to you.

Those are the three published works so far that you can go read. We've got white papers in progress on possible incentivization programs to take it out of the bad actors getting punished and put it into the good actors getting accolades area. We also have a white paper on registrant protection because at the end of the day most of our contracts indicate that it is the registrant that we need to be protecting. That, that is why we're here. So look for that in the future.

Finally, I always forget what BEC stands for. Luke, I'm sure, my co-chair, can correct me certainly in the chat or by him meeting me and reminding me. We've got a white paper on BEC scams coming up. We

also are considering putting dev work into a centralized resource, where you can put a domain name in and it will spit out information about who you can contact with concerns about the domain name. And that's going to include the registrant themselves, a hosting company if relevant, the registrar, the registry, and ICANN. So those are our main points and I will hand it back to Keith for the next section of this event.

KEITH DRAZEK: Okay. Thank you very much Reg. And thanks to Jim and Brian for an introduction on the Registry side of things and Reg and Luke, her co-chair, on the Registrar-side of things. If we could move to the next slide, please, and this gets us into our engagement and our dialog. So we've included … Again, that's the definition of DNS Abuse as I cited and went through earlier, just for reference.

But the three questions that we, as part of our outreach over the last several months with various parts of the community … And as Jim noted these are ongoing conversations. We've met with several groups already, we have other meetings scheduled in the coming weeks. We're still working on and establishing and finalizing the scheduling for some additional meetings with various groups but everybody's invited to engage with us directly as the Contracted Party House in these conversations.

But I just want to tee up the three questions that we've posed. And the first is, what information do you, as community members, use and how do you use it to assess DNS Abuse levels? The second question is what

are your concerns regarding DNS Abuse—specifically, anything that you'd like to focus on in terms of the conversation about raising awareness among the Contracted Parties, about your concerns regarding DNA Abuse under the definition above. Then specifically, are you seeing practices from registrars or registries that you'd find helpful, that we should be understanding better, taking on board?

And one of the things that we're looking at as Contracted Parties is the development of best practices and recommendations that we, as very active members of the ICANN community, and those who contribute regularly to the policymaking process and making sure that we're compliant with our contracts—that we can provide best practice guidance to other registries and registrars who might not be as directly involved in the ICANN policy development processes, etc. So if you, as community members, are seeing practices from registrars or registries that you do find helpful we'd like to hear that as well.

Those are the three questions that we've posed—thought-provoking, thought exercise-type questions. But don't feel limited to these questions. If there is engagement that you'd like to have with us, we have a bit of time today to actually have this dialog. And, again, this is just the beginning and we look forward to carrying on these conversations for the weeks, months, and time to come. So with that, let me pause and ask if anybody would like to get in queue at this point. If there's any community engagement, any input questions for the Contracted Party House, now's a great time.

Any hands? All right, I see a hand from Jonathan Zuck—Jonathan with ALAC. Go right ahead, Jonathan.

JONATHAN ZUCK: Thanks, Keith. Jonathan Zuck from the ALAC. We had the chance of having one of those face-to-face meetings with you so thanks a lot—or to the extent we have face-to-face meetings anymore. But so thanks a lot for that meeting. And we had a couple of conversations about sources of information during that meeting, which was your first question here.

And we pointed you—not to put you on the spot so feel free to just say no. But I don't know whether you've had a chance to look at the—and collectively I mean you all, y'all—have had the chance to look at the FTC data about COVID-related complaints that came in via emails, and websites, etc., and whether or not you found that data useful or interesting as a data source for what was happening, just overall this past year and also during the COVID crisis. Thanks.

KEITH DRAZEK: Thank you, Jonathan. Just coming off mute. Yeah, thanks for that, and thanks for your engagement. You, and Joanna, and others, as the ALAC, engaged with us several weeks ago now, so thanks for that follow-up. I'm going to hand that one off to Jim Galvin first. And if Brian would like to add anything to that feel free. But, Jim, let me hand that question over to you. Thanks.

JIM GALVIN: Thanks Keith. And thanks, Jonathan, for the question, and thank you for the pointer during our outreach session. I certainly do appreciate contributions made by others to what we're doing here.

I think the most important takeaway for me, with respect to the FTC report, is that it does show quite handily that abuse on the internet at large is increasing and is an issue. It's fair to say that the number of victims is increasing, the amount of loss is increasing, the amount of methods of abuse is increasing. But I think you have to compare that to what DAAR shows. DAAR is actually reflective of the individual abuse with respect to domain names specifically. So it's looking at and characterizing the abuse that registries and registrars address directly.

So while we agree certainly there's obviously an abuse problem on the internet in general, it's just important to keep in mind that that report reflects a broad range of kinds of abuse. It's much more than just the abuse that registries and registrars generally look at. As David Conrad, on behalf of ICANN, on behalf of OCTO, and the DAAR report has shown many times, DNS Abuse as defined here is actually on the decline and going down. It's on a steady decline.

So to me, that means that there's opportunity potentially for some changes and some additions but we have to have that discussion. We have to consider what else could we be doing that might have an impact on this broader sense of abuse? We don't have an answer for

you yet but that's something that we can have a continuing dialog about. Thanks.

KEITH DRAZEK: Okay. Thanks very much Jim. Brian, did you want to follow up?

BRIAN CIMBOLIC: Yeah, I do. First, thank you, Jonathan, for sending that over. It's a very interesting report and it does go to show that the problems. It's pretty clear what's outlined in that report.

But just a couple initial thoughts. One, as Jim alluded to, it highlights the difficult position registry operators or registrars, because of the varied nature of the complaints that are covered there … So that report included in some of its most frequent instances of fraud, things like identity theft, online shopping, and negative reviews. And those are really necessarily always very fact-intensive things that require investigation that, unlike something like True Blue DNS Abuse, a registry operator or registrar can identify, rely on blocklists, things like that, and ultimately take action.

It's not so apparent when you're looking at some of the things covered in the FTC report. Especially, that report actually showed that overwhelmingly, the preferred method of contact was phone call and text, as related to the instances that were reported. And only 11% actually related to websites in general.

All this is to say … That's not to minimize the harm or the impact of that potential fraud, but just the very factual, specific analysis that's required for that subset of the report that actually did relate to websites or domain names. It's a good indicator for something like a trusted notifier program, where relying on expert third parties like an FTC, or a number of registries participated in a similar program with the US Food and Drug Administration to identify opioids. Because DNS operators are not in the best position to be able to be arbiters of facts in those scenarios, those relationships can be really helpful for the types of harm that are covered by the FTC report.

KEITH DRAZEK: Okay. Thanks very much, Brian. And I've got a queue building but I just wanted to flag that I think what's been highlighted here already is that there's an important distinction to be made between … As we look at definitions and we look at abusive behavior on the internet, it's a question of roles and responsibilities and a question of what is appropriately within the remit of various parties to mitigate abuse.

As noted, and again on the slide before us the definition that the Contracted Parties are looking at is limited to DNS technical abuse—DNS Abuse in terms of the technical infrastructure and the capabilities that we would have as registries and registrars. Proportionality is an important concept and there's a number of different things we could talk about here. But there are other actors in the ICANN stack who have far better capabilities to deal with certain types of abuse, particularly that that would be considered content related or website abuse, that

would be a different role or responsibility than registries and registrars as it relates to the DNS infrastructure.

Happy to talk about that further but let me get to the queue, and if anybody else would like to get in queue please do so. I've got Mason and then Fabricio. Mason.

MASON COLE: Thank you very much, Keith. This is Mason. Can you hear me?

KEITH DRAZEK: Sure can. Go right ahead, Mason. Thanks.

MASON COLE: Thank you. Good morning everybody. Mason Cole here, chair of the Business Constituency. First, I just want to say, on behalf of the BC, that we're thankful for and are happy to see what Contracted Parties are doing in terms of outreach. The BC is looking forward to its first meeting with the Contracted Parties small group. So thank you very much for doing that, we look forward to the discussion.

However, I need to ask the other guy's question, which you probably saw coming, which is in terms of the parties that don't sign on to what you're doing in terms of proactivity on DNS Abuse, what can we do about those parties that aren't taking DNS Abuse seriously or not doing their part to address it? And what can we do as a community to help address that?

KEITH DRAZEK: Okay. Thanks very much, Mason. I'd like to see if anybody would like to respond to that. Jim maybe I'll hand this one over to you to start with and if others would like to jump in please do.

JIM GALVIN: Yes. Thanks, Keith. Thanks, Mason for the question. I think I don't have an answer for you for the question. I think that that's part of the reason why we're here in general. Part of the role and purpose of our outreach is, in fact, to begin to open that question and ask of the community what can we do collaboratively to do more, to better address different kinds of abuse and the ways in which it appears?

One of the things that I do want to call out though, that part of the conversation has to recognize the fact that even though we might focus on who we might consider to be problematic players in the community in which we live, it's important to keep in mind a couple of things. One of those is that this community that we can focus on is just the gTLD community, because we have essentially an enforcement mechanism readily available to us. And so we get to ask the question is there something we can do differently within the context of that enforcement mechanism, which is ICANN compliance? We get to examine whether or not there's opportunities there.

But what's important to me, when I think about this problem of what do we do about abuse, is there are so many other players. Even within Registries and Registrars, there are other players. ccTLDs, and the

registrars that go with them. There's obviously some problems on that side. And we can't impact that, just as we can't impact the broader kinds of abuse that exist on the internet. So it's very easy to say, "What do we do about potentially problematic players in our immediate space?" Truthfully they're not the most significant problem in the Internet abuse space. So it's important to keep that balance in mind.

But we're certainly open to having that discussion with you. No obvious answer. It's just that it's a larger problem space than just the question that you're asking would seem to imply. Thanks.

KEITH DRAZEK: Okay. Thanks very much, Jim. And I think Reg would like to respond on behalf of the Registrars. And then I would like, at that point, to circle back to some of the questions that have been posed in chat and I know we have Fabricio also in queue. So, Reg, over to you.

REG LEVY: Thanks, Keith, and thank you, Mason, for that question. The DNS Abuse definition that we've got up here comes directly out of our contracts so we firmly believe that this is something that ICANN Contractual Compliance can help enforce. If there are domain name registrars that aren't appropriately acting on these particular types of DNS Abuse, then absolutely we should take them to ICANN Compliance and work with them to help them enforce the contracts.

KEITH DRAZEK: Okay. Thanks very much, Reg. Fabricio, if you give me just one second, I want to capture the ongoing questions. First I'd like to note that Liz Behsudi has noted that there are additional tools focused on addressing abuse at the DNS level captured in the Internet Jurisdiction Project toolkit that was released recently. And I did want to acknowledge Liz and the excellent work of the Internet Jurisdiction Project in augmenting and contributing to the ongoing discussions and certainly input to the Contracted Parties' considerations. Liz, thanks for that flag.

I've got a question submitted from Steinar Grotterod, "Great news that the CPH has managed to agree on a definition of DNS Abuse. Good work." And the question is, "How can we identify 'spam as a delivery mechanism for other forms of DNS Abuse,' compared to other categories of spam?" If I could ask our Contracted Party colleagues to take that on board for a response after we get to Fabricio.

Then I've got another question submitted by Chris Lewis-Evans from the Public Safety Working Group, the GAC. Question, "Once the work within the Work Groups is carried out and you come to conclusions to improve tackling DNS Abuse, how do you get this applied across all the CPH?" End question. Great question. Thank you. There's some additional commentary here. But, Fabricio, if I could turn to you and then maybe we'll come back to a response to the written questions. Fab?

FABRICIO VAYRA: Sure. Thanks, Keith, can you hear me?

KEITH DRAZEK: Yeah, sure can. Go ahead.

FABRICIO VAYRA: Wonderful. Thanks. Thanks for having the session. Just one quick comment to the prior conversation. James had some really good notes, just talking about the extent of the problem and the players. But you'll see in the chat, I think maybe some place to start or a suggestion on that is Compliance and ICANN itself, for at least three or four ICANN meetings before this, constantly talked about this known up to eight actors that are bad, where a lot of DNS Abuse aggregates. I don't think it's anyone on this call. But that might be a really good place for ICANN to start focus. I mean, if they've gone on the record and said, "We know that there are 8 to 10 bad actors out there," maybe that's where they should start as part of their compliance.

My question is this. As much as I appreciate the framework … I've read it. I've gone through it. I've referenced it when reaching out to parties. Some parties act. But what do we do—back to Mason's point about what do we do about the people who don't sign onto this? My question's more what do we do with people who are signing onto this? They're showing up at these ICANN meetings. They're touting that this framework is there. But then when you reach out to them and say, "Hey, here's an example of financial fraud phishing that squarely fits under the definition that you've agreed to under the framework. Can you

please take this domain name down?" You just get a runaround or no response.

Who do we report that to? Because if we go to ICANN Compliance, what we're going to get is, "Submit a ticket." And that just goes into the ether. You go to the party who's repping at ICANN that they're going to take action and they're not taking action. What do we do? Who do we report that to? Are the signatories to the framework interested in knowing who amongst them isn't acting, despite the lip service they pay at ICANN?

KEITH DRAZEK: Thanks, Fabricio. That's a great question and I will see if anybody would like to weigh in. As you noted, I think the first step, if there is a Contracted Party of either group--Registries or Registrars—not living up to the expectations or obligations, then ICANN Compliance is certainly the first step. If what I'm hearing you say is that submissions to ICANN Compliance are, I think as you said, "going into the ether," that raises another question in my mind as to responsiveness and follow-through and are the submissions actionable? But I think these are really important questions that you're raising. I will turn to colleagues, if they'd like to provide some response or feedback on this one. Anybody want to weigh in?

BRIAN CIMBOLIC: I can jump in.

KEITH DRAZEK: Yeah, Brian. Go ahead. Thanks.

BRAIN CIMBOLIC: Thanks. And, Fab, thanks very much for the question. I just want to make sure we're talking about two separate buckets and not to conflate the two, although that's not to say that both concerns aren't valid. So there's the Framework to Address Abuse, which is a document, as some of you may or may not know, with more than 50 signatories from gTLD registries, ccTLD registries, and registrars, that deals with two categories—DNS Abuse, which uses this same definition, as well as categories of website content abuse.

And the important distinction, it says, is that registries and registrars that sign onto that framework must take action when they've identified DNS Abuse. And then for those categories of website content abuse, there are instances where the level of harm is such that they should take action. It is a voluntary document but it's … Absolutely, the intent was if you sign your name onto that document that you live by those expectations that are set forth therein. So I have no problem, if there is someone that is not living up to the framework … It's not a formal body. It's a voluntary framework. But making that known, absolutely. But that document is separate from the contractual obligations on registries and registrars.

So if someone doesn't live by the letter of the framework that's not a 1:1 the same thing as someone not living up to the obligations of their contract. They can be. If you're failing to mitigate DNS Abuse, then sure.

Then you might be in that bucket where both instances, you'd be violating the terms of the framework as well as your contract. But just wanted to make sure that those are two separate tracks that we should keep in mind. Yeah, and so with that, if anyone else has anything to add there.

KEITH DRAZEK: Great. Thanks very much, Brian. I'm going to turn to Brian King next and then we'll get back to the queue.

BRIAN KING: Yeah, thanks, Keith. Just to add onto that point that was well said by Brian Cimbolic. Just to, I think, cut through a lot of the confusion the registrar's contractual obligation is to respond appropriately to complaints of abuse and it's up to ICANN to enforce that contract. And in some cases—and certainly, not all cases—but in some cases, where there's clear-cut examples of phishing, for example, that are technical DNS Abuse and the domain name's not being used for anything else … In those cases, there is only one way to respond appropriately to complaints of abuse.

The problem is that ICANN Compliance won't go that far. We don't need changes to the contract. It's right there. The registrar has to respond appropriately. What we really need is for ICANN Compliance to, especially for those registrars that are getting a bad reputation … I won't call any registrar a particularly bad actor. But ICANN Compliance

needs to step up and say, "You have not responded appropriately to this abuse complaint," and that's what we need.

KEITH DRAZEK: Okay. Thanks very much, Brian. I think, Jim, did you want to respond to … Let me just pause there for a moment. Good conversation so far. Thanks, everybody. I'm going to turn back to the questions that I noted earlier. And I think Jim Galvin wanted to respond to Steinar's question earlier in chat.

Let me just say, for anybody contributing in the chat, you are more than welcome to put your hand up and speak. We've got time. This is important engagement and dialog so feel free to put your hand up. Sorry, Jim. Over to you.

JIM GALVIN: Thanks, Keith, and thanks, Steinar, for the question. The best way that I can think of to answer this question is simply to observe that all of the forms of technical abuse that we identify here—malware, botnet, phishing, farming, and spam, probably most notably phishing and farming as compared to spam—all have a variety of different types. You can do phishing in all kinds of ways which are unrelated to the domain name. Do phishing with phone calls, and with email, and with texting, and pure straight-up website content.

So, our focus, really our ability to focus and the area which we can work most effectively, is quite clearly when it intersects with the DNS directly.

We deal with spam insofar as it intersects with the use of the domain name and the domain name itself is part of the delivery mechanism and/or maybe it appears—it's a way in which the rest of the other forms of abuse are being delivered, whether it's in an email message or some other mechanism.

It's just anything more than that is really a content-based issue. And I hate to call it out in quite that way but that's part of the problem here. The issue with content is just that it's not a universally accepted definition. These technical forms of abuse are very easy. They're uniform. There's generally a pretty bright line as to what is and is not included so it's easy to make that the baseline and to do that. Doing more than that just requires additional study and additional work.

So again, I don't want to set aside the fact that spam, in general, is a problem on the internet. It's just not, as a general thing, something that we can deal with, just as we don't deal with phishing in general or farming in general, just the phishing, farming, and spam that intersect with the domain name space that we deal with. Thanks.

KEITH DRAZEK: Okay. Thanks very much, Jim. Much appreciated. Reg, I'm going to turn to you for a response to the question proposed by Chris Lewis-Evans earlier and then we will get back to the queue, which is, in order, Jonathan Zuck, Gabe Andrews, and then Fabricio again. If anybody else would like to get in queue, please do. Reg?

REG LEVY: Thanks, Keith. And just to remind everyone of context, the question was, "Once the work within the Work Groups is carried out and you come to conclusions to improve tackling DNS Abuse how do you get this applied across all the CPH?"

I would, again, gesture back to the slide that we've got up that this definition of DNS Abuse comes straight out of the contract. So it doesn't need to be applied across the Contracted Parties because it's already in the contracts. It already is applied across the parties. So if there is a domain name registrar, if there is a registry that is not complying with this portion of their contract, then that's something that Contractual Compliance needs to feel empowered to and approach them on, right? The contracts need to be enforced. And we agree and it sounds like you guys agree, so that would be my answer to that.

KEITH DRAZEK: Okay. Thanks very much Reg. I'm going to turn back to the queue. Jonathan Zuck, go right ahead.

JONATHAN ZUCK: Thanks, Keith. And thanks, guys, for this great discussion. I'm going to go back a little bit to what we were talking about earlier, which is that there seem to be instances in which there's recognized problems with a particular Contracted Party and there's a reluctance on the part of ICANN Org to act. And that's come up in a number of conversations. I know that Elliot mentioned in the chat, "Let's go name and shame." And Goran mentioned that he disagreed with that characterization.

I guess I'd love to just bring that idea to the surface. The most recent example was the Net4 India that took a very long time to have its contract revoked. And once again, it seemed to come down to them failing to pay their fees. And it's concerning. I think that to many of us in the community, that it's almost become a cliché that the only thing that's solid enough in the contract to actually provoke a revocation is fees. I think the optics of that are really bad for the organization and for the community as a whole

And so I'm wondering what you, as the Contracted Party House, can do in conjunction with Compliance to apply some pressure to get them to act on Contracted Parties that are really only making the rest of you look bad, if that makes sense. Thanks.

KEITH DRAZEK: Thanks, Jonathan. And I'll turn to colleagues who might want to respond. But I should note that Jamie Hedlund has added in the chat some data related to Compliance updates. There was a Compliance update in the prep week and some additional data is there. And I just wanted to note that Jamie has put that into the chat. And, Jamie, if you would like to speak you are more than welcome to get in the queue. But thanks for contributing what you did.

With that, would anybody from the Contracted Parties like to respond to Jonathan more directly? Jonathan, I'll just note that … I see some hands going up as well.

I'll just note that the Contracted Parties and ICANN Compliance have regular engagement and regular interaction as the Contracted Parties together—ICANN Registries/Registrars—and that certainly I think that we will endeavor to continue engaging with ICANN in terms of Contract Compliance. If there's a way for us to do it proactively and constructively, to try to identify bad actors and mitigate abuse as it relates to DNS Abuse and the definitions that we've put forward, that the Contracted Parties will certainly do that.

With that, I have Gabe, Fab, and then Elliot.

ASHLEY HEINEMAN: Keith, before we go, this is Ashley, chair of the Registrars Stakeholder Group. I just wanted to note that this has become I think an issue that keeps rising to the top with respect to our efforts with DNS abuse and that's how can we engage with Compliance? I think we realize that—we keep saying that we don't need contractual amendments because we already have hooks in the contract. So then it comes down to, well, how are these hooks being enforced?

I think you guys are all touching upon an area that Registrars and Registries … I can't speak for them but I think we do need to sit down with Compliance and figure out ways that we can more—or how they can more effectively and efficiently utilize the contractual hooks to really meaningfully address DNS Abuse. I think that's the issue. Compliance is working. They're working hard. We see their actions all the time. It's just can we find a way that we can more effectively address

abuse through the contracts? Because I think that's what we're all getting to, is that we're not seeing, necessarily, a real impact on DNS Abuse out in the wild.

So for whatever that's worth, we're hoping to sit down and figure out ways that we can talk to Compliance and work constructively together. Thanks.

KEITH DRAZEK: Okay. Thanks, Ashley. I've got a few other folks who'd like to weigh in here on this. So Martin Sutton, and then Brian, and then over to Sam, if she's got anything from the registries side.

MARTIN SUTTON: Thanks, Keith. Yeah, I think these are good points. Thanks for raising, Jonathan. One of the clear aspects that we see and need to appreciate is that there are greatly different models that exist within the Contracted Parties space to start with, especially since the new gTLD round of 2012. And they present different risk models.

Some that are more open, highly commercially-orientated, and rely on big distribution channels across the globe may attract more activity regarding DNS Abuse, as opposed to those that set up a model of more highly-restrictive entrance. They know their registrants. It's a very limited distribution channel, where it probably deters any DNS Abuse activity. It's not to say that those that may be at risk or more susceptible to their platforms being targeted don't deal with it. They do. We've seen

that in evidence with regular reports via ICANN themselves and that's some positive outlooks there.

But I think one of the key messages here is how do we identify the concentration of abuse? How do we understand what the cause is? Is it ignorance, so does it need to go towards more educational steering? Does it need more Compliance effort to tackle it? A combination of these sorts of things is probably where we need to get to.

But one thing that we do need to appreciate is that it's not a one-size-fits all and you can't just hammer down everything with policy or one heavy-handed swoop across all of the Contracted Parties because the majority of them are doing exactly what needs to be done and responding to these incidents. Thanks, Keith.

KEITH DRAZEK: Okay. Thank you, Martin. Much appreciated. So, we've got a queue building. So I want to make sure that we respond to the questions but make sure we get back to the dialog. So, I don't know. Brian Cimbolic or Sam, anything that you'd like to add at this point before we move on?

BRIAN CIMBOLIC: No. Just very quickly, Keith. I appreciate the question and I definitely do appreciate the desire to target the fringes of those that are really not living up to their end of the bargain. But part of this is also more aspirational, as opposed to just the pure Contractual compliance route, where we recognize that DNS Abuse is … It's not even just a problem

limited to the gTLD space. Clearly, there are ccTLD's where DNS Abuse is an issue as well.

And so we're are trying to, in the stakeholder group abuse groups, develop practices that can be implemented not just across gTLDs but across ccTLDs as well. Phishing is phishing, if it's in a gTLD or a ccTLD. And we actually have participation from ccTLDs in the group as well. Nominet participates and we can pull from their expertise, both from—they're obviously both gTLDs and ccTLD operator.

But we want to develop practices and recommended procedures that are implementable across the DNS, not just gTLDs or ccTLDs. We're trying to help provide resources to registries that might not be as well resourced or have the same know-how as other registry operators. Right now we're trying to, as Martin put it, focus on that educational phase and trying to make registries that are interested in getting better, better at dealing with DNS Abuse.

KEITH DRAZEK: Yeah. Thanks very much, Brian. And I think we need to move on in the queue so we will do that here. But I think Brian makes a really good point. It's about education. It's about identifying processes and resources that would be helpful to those registrars and registries that perhaps don't have the resources, the expertise, the experience, the current focus to help them do better with tools that we may be able to develop and identify. And that's definitely one of the action items that the DNS Working Group, under the CPH, have been focused on and will

continue to focus on. So, thank you for that. I have a queue now and that is Gabe, Fabricio, Elliot, Mason, and Susan. Gabe, over to you. Thanks.

GABRIEL ANDREWS: Thank you. Speaking as a member of law enforcement within the Public Safety Working Group, we sometimes see complaints from victims—victim organizations, typically—that might be smaller to medium-size and not really have the resources available to necessarily be aware of the types of blacklists and threat reporting that others might know and use on a daily basis. Sometimes, these complaints will be something as simple as knowing that there's a domain registered that might be a look-alike of theirs or perhaps a file path that's looking alike within a completely unrelated domain. But then, when they visit it, they'll see essentially a copycat site of their site setup. And it's especially egregious if that copycat site is perhaps a login portal for their customers to log in to provide their credentials.

In those circumstances, would we all agree? Would this meet the level of reasonable belief, that this represents evidence of phishing of that company's customers? And where would you draw the line to reach that threshold? And I suppose, Brian, not to put you on the spot but this is predominantly a question for Brian Cimbolic with regards to the DNS Abuse framework but I welcome others to throw in their comments too. The main concern here being that when you have evidence of phishing but not actually insight into the phishing vector itself, whether it be email, or SMS, or Facebook Messenger, or whatever—any number of the

1,000 different communication channels that exist. Can we still agree it's phishing?

BRIAN CIMBOLIC: So, since I was named, I can jump right in. Thank you for the question, Gabe. Phishing, to an extent, still can often be a factually intensive analysis too, because it depends on what the page is set up. But in theory, what you're describing, does it seem to rise to the level of phishing? Yes. I think that the answer to that question is yes. Without having, actually, the benefit of reviewing that potential site, yes.

The only thing I would say is that there's obviously nuance in any of these questions and. For instance, if the domain was compromised or if you're talking about a third-level domain, or a subpage, or just a particular URL on an otherwise legitimate site, it's important to remember that taking action doesn't always mean suspending the domain name. In particular, there's almost nothing a registry itself can do about a compromised domain other than working with the registrar or trying to get the registrant back online to get control of the domain itself. So, in a vacuum, it's hard to say. Does that sound like it rises to the level of phishing? Yes, but the devil's in the details.

KEITH DRAZEK: Thanks very much, Brian. And thanks Gabe, for the question and for the very concrete example. I think that's actually very helpful to all of us as we move forward and take next steps in terms of these ongoing conversations and dialog. Fabricio, over to you and then to Elliot.

FABRICIO VAYRA: Thanks, Keith, and I'll be quick. I just wanted to pop up to say thank you to Brian for offering to open channels of communication on people who aren't following the framework. I understand the difference, obviously, between the framework and Compliance. And I guess that led to my next question, which is … Brian, I'll definitely reach out. And I'll log who it is we're contacting and who isn't following the letter of the framework.

The query, then, on the other side of the fence, would Compliance or ICANN Org want to know about those people as well—I know Jamie and Goran are both on here—and query whether they would want to know who it is who signed this framework and isn't dealing with just obvious things that fall under the framework. Would that be helpful?

KEITH DRAZEK: Okay. Thanks, Fab. Anybody like to respond? Fab, maybe we'll circle back to that one and I'll see if anybody else would like to respond in a moment. But let's keep it moving through the queue. We've got just a little bit over 30 minutes left. Elliot, over to you.

ELLIOT NOSS: Thanks. I think that I'll respond to the previous, Fabricio. And let's use Gabe's facts because I think that they really do provide us with a nice opportunity here. It is our view that in general—and Brian did a good job of caveating—that we would take something like that down. Now,

in order for us to do that we've got to believe that we can do that inside the frame of our existing contracts. And we do think we can, under 318.

I want everybody here … We have to go into a little bit more pragmatic detail. 318 has general language. That language, then, if it was ever litigated, would be interpreted by a judge. It is my strong view that when we have something like this framework that a number of industry leaders have signed up for, it creates a significant presumption for any litigation. I could not imagine a judge trying to substitute his judgment for 12, or 15, or 20, or however many signatories there are—their opinion as subject matter experts who have been living it for years and years.

So that's important. I want Jamie to hear that. I want Goran to hear that. I want Russ to hear that. Because I want you guys to see that as what would allow you to aggressively enforce. Let's make Gabe's situation simple. Simple would look like the content he described with a vowel, with a French or Spanish accent on it that was Bank of America but with an A that was accented. We just have a Unicode variant. That's it. Simple, right down the center of the highway example. As far as I know, no registrar has ever even had a breach letter under 318 in a situation like that.

I absolutely not only understand, but on a couple levels appreciate, that ICANN Compliance has not been liberal in their application of 318. But we're in a place in the world today that's different than it was two years ago, five years ago, and 10 years ago. We live in a world today of much

greater platform responsibilities. And so I think that we have to start crafting things like that.

For those following the chat, Fabricio, I invited you to, "Hey, let's go do a couple things together." Gabe, maybe it's better for you because, frankly, I think that examples of phishing are much better than examples around intellectual property. Fabricio, I apologize if you might also have phishing examples. But we've got to start, together, creating a body of—and I'm using this in the smallest L sense possible—law and precedent that is going to create the contours for what's okay and what's not in the DNS. Thanks.

KEITH DRAZEK: Thanks very much, Elliot. And I think very constructive suggestion for more direct engagement in a very focused way. And thanks to Gabe for teeing up the example. There's some really good exchanges going on in chat. I want to make sure that nobody's missing that and if folks would like to weigh in, please do.

But before we move on, Fab. I think you've seen it. But just to ensure that the question that you posed earlier, that we took offline for a moment, I think has been responded to by Jamie from ICANN Compliance and, I think, an opportunity for further conversation there. But I did just want to flag that for everybody.

Okay. So next in queue I've got Mason, and then Susan, and then Alan Woods. Mason?

MASON COLE: Thanks, Keith. I wanted to follow up a bit on what Elliot just elucidated and then, also, on what Ashley was talking about earlier, in terms of hooks in the contracts. I know we look at these contracts pretty extensively. And if there are hooks in those contracts, that's all the better. But if those hooks, I think, were meaningful or impactful, then we probably wouldn't have the level of DNS abuse that we already have.

Is there another role for Compliance in this situation, whereby we could, say, issue advisories to meaningfully address DNS abuse or take other steps that Compliance can take to help the community in this obviously wide effort that's now underway? Is that a possibility? Thank you.

KEITH DRAZEK: Okay. Thanks, Mason. And we'll keep going through the queue, if folks would like to weigh in. Actually, Sam, do you want to jump on that one? Thank you?

SAM DEMETRIOU: Yeah. Thanks very much, Keith. And, Mason, thanks for the question. I think was you're describing is at the heart of what each of these respective working groups are trying to accomplish with our output documents. It's not only educational materials but materials that are seeking to normalize the way Contracted Parties do respond to things by making very clear what the various actions are. And, "If you get a

complaint about x, here is a list of options. Here's what makes sense in various situations," and things like that. So I think that's one of the things we're aiming at.

In future documents that we're planning to work on and put out there for the use of other registries, other registrars, whomever, is also going to be focusing on how complainants—how folks who observe DNS abuse—can put together a good and complete plan that has all the necessary information for a registry or a registrar to—they would need in order to potentially take action—obviously, not a guarantee of action. But what information is needed for them to even be able to get off the starting blocks?

So I know that the Registrars, we have gotten pretty far along something like this. It's something that the Registries Working Group is also going to be working on pretty soon. I think it's one of the next ones up in our docket for things to work on.

So I think what we're trying to do is we're trying to continue to close that gap further and further by making that variability that you talked about a little bit decreased. I know this doesn't really get at the question of ongoing compliance enforcement across every single party. But we're also sort of thinking about it from the perspective of you have to start somewhere. And this is where we're focusing our attention right now because we think there's a lot we can accomplish by setting some of these foundations and setting that groundwork.

KEITH DRAZEK: Thanks very much, Sam. And I'll just note that there's further discussion going on in the chat, questions about voluntary versus Compliance, etc. So just want to flag that. Fabricio, Susan, then Alan. Fab, over to you.

FABRICIO VAYRA: Sorry. That was an old hand. I'll put it down. I'll yield my time.

KEITH DRAZEK: Okay. No problem. Thanks. Feel free to get back in queue, if you like. And appreciate everybody's patience as we work through the queue. Susan, then Alan.

SUSAN KAWAGUCHI: Hi. Just wanted to check that you can hear me.

KEITH DRAZEK: Sure can. Go right ahead, Susan. Thanks.

SUSAN KAWAGUCHI: So one of the questions which goes with Gabe's introduction of the issue he brought up was we'll see phishing. We take a screenshot. Sometimes we can't always grab a screenshot because by the time you get back to it, you've reviewed it. The phishing doesn't always stay up for a long time, right. Or sometimes, an IP address is blocked. But abuse report is critical and important to the health of the internet, even though the phishing may be over.

So how do we deal with that when we're reporting those for our customers? And in fact, when the registry or registry receives a notice that the phishing is gone. We're alleging phishing. We may or may not be able to provide that screenshot that shows phishing. How would you recommend dealing with those? Because as we all know, even if someone else in the ecosystem has detected it, they may have already taken action. But that registrant may use that domain with a different ISP, different hosting. So the registrar and the registry are really critical there. So that's one question.

The second question I have is, is it possible to be, in the response from the registrar or the registry that have signed onto the DNS Abuse Framework, to be more specific in tracking what actions are taken? It's very hard to tell at times. Did the registrar take action, did the ISP take action, or did the registry? If we see a server hold on a registration, we're going, "Oh, okay. Registry must have taken action. Client hold." But it's not always clear. And that would be very helpful to understand, if we had a more concise response and not so generic.

And I understand why you could create generic responses. But in these cases, because this is a very high-level abuse, I think that it's critical to really understand the problem, to have an exact response to that specific domain name. And you could still have categories. But if the registry takes action, it would be great to know for sure that they took an action—that they confirmed that. So those are my two questions.

KEITH DRAZEK: Okay. Thanks, Susan, for the questions. Much appreciated. I'm going to turn to Reg for a response, at least to the first question. And then, we'll see if anybody would like to respond to the second. And if they're directly related, then, by all means. Reg, over to you.

REG LEVY: Thanks, Keith. And thanks, Susan, for the question. So we typically see phishing reports that have already been actioned. We have a reseller network, which I know is not necessarily common in the industry, as well as hosting companies and registrants themselves.

So if the phishing has been resolved before we get to it, we do consider that to be a win. The registrant has been educated. The hosting company has taken it offline or the reseller has taken action. And often, the action that we would take is … The first line of action would be to send it to our resellers and say, "Hey. Did you know that this is happening?" so that they can interface with their customer.

Often, phishing manifests on a website that has been defunct for a while. So the registrant doesn't even know that their domain is being used for phishing. So it's not necessarily going to be the case that just because phishing isn't there, we should still take the domain offline. So that'd be my answer to your first question.

And as to the second, we have generic responses that we send out because, again, using phishing as an example, we probably have 10 or 15 concerns about the particular domain from various different sources and we're not going to respond to every single one with exactly what it

was that we did. We'll say, "Thanks for telling us. We'll investigate." And as I indicated earlier, our investigation's going to be to make sure that the phishing is still active, to tell our reseller, and then to help the reseller or the registrant fix it, if that's possible, or to take the domain offline, if that's necessary.

So my question back to you would be what is the issue that you're trying to solve with determining whether the ISP, the hosting company, the registrant, the reseller, the registrar, or the registry took action?

KEITH DRAZEK: Okay. Thanks very much, Reg. And, Susan, I'll give you a minute to think about that and to get back in queue with a response, if you'd like. But let me go to Alan first and then to Volker.

ALAN WOODS: Thank you, Keith. I always have the distinct pleasure of going after people like Reg and Sam because they steal my thunder and they basically say exactly what my thoughts were. So I will not labor the point on this one.

I think what I wanted to talk about specifically was the importance of and why we see such a prevalence now of things like the Internet and Jurisdiction, the Framework to Address Abuse, and of course this DNS Abuse Institute because it's so important to understand that we are just a part of the puzzle—that we are one cog in a much broader mechanism. And it's important that when something comes to us, that

it comes to us fully-baked in a way, but also that it comes to us at the right time, the right place.

I always see it as being there as a temptation, from a Registry or Registrar point of view. We wield a very large power. And that is the ability to take a sledgehammer to the DNS and take it down. But sometimes, that fails to see the nuance that is involved. We do not have a scalpel and we cannot surgically remove elements. So it is important when reports come to us that we are provided with the evidence that can support us.

So this somewhat goes to Susan as well. In the case where a phish has been observed but not evidenced, it's very hard for us to be able to take that, unless we see that evidence along with it because there are elements such as is the domain compromised? Is it not? Where can we point a registrant if they are the innocent actor in this? Where can we point them to?

So I think why, personally, I'm embracing things such as the Framework to Address Abuse and the Internet and Jurisdiction is because it gets us to be able to point out where our pain points are. How can we help you better? But more so, how can you help us to help you?

And I know that sounds trite but it is important. When an abuse report comes to me, if it has its ducks in a row, if we can see where the more appropriate parties have just failed to do anything, then we are in a much stronger position to be able to take action. And also, that could then also inform ICANN Compliance, where in those well-rounded cases, a particular party does not take action. And that means that they

have much more to be able to grab on, based on the current contracts as well. So I'll leave it there. But thank you very much, as well, for this. It's a great session.

KEITH DRAZEK: Yeah. Thanks very much, Alan. Susan, if I could come back to you, if you'd like to respond at this point.

SUSAN KAWAGUCHI: Well, one of my concerns is … And I may have lost track of Reg's question. But in the phishing that I see, it is very rarely an old domain. It is a recently-registered domain. And in viewing the domain name itself, it pertains to a brand.

So there is no working with the registrant, in my opinion, and it just should be taken down because the intent is pretty clear, when you read the domain name, that the intent of registering that domain was to use it for abuse. If something's registered and three days later, or even three hours later, it's up and it's phishing, there's no confusion by the registrant. They know what they're doing. So swift action needs to be taken. So I think that's about it.

KEITH DRAZEK: Okay. Thanks very much, Susan. Brian King, if I could turn to you for a follow-up.

BRIAN KING: Thanks, Keith. Glad you saw my hand. I think one point that Susan alluded to earlier, that I'd like to make clearly for our Registrar friends is that we see often—or at MarkMonitor, we used to see, when we owned a brand protection business—that we could get action very swiftly from webhosts and ISPs to take down the site content—to use that scalpel and surgically remove the phish.

And that was good until the bad guy still owned an infringing domain name and still had control over that HTML code that made up the phish website. And what would happen is … If any registrars are an ISP, cover your ears. Hosting is a dime a dozen. And the bad guy would just hop to a different host, use that same domain name, which remains active and plugged into the DNS, and then put the phish right back up.

So IP owners, then, engaged in a game of whack-a-mole, where they're taking action over and over again on the same domain name. And I think what owners would like to convey to registrars is that with evidence that this is a phish—potentially one that by the time it gets to the registrar's queue may have been taken down—it might still be appropriate to suspend that domain name to prevent the phishing attack from popping back up in another host, using that same infringing domain name.

And the UDRP exists—I know what registrars are going to say—to recover that domain name. And often, that's a step that's coming, and that the IP owners will be taking advantage of. But as we all know, the impact of the phish, as Susan mentioned is that it happens very quickly and needs to be addressed very quickly before more harm happens. So

that's a concept that I think is worth just explaining very clearly to registrars. Thanks.

KEITH DRAZEK: Yeah. Thanks very much, Brian. And thanks for bringing the perspective. Really appreciate that. Everybody, we have about 15 minutes left. Just a quick time check. I'm going to turn to Volker next but if anybody would like to get in queue here, I encourage you to do so. But this really does strike me, I think. I'm seeing some opportunity for continued conversation and engagement, particularly around the output documents that the Contracted Parties are working to develop.

I think that'll be an important opportunity for us to make sure that, from a Contracted Party perspective and from other parts of the community, to make sure that we're being as clear and helpful as possible, in terms of identifying the type of information, the type of data that we would need to act expeditiously and that this is an important opportunity for continued dialog. So thanks. Volker, over to you.

VOLKER GREIMANN: Yes. Thank you. I think one of the most important things that we need to fight abuse is sufficient evidence—evidence that has to be presented with the complaint. The more you can provide, the better it is for us and the easier it is for us to reproduce the abuse and take action upon that. Many abuse complaints just say, "There's abuse on that site. It's phishing. Take it down."

That leaves all the research—all the work to us to find out, a, how can we reproduce that phishing, if it's not immediately visible. Is it fast flux? Is it something that we are geoblocked from? Is the phisher clever enough to exclude a registrar IP and we have to use a tunnel from a certain country that we don't which this is targeted for? There's a lot of evidence that the complainant can provide.

And even then, we can have complaints where the best evidence is provided and it's still a false complaint. We had a recent complaint from a producer of a gaming console that complained about a domain name that was registered, that sounded like the console that was being registered. It looked like a phish. It smelt like a phish. But the registration data ultimately told us, "Let's ask the registrant if there might be something going on here."

And we ultimately found out, yes. The European division registered the domain name without the knowledge of the Japanese division. And therefore, it was actually a good domain name. And had we taken action upon that, then we would have taken down a very, very important domain name for them.

Therefore, for us, it's very important that the complainant does their research, that the complainant is absolutely sure about what they send us. Because the more false requests we have, the less good requests we can action in due time. I think that's also a consideration that we want to be fast on that. So may we urge you, the complainants, whatever you can provide as information, give that to us so we can take action.

KEITH DRAZEK: Okay. Thank you very Volker. If I could turn to Brian Cimbolic to add on and then, Mason, I'll come to you next.

BRIAN CIMBOLIC: Thanks very much, Keith. I just wanted to actually briefly touch on something that both you and Sam mentioned about our output documents. Those output documents are really meant to be informed by our outreach sessions.

So if there's any … Much in the same way that there was that shared areas of interest and really a low-hanging fruit for the Registries to work with the Public Safety Working Group on this DGA Framework—this malware and botnets at scale—we're certainly very interested to hear from you, from the rest of the community, as far as what are some outputs that we can create that would be helpful for you as far as what goes into an effective notification for abuse, as far as expectations for someone. Once they've made a notification, what happens from there?

We want to do this to really help inform both Registries and the broader community. So please don't be shy in letting us know what we can do to be most helpful to you, as far as advancing the dialog here.

KEITH DRAZEK: Okay. Thanks very much, Brian. And Volker, I think that's an old hand. Mason, you're next. And then, I will turn to Martin Sutton. Mason?

MASON COLE: Thanks, Keith. I just wanted to return to question number three on your slide on the screen, "Are you seeing practices from registrars and registries that you find helpful?" Yes. One of those programs is trusted notifier. I've seen that work in past scenarios. I don't know to what extent it's being applied right now by registrars and registries but I know I'd be interested in knowing that. And if they're not being employed, what, if any, plans are in place for those being deployed out into the market? Thank you.

KEITH DRAZEK: Thanks, Mason. I think that's a really important point you make about the role of trusted notifiers, and trusted notifier frameworks, and relationships that exist or might exist. I think you or somebody mentioned earlier, in the chat, the pilot program that was engaged late last year with the FDA, around the illegal sale of opioids online in the United States. Several registries, including Verisign, participated with the FDA and the NTIA to engage in a pilot program, which was essentially a trusted notifier type of framework. So it was a Verisign, PIR, and Neustar Registry were the three that participated in that pilot program.

And I'll defer to others to speak to it specifically. But I think your point about trusted notifier is a very important one. Some excellent work has been done in the Internet and Jurisdiction project and policy network on this point. And I think that there's more to be discussed, looking ahead, around trusted notifier engagement and frameworks within the community.

With that, I'm going to turn to Martin Sutton, who wanted to follow up on an earlier point. And then, I'll turn back to Susan. So, Martin?

MARTIN SUTTON: Thanks, Keith. I think I just want to flag the webinar that was presented last week by the DNS Abuse Institute. It seems that I think I recall Jeff Bedser's—who's probably on here, can probably explain it a lot better than I. But I do recall his approach and suggestions string a lot of these issues together or ideas that people have presented today.

I remember his recommendations were around making sure there's a standard definition of the abuses. Adopt relevant evidentiary standards was a key one, which is cropping up here quite a bit. Developing the best practices to reduce the lifecycle of the affected domains. And apply standardized escalation paths for abuse resolution. And then, establish reasonable timeframes, also, for action on abuse reports. That seems to bring together quite a lot of the concerns and issues that have been raised, plus ideas about how this could be improved. So, just wanted to flag that, that there's some good ideas and try to bring this together into a coordinated effort is continuing. Thanks, Keith.

KEITH DRAZEK: Yeah. Thank you, Martin. And again, just to reinforce what Martin said is that there was a great webinar recently. I don't remember the specific day. And Jeff Bedser's input on that, I think, was particularly helpful. So just to flag that for everybody. If you haven't had the chance to see

that—to follow that—I encourage you to do so. Susan, I'm going to turn to you next and then to Rowena from the Contracted Parties. So, Susan.

SUSAN KAWAGUCHI: Thanks, Keith. So really, this is in response to Volker. You named off a string of things. And it would be interesting to include those requirements or proposed requirements for a report in the documents that the CPH—the Registries and the Registrars—are working on. We could look at those and see how feasible it is to do that. I'm not sure, on figuring out tunnels and all of that. But it would be helpful to have a better understanding what is the best evidence to submit. And if it's feasible to submit that. So that is something that would be helpful to work on.

KEITH DRAZEK: Thanks very much, Susan. And let me turn to Rowena. And then, Volker, is that a new hand?

VOLKER GREIMANN: Yes. It is.

KEITH DRAZEK: Okay. Let me go to Rowena first and then I'll come to Volker. And then, just time check, we have less than five minutes left. Thank you.

ROWENA SCHOO: I'll be brief. Thanks, Keith. I just wanted to say something quickly on the trusted notifier concept because I think people might not be as aware as how we treat this in .UK as a country code, and even with our gTLDs, .wales and .cymru because we have the benefit of being very geographically linked to our location. And we've always taken the view that what is criminal under the laws of England and Wales is also unacceptable online.

And the way that our abuse practices have developed has basically been around having a trusted notifier relationship with a selection of different law enforcement agencies. So we have 13 different agencies that we've inducted into that process, gone through a series of educating them and hearing from them about the types of crime they see. And then, we have an arrangement in place where they can send us notifications to suspend domain names.

And recently, we've also expanded that to include redirecting domain names so that we can, after those criminal activities have taken place, we can put up a page where we give a bit of official advice and help to people that might come across that on the web so they can reach out to the appropriate areas.

That covers more than just technical abuse because it is anything that is criminal under English and Welsh law. But there is obviously a bit of an overlap with that Venn diagram. So for example, that could include phishing that's come through as fraud, as well as other things.

KEITH DRAZEK: Okay. Thanks very much, Rowena. This suggests to me that in the conversation around trusted notifier engagements, we could probably have a whole other session and take up the entire time on just that conversation. So maybe something to look ahead to. But Volker, I see you're next. And then if anybody else would like to get in queue for last questions, last input. And then, I will hand it back over, briefly, to Jim, and Brian, and Reg, for any concluding remarks from the Registries and Registrars, respectively. Volker, you're next.

VOLKER GREIMANN: Yes. Thank you. Just to come back to Susan's remarks, which I think are helpful here. I don't consider these requirements, per se, because every abuse case that we deal with is different in some cases. And the evidence may be different as well. So, if we say, "You just include a screenshot of this or that," then that might not be relevant for that kind of abuse type.

So we would ask the complainants to use their own judgment when making a complaint and provide everything that they can think of that would be useful for us, such as how to reproduce the abuse case. Where has it been accessed from? What time? That allows us to follow that back so we can take action or inquire whether customers—what might have been the root cause for that.

And in some cases, it's the domain name that is being abused by a third party and the registrant would be very interested, indeed, in these details as well so they can exclude their advertiser, for example, that

has been abusing their domain names, that is being used for various monetization schemes.

And one further information that I would ask of complainants to look at as well is has that domain name been reported before? Is it included in certain abuse lists? If so, for how long? And if it is, do you think that reporting that again, for those registrars that use these abuse lists, provides extra value? Because we sometimes get 10 or 20 reports for the same domain name that is also included in certain abuse lists that we scan. And we are in the way of taking care of it but having to close multiple tickets for the same case and responds to the complainant of each case, then it becomes unwieldy and, again, takes up time that could be spent more efficiently fighting abuse directly. Thank you.

KEITH DRAZEK: Thank you, Volker. Just, again, to note, I think there's been some extremely constructive and specific focused discussion on the key questions. And you're getting into some operational dynamics here, which I think is really important.

For the last several years, we've been talking, as a community, about DNS Abuse at a fairly high-threshold level or a high level. And the opportunity for us working together to identify what can be done, what should be done, what specific information do Contracted Parties need to be more effective and more expeditious in our actions, our engagement with ICANN Compliance, and with the community and trusted notifier engagement. I think these are all really important discussion points.

And the more focused, and explicit, and concrete we can be with our examples, and our recommendations, and our questions, will only help to serve us moving forward as we working mitigate and make this better.

So with that, Jim, and Brian, and Reg, if I could hand it over to you for any concluding remarks and then we will wrap.

JAMES GALVIN: Thanks, Keith. I'll just launch off of what Keith was just ending with there. I think the major takeaway for me in this session is that we all come from a different perception of DNS Abuse. We all come from a different perception of what we think can or should be done about it.

One of the main goals, from my point of view, of our outreach that we're doing with all the various SOs and ACs is to hear these stories more directly and to really reach out and understand, as much as we can from everyone in the community, just those kinds of answers—to talk about those questions. What is important to you? What are your pain points? And what would be helpful to you?

And we want to look for ways in which we can be helpful. There clearly are limits. And maybe understanding each other is probably the best path forward. More discussion about what the limits are of what we can do. And yet, even with that, maybe we can be helpful in launching off something else, somewhere else, that would be helpful to your pain points. We are trying to be part of the overall solution to DNS Abuse.

So thanks very much for that. Look forward to further engagement as we continue to engage with each of the individual groups here within ICANN. Thanks.

KEITH DRAZEK: Thanks, Jim. Brian, anything to add?

BRIAN CIMBOLIC: No, just thank you very much, everyone, for participating here. I think it was a great dialog. And we hope it's just part of an ongoing dialog. We both in the Registrar and the Registry abuse groups want to help the resources, not just for Registries and Registrars but the community. So again, just an invitation. Where can we helpful? How can we help inform or contribute to community discussions? Let us know and we look forward to continue talking to everyone. Thanks.

KEITH DRAZEK: Thank you, Brian. Reg?

REG LEVY: Thanks. And thanks to everybody who participated. As everybody has already said, I appreciate the dialog and the questions raised, both in the chat and orally. That was great to engage with everybody. I look forward to more in the future.

KEITH DRAZEK: Thanks very much, Reg. And thanks to everybody. Final comment, this is just part of the discussion and the dialog. We expect this to be ongoing. If you've already met with the Contracted Party DNS Abuse Working Group in a one-on-one way with your various groups, it's not the only time. We have opportunities. And we really hope and expect to have those ongoing discussions and this be an iterative process. So thanks, everybody for joining. We're a couple minutes over time. Have a great ICANN 70 and we look forward to seeing you soon. Thanks very much for your input. Bye.

SUE SCHULER: Thank you, Keith. We can end the recording.

JONATHAN ZUCK: Thanks, guys.

[END OF TRANSCRIPTION]