ICANN77 | PF – DNS Abuse Negotiation: CPH Outreach Session
Tuesday, June 13 2023 – 13:45 to 15:00 DCA

TERRI AGNEW: Hello and welcome to the session of the DNS Abuse Negotiation-CPH Outreach. Please note that this session is being recorded and is governed by 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. I will read questions and comments aloud during the time set 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.

This session includes automated real-time transcription. Please note this transcript is not official or authoritative. To view the real-time transcription, click on the closed caption button in the Zoom toolbar.

To ensure transparency of participation in ICANN's multistakeholder model, we ask that you sign in to the Zoom session using your full name. For example, a first name and last name or surname. You may be removed from the session if you do not sign in using your full name.

With that, I will hand the floor over to Chris Disspain.

CHRIS DISSPAIN: Thank you very much. Welcome, everybody. Good to see everyone here. I have a very important job which is basically to hand the floor to Russ who is going to take us through some slides.

We're going to go through the background, the amendments, and so on. And we're going to stop at each relevant section for questions rather than save them up until the end. That way we hope it will be a bit more interactive and we can answer questions as we go.

So, Russ, over to you.

RUSS WEINSTEIN: Thanks, Chris. This is Russ Weinstein. I'm the vice president of the GDD Accounts and Services team at ICANN within the Global Domains and Strategy function. One of my other roles within ICANN is also leading our DNS Security Threat Mitigation Program.

And so this project here to develop contractual amendments related to DNS abuse fits into both of those roles within our team. And we did this as our cross functional effort within ICANN in partnership with Contractual Compliance, our OCTO team, and legal teams putting our heads together and working collaboratively with the CPH to develop these amendments.

Today, we'll go through, as Chris mentioned, the background and scope, how we got here. We'll talk through the detail of the amendments. We'll talk a little bit about DNS abuse and what that looks

like in practice. What are the options contracted parties have when faced with abuse?

We'll talk about how we intend to enforce these amendments. And you may have noticed we published an advisory in addition to the amendments as an item to support the documents, and we'll talk more about that.

And then we'll talk a little bit at the end about the procedures and how we bring these things into reality from where we are today in the process to bringing them into fruition which is, as usual at ICANN, something more complex than you'd expect. So, as we said, we'll do Q&A as we go. And with that, let's dive in.

So hopefully you've all seen we opened the public comment on May 29, and that public comment will be open until July 13. What's out for public comment are proposed amendments to the Registrar Accreditation Agreement, and the changes are Section 3.18 which is where the abuse provisions are already. And for the Registry Agreement we're looking at Specification 6, Section 4 and some minor changes in Specification 11.3(b).

Earlier I mentioned there was a draft ICANN advisory, and that advisory is a supporting document for these amendments and will be something that we could use if these amendments get adopted that helps provide expectations for compliance with the proposed obligations. I really encourage you to check that out. It's about 15 pages long. It walks through what we mean about each of the obligations and provides examples, and we'll talk more about that as we go.

With that, we'll turn back to Chris who can provide background and context for how we got here.

CHRIS DISSPAIN: Thanks, Russ. I think there's a next…yeah, here we go. And the next one, please. I'm not going to read them, but they're up there. Please feel free. So basically, as you know, DNS abuse is a topic that's been around for quite some considerable time. There has been action. Things have happened. We have the framework DNS abuse which was launched in 2019 and many registries and registrars are signed up to. And also, work goes on.

But about a year ago the community, the contracted parties started to get together and say what we need to do is to start being proactive, take some action. The goal was to lift the floor, to create a floor in the contract. It is not about creating best practice. It's about creating the minimum standard to improve on the current contracts to actually make sure that registries and registrars were obligated to take some action in respect to DNS abuse and to provide ICANN with contractual amendments that enable them to enforce those clauses in the contract.

Now everybody acknowledges that the contractual amendments are only a part of a larger and wider process. It is the first step to get this floor in place. And then there needs to be policy and there needs to be a series of very narrowly scoped PDPs that deal with each individual piece of the jigsaw and create the policy for dealing with DNS abuse.

And that is the goal. So the goal is to put the floor in place which we believe these amendments do, make sure that Compliance can enforce them, and then move forward to the next step as I said which is policy.

I'll happily take any questions on that if anybody wants to, but that's merely intended to be background. Okay, so in that case, Russ, if you want to now take us through the amendments, that would be fantastic.

RUSS WEINSTEIN: Sure. So as Chris said—we can go a couple more slides down the line—it was really in January that we began work in earnest after formal notification that we needed to negotiate these amendments with the contracted parties. And so we worked together quickly and effectively to deliver proposed amendments for the community in under five months' time here. And I think that's something that everyone should recognize and hopefully appreciate there, the pace at which we worked to deliver these really meaningful changes to the agreement.

Before we dive into what's changed, it's always helpful to start with where are we now. And the current obligations in the registrar agreement are in Section 3.18. Essentially, the requirements are up on the screen, but the keys behind that are there's requirement to take reasonable and prompt steps to investigate and respond when there is an abuse report.

Registrars need to display abuse contact information about how to submit a report and what they will do once they get a report. They need to maintain records of how they handle reports and the responses they take. And they need to maintain a dedicated channel for law

enforcement or government authorities to provide abuse reports and respond within a certain SLA. So that's the floor which we started with, and endeavored to improve upon those with meaningful changes related specifically to DNS abuse. Next slide.

So the key, and you'll see very mirrored in the Registry Agreement, the key things we accomplished in these amendments are starting with what we had in place and building on top. There's no taking away in these amendments.

We clarified abuse contacts and making the reporting process a little bit better by making sure those contacts are readily accessible and ensuring that registrars have an obligation to provide a confirmation of receipt of an abuse report. That was something that would come up continually in community discussions about a challenge with tracking abuse reports and having evidence that you submitted it to the registrar before coming to ICANN, for example. So we solved a problem there.

We've added a clear definition of DNS abuse for the purpose of these agreements, and it's something that has been a longstanding discussion within the community and we built off community work to do that.

And then we added the core obligation at the bottom here, 3.18.2, an obligation to take mitigation action to stop or disrupt DNS abuse when they have actionable evidence to do so. And we'll talk about each of these things more, but this is the core one that's been missing in the conversation for some time and so is the really meaningful addition to the contracts. Next up.

So again, the first area we tackled was around how to improve the process of submitting an abuse report with adjustments to how the abuse contact needs to be displayed on a website for the registrar.

And also addressing an issue that's been a longstanding problem which is by publishing an email address, that email address becomes a target of spam and makes it harder and harder for registrars to identify real abuse complaints and follow up on them quickly. And so we gave them the opportunity to use webforms to help reduce the junk, essentially, and get right to the core problems. So we've made that adjustment in the amendments.

We're also added, as I mentioned, requiring the confirmation of receipt which we think is an improvement to the process for all users. There have been no changes to the requirements for law enforcement agencies, and there have been no changes to the retention requirements either. Next.

So definition of DNS abuse is something that's really helpful in this context. The current obligation has a little a "abuse" which is a broad terminology. For the purpose of these amendments, we use the term DNS Abuse and it means malware, botnets, phishing, pharming, spam when used as a delivery mechanism. Leveraging the work that's already gone on in the community, particularly the definitions in SAC115 to draw this definition of DNS Abuse.

It adds these specific requirements that we'll get into when we're talking about these things. It doesn't remove the requirements that exist today relative to little a "abuse," but it adds when we're talking

about DNS Abuse in these forms this obligation that we'll talk about next to mitigate DNS Abuse. Next.

So the core obligation here is when a registrar has actionable evidence that a registered name is being used for DNS Abuse, the registrar must promptly take the appropriate mitigation actions that are reasonably necessary to stop or otherwise disrupt the name from being used for DNS Abuse.

What this means is now just investigate and respond is no longer good enough when it comes to DNS Abuse. They must take a mitigating action, and we'll get into a little bit more about what that means. We tried not to be overly prescriptive, and we'll talk about why that is. But requiring that mitigation action is a big step forward in this space. And that mitigation action will always focus on how do you try and stop the name from being used for DNS Abuse or otherwise disrupt it from being used for DNS Abuse. And there are good reasons for both. Next.

I'll pause here and give the opportunity for questions. Then we can go on to the registry side. Not seeing any questions in the room. Are there any in the chat or in the Q&A pod or anything that we need to address. All right, we'll keep going. Oh, Steve?

STEVE DELBIANCO: A little slow raising the hand. Steve DelBianco with the BC. First, the BC wants to thank the contracted parties for more than just starting this process but now finishing it with a vast improvement over the status quo. I wanted to first start off with saying thank you. Really happy with it.

And then I had an ignorant question with respect to the submitting of a DNS abuse. We'll often have to attach a PDF to show the evidence of actionable harm and if a registrar chooses the webform method, is there a way to require that it allow a PDF upload? And if the email's there, we can't have them discarding attachments. Even though attachments carry security risks. I get that. So you can see the importance of being able to have a PDF under the new standard. How do we address that and make it happen? Thank you.

RUSS WEINSTEIN: I think that's a great question, Steve. I think when you read the requirements in total, I would say that that is a reasonable expectation that we would have as ICANN that if you're going to go the webform route, and correct me if I'm wrong our Compliance team, but if you're going to go the webform route, that you would have to enable the ability to provide evidence. Because what they need is actionable evidence. And so I think it's a very reasonable conclusion, and I don't want to put words in your mouth, but I think that's the way we've talked about it internally. And I don't know if the CPH wants to add.

OWEN SMIGELSKI: Thanks, Steve, for that. I'm speaking Namecheap personally. We already do accept those. I think we probably want to future proof it so it doesn't say "must accept PDF" because who knows in the future. But again, if it's going to be actionable evidence with the report, I don't know how you can provide that otherwise. So I know you said this is a good start and that it's ending. But, no, this is just the beginning of this. I know it came through the GNSO small team on abuse. They identified

some of these concerns, and so we've run with it. So it's been a very good multistakeholder effort, and there will be more after this. Thanks.

CHRIS DISSPAIN: Volker?

VOLKER GREIMANN: I think that's a good suggestion, and I think that we should probably include some language to that effect in the next iteration of the advisory that basically we include some ideas of what we feel that such a webform should have as a minimum requirement. And I agree absolutely that if we require that we are provided with actionable evidence and then shut off all doors to provide such actionable evidence, then we ourselves are defeating the purpose of what we are trying to achieve here and therefore we should be clear about that. Thank you.

CHRIS DISSPAIN: James?

[JAMES]: Yeah, thanks. James speaking. Yeah, Steve, I think one of the challenges operationally with just DNS abuse reporting and one of the reasons we're excited about being able to use webforms is that we are desperate for actionable evidence. We're probably in the high single digits in terms of percentage of reports that are complete and actionable and contain enough information to move on. But different types of DNS abuse would maybe have different types of evidence

requests. Some may have attachments, some may not. But I don't think you're going to get pushback from at least the contracted parties that are taking this seriously that any suggestions for improvements or how we can clean up and make those reports higher quality, we're going to jump all over it.

STEVE DELBIANCO: Thank you for the responses. It's definitely true we wouldn't want a hardcoded requirement for a certain kind of an attachment, and it may well be that I would provide a hyperlink to a file. But all of these carry security risks for the registrars that are opening it and I'm conscious of that. I would also just like to clarify that sometimes the evidence of actionable harm isn't actually occurring in this instant. It might have been two days, two weeks, two months ago with respect to that domain name and the registrant. So the harm doesn't have to be happening in the instant that you receive the report. It could be prior. Okay, thank you.

CHRIS DISSPAIN: Absolutely. Okay, anyone else before we go back through to the registry changes for now? So, yeah, go ahead.

SUE SCHULER: We have a question from Brian King. Same question as Steve DelBianco's but with respect to unduly limiting character limits in the webform, same answer?

RUSS WEINSTEIN: Yeah, I think that's something we can look at as Volker mentioned. I think overall you've heard from the contracted parties and from ICANN that the intention here is not to create barriers to entry. It's to create better quality abuse reports. And so I don't think that should be a problem.

CHRIS DISSPAIN: Okay, anything else? Do we have anything else, Sue? Okay.

ABDALMONEM GALILA: Actually, I would like to know what are the keys behind identifying the severity of the harm for such actions for these domain names.

CHRIS DISSPAIN: Can I just make sure we heard that right. Are you asking what are the criteria for deciding the severity of the harm?

ABDALMONEM GALILA: Yes.

CHRIS DISSPAIN: Okay, do you want to answer? Go ahead.

OWEN SMIGELSKI: Hi. Not every DNS abuse complaint is the same. The registrars/registries will have to look at them on a case-by-case basis and sometimes we've identified the four types—Internet phishing, malware, botnets, pharming, and then spam as a delivery—so we've kind of taken those as

a serious thing and that's something that's well defined across the community. We do find that they all are kind of severe, but also the approach can be what is the action that the registrar or registry could take and what would that have on the site? Is the site solely registered for abusive purposes, or is it a ten-year-old website that had a WordPress plug-in hack that has a phishing page on it? So that would be something that would have a different type of response to that.

CHRIS DISSPAIN: Sue?

SUE SCHULER: We do have a question, and it just scrolled past me. We have another question too. So let me go back to the first one. From Bill Jouris, "Is there a requirement to tell someone trying to report abuse what will be required as evidence?" Oh, somebody answered it in chat. Okay, then we have another question from Alexander Urbelis, "What about prospective harm? Login.bankname.com is a clear indication that a domain will be used as a credentials harvester. Would you need evidence of actual use to harvest credentials for a registrar to act under these new requirements?"

OWEN SMIGELSKI: Hi. This is a type of example that comes up frequently. We're not in the business as registrars and registries of combatting future crime or trying to read the intent of a customer. It's possible that that could be a legitimately registered domain name for purposes of, say, testing whether people who work at a certain company are being tricked by

that domain name as part of anti-phishing type efforts. So just because something is registered and could be abusive does not necessarily mean that action will be required.

That said, every case is different so it could really depend upon the circumstances. And that's why we do want to have actionable evidence because when a registrar or registry is taking action against an abuse there's potential for us to violate our contract with our customers. So we need to make sure that we have a solid legal basis for that. Thank you.

SUE SCHULER: There's another question. This one is from Tomslin Samme-Nlar, "I heard earlier that these proposed texts in the contract are meant…." It just scrolled past me, sorry. "…are meant to lay the floor for further work such as specific and narrow policy development work. What do you need the policy work for, and can you give an example of an issue coming out of this that you think the contracted parties might want the community to develop policy for?"

OWEN SMIGELSKI: I can't really put my hat on and see what it is, but this is something that originated through the GNSO Council small team on DNS abuse. That was a multistakeholder-ish model that the community was represented in that made these types of recommendations, so we ran with that. It will be up to the GNSO Council to scope and determine what comes next after this. Again, this is just something that ICANN and the contracted parties were able to get through in five months for these amendments

plus a 15-page advisory. That's extraordinarily fast in ICANN time, so we wanted to get this done to do something now actionable that cleared. And then moving forward, it will be up for the community to decide what is next for us to tackle. Thanks.

CHRIS DISSPAIN: Thanks, Owen. And just to add to that, I think the clear point is that we think—and it's not up to us—but we think that the best way to deal with it is rather than having a throw everything into the bucket major policy development process that we all know will take forever and etc., a series of narrowly scoped targeted ones that set out what the areas are that need to be worked on is the way to do it. But actually, the topics and the order that they get done in is a matter for discussion in the larger community, not for us.

Russ, I think we can go back to you now and go to the next slide.

RUSS WEINSTEIN: Sure. Thanks. Good discussion there. So on the registry side, the obligations will look very similar to those on the registrar side. And that was deliberate so that there's consistency and a common way of doing this across the industry, so to speak.

The changes between the registry and registrar agreement really focus on the difference in the role the registries play versus the registrars and this theory of closest to the action sort of thing. So the existing obligations related to abuse in the Registry Agreement are currently under Section 4 of Specification 6 of the Registry Agreement and it's to publish an abuse contact for handling inquiries and to remove orphan

glue records when used in connection with malicious conduct. Next one.

There are also obligations and Specification 11 of the base Registry Agreement. That's the public interest commitments. And in Section 3(a) there's a requirement, it's a flow down requirement to the registrar and on to the registrant via the registrar agreement to prohibit certain uses and activities of domain names within the TLD and for the registrar to invoke consequences when those are violated.

And Specification 11.3(b) is the requirement related to conducting technical analysis on a periodic basis to identify security threats and to maintain statistical reports related to those security threats that are identified and what actions are taken and to be able to provide those to ICANN as necessary. So again, that's the foundation which we built on top of for these amendments. Next slide.

So similarly to the registrar agreement, in the registries we clarified information about the abuse contact, where it needs to be located, and providing that confirmation of receipt again being and important element to it. Again, trying to improve the quality of abuse reporting and the whole process and the workflow. Next slide.

Same definition used so that we're consistent across. Next slide.

And a very similar obligation to take mitigation action. And again, the differences focus on the respective role of a registry versus a registrar, but they don't preclude registries from taking action directly themselves. So we'll read it through together.

When a registry reasonably determines based on actionable evidence that one of the domains in the TLD is being used for DNS Abuse the registry must promptly take the appropriate mitigation actions that are reasonably necessary to contribute to stopping or otherwise disrupting that domain name from being used for DNS Abuse. And at a minimum that should include either referral of the domains and the evidence to the relevant registrar or taking direct action by the registry when they deem appropriate. And again, allowing for the existence of different circumstances to dictate different types of action. But no matter what, action is still required and, again, that action is targeted at stopping or disrupting the DNS Abuse which is a big important factor. Next.

In Specification 11 under the 3(b) section we replaced the undefined term "security threats" with "DNS Abuse." We think this provides important clarification, helpful clarification to both registries and ICANN and the community that what we're looking for is domains that are being used to perpetrate DNS Abuse.

And what those actions are in thinking about the mitigation action requirement, when a registry has an action or has the obligation to refer to a registrar or take action themselves, when they refer it to a registrar that then would kick in the registrar obligation to do their mitigation steps. And so it's a good chain, a value chain.

And I think that's the end of these changes here.

CHRIS DISSPAIN: Let Owen go now and then do questions.

RUSS WEINSTEIN: Great. So Owen's going to talk briefly about DNS abuse mitigation techniques and considerations, and then we'll open it back up for questions because I think that will be a helpful foundation for those questions.

OWEN SMIGELSKI: Thanks, Russ. Next slide, please. As I touched upon briefly earlier, there is not one action that registrars or registries can take to combat or when dealing with an abusive domain name. Usually at the registrar or registry level there's really only a nuclear option that we can take, shut down the whole domain name. And since that's a very drastic step, it's not always the first step. And I know sometimes people think that the site's doing abuse, you need to shut it down. That's not always the proper approach for that.

So a number of things that registrars and registries can do is to suspend the domain name. For the registrar side, that's by using the EPP status code called client hold. That makes it so the domain name just does not resolve, period. Registries also can do that through something called server hold.

There are some other things that the registrars and registries can do. They can delete the domain name, completely get rid of it. And that is something that often happens if there is a domain name that's very recently registered.

And then there are some other things that registrars and registries can do that aren't necessarily the full nuclear option but there are ways to help stop that DNS abuse or mitigate it. And sometimes we might want

to lock that domain name so that it can't be, say, transferred to another registrar or so that it can't be deleted.

There's another time the registrar can update the nameservers so that it's being redirected. And this is something that's done often when there is a need to log traffic and help that. Quite often if, say, there's a malware or a botnet set up, law enforcement might want to know this information to see who is being targeted and who needs assistance. So again, it's not always something that just because there's abuse going on that the domain name is going to be shut off. There are times when it does actually need to be kept online.

And then another thing we do also is to escalate it. We can either send it to the hosting provider or send it to the registrant based upon what type of actual abuse is ongoing. Next slide, please.

One of the things we do need to consider here is whether the domain is compromised or not and whether there is collateral damage. And there are some examples in the advisory that we worked on that highlight this, so I'll just go over it at a high level.

A compromised domain name is one that was not registered primarily for the abusive purpose. And that's generally where either it's been hacked somehow or there's been a plug-in or a WordPress thing that's been exploited.

Of particular note, the Registrar Stakeholder Group created and announced at the Cancún ACIDTool.com. That's a free resource to look up hosts and other information about a domain name. The week after

the Cancún meeting we had a DDoS attack and were hacked and for some reason bad guys wanted to shut that site down.

So instead of that, I happen to be the one who maintained that registration, so instead of just shutting down that website—which it was still functioning even though there was a phishing link hidden on it—what we did was we worked with our host to remove that plug-in. We added Cloudflare, some other things in there to help mitigate and resolve those issues rather than just taking that domain name down.

So when you have a compromised domain name it's not usually the first approach to shut the whole thing down. Comparing that also with a domain name that was registered two days and now suddenly has a whole bunch of banking information on it or something like that. That's how you can compare and contrast. But again, these are very high level examples and every single case is different.

Another concern with just suspending a domain name completely is that stops everything for that domain name. So if it was domain.tld was the whole thing but they are, say, providing some resources down below that, so it would be sub.domain.tld and that's where the abuse was, shutting down domain.tld will shut down every single thing else on there.

So if it's the third-level domain, you would want to work more with that or the hosting provider or the registrant so that anyone else who is using that is not impacted by that. And then also registrars and registries do reach out to hosting providers and registrants to help them resolve those things. Next slide. I think that's it for me.

RUSS WEINSTEIN: Great. Thanks, Owen. I'll turn it to Leticia from our Contractual Compliance department who's going to talk through….

CHRIS DISSPAIN: [inaudible]

RUSS WEINSTEIN: Oh, yeah. My mistake. Q&A.

CHRIS DISSPAIN: We'll probably do some questions so that we don't get too queued up. Sue, do you want to?

SUE SCHULER: There is a question in chat from [Eleanor Stalick], "How can businesses prevent third-parties from maliciously registering domains that are confusingly similar to their IP aside from proactively registering every single iteration of a domain that might be mistaken as belonging to the business?"

OWEN SMIGELSKI: Hi. In addition to my role in the Registrar Stakeholder Group and Namecheap registrar, I'm a trademark attorney too. So I've been well aware of that concern. Quick answer is you can't. It's impossible to register every single iteration of a potentially confusing or lookalike out there in every TLD, ccTLD, gTLD, etc. But we do have these tools. There is the UDRP. There are other things if there are these things that are

being done, these abuse types, assuming that the amendments go through, that will be able to shut those down and stop them.

And again, it's also not just confusingly similar names. I've seen phishing attacks where the domain name has absolutely nothing to do with the trademark brand that's being done. It's random strings of letters and numbers or something and it's pretending to be a major bank or something like that. So it's impossible to stop crime like in Minority Report. You can't figure out that somebody is going to commit a crime in the future. But it's something that we can monitor and be aware of and adjust to when we find out about it.

SUE SCHULER: Okay, we have a few more questions. Steve, was yours sufficiently answered by Brian in chat? Good. Okay, we have a question from Jahangir Hossain, "Can we add the response time and policy for registrar after issuing DNS abuse reporting from registrant or other entity to mitigate the DNS abuse?"

RUSS WEINSTEIN: Thank you for this question. This is an interesting question. We've talked about this quite a bit. But DNS abuse is a case-by-case situation, and so trying to define single common SLA across the whole landscape is probably not the right solution that we came to. We came to the solution that the words that we used—"reasonable, prompt, timely"—provide the right amount of flexibility for both the contracted party and for ICANN as the enforcer of those contracts to make the correct business decisions.

And if and when those don't, when there's a misalignment there, that we can follow up appropriately through our compliance function. And Leticia will talk more about that in her section, but this case-by-case nature of DNS abuse is really important. Owen just describe a variety of different use cases, and having a single prescribed SLA proves rather challenging and we didn't believe that was the approach here to set a good floor.

SUE SCHULER: Okay, we have another question from Tomslin Samme-Nlar, "Could you explain a bit more about your rationale for replacing the term 'security threats' with 'DNS Abuse'? Do I understand correctly that the reason for this change was to allow for the inclusion of spam in the definition of DNS Abuse and to align this with SAC115?"

CHRIS DISSPAIN: I'll take this. Thanks, Tomslin. In essence there's a lot of work being done on defining what DNS abuse is and there are agreements in place. There's a framework that we've had since 2019. The DNS Institute is doing a heap of work, and that's using the definition of DNS abuse. There's an ICANN definition of DNS abuse in SAC115.

So it seemed to us logical to use a term that we could define rather than a term such as "security threats" which effectively could mean all sorts of different things. I'm not suggesting that the current situation with DNS abuse is closed in the sense of who knows what may come along. But right now, there is consensus that that is what DNS abuse means,

and it seemed to us to make sense to use that term since we all use it anyway to put these contractual amendments in place. Thanks.

Do we have any questions in the room at all? Yes, go ahead.

ABDALMONEM GALILA: Actually, the list of actions that could be taken by the registry or registrar against DNS abuse for one of the domain names, for example, actually this list should have to be [accumulative ones]. For me, as a registry at this side of the table or registrar I think this action is really good. But actually for the other side of the table as a registrant maybe it is end user or organization [leave] the domain name [for] the DNS I think it could harm me, harm my business.

So I could go for some [other decisions as issues]. So I think that if it will go for [accumulative] action against this domain abuse in order to make the domain name holder to take an action or be notified that his domain name is going to be some kind of [abuses] and make some harms [inaudible], for example, a registrar looks, registry looks, suspends, then go for other [inaudible] for the domain name. That's my idea.

CHRIS DISSPAIN: Thank you. Appreciate that. Steve?

STEVE DELBIANCO: Thanks, Chris. When we talked in Cancún I became aware from James and Crystal that of the two contract party houses the registrars seemed to confront the largest challenge getting approval of the amendments

especially when there are two dozen registrars in the room and a thousand or so out there and there's a high bar to get it.

So since Cancún or from this point forward share with us your assessment of the prospects for approval. How has it gone so far, and is there any way the rest of the community can be helpful? Thank you.

CHRIS DISSPAIN: Thank you, Steve. And I think we're going to come onto some slides that talk about that, and we'll explore that in a little bit more detail after we've talked about the draft advisory.

I do just want to add one thing before we move on to the advisory which is just those of you who were in the GAC session yesterday morning on DNS abuse will remember that Gabe Andrews from U.S. law enforcement gave an example where there was a phishing domain. Obviously, he didn't give the details, but apparently the name was very similar, etc., obviously a phish. It was a government website and very important.

And he gave an example of the registry saying that it wasn't their responsibility to deal with it and the registrar saying it wasn't their responsibility to deal with it but the registrar passing it on to the reseller and the reseller taking it down. I made the point at the time in the chat that that may well…that is obviously what happened. He said it. It clearly happened. But there's an awful lot of times that it doesn't happen. An awful lot of times when stuff does get dealt with.

But the key point is to understand that these amendments mean that will not happen. Well, it [inaudible] to be enforced, but the point is to

not do something will be a breach of the contract. This stops that because there is a specific obligation to take action, and that's the key thing. So I wanted to make sure that those that may have been left with the impression that that sort of things is commonplace, it isn't. And secondly, this fixes it anyway. Russ?

RUSS WEINSTEIN: Thank you, Chris. A good addition. Leticia, may I turn to you?

LETICIA CASTILLO: Thanks, Russ. Hi, everyone. My name is Leticia Castillo. I'm with ICANN Contractual Compliance. Next slide, please.

As Russ was mentioning before, ICANN Org produced a draft advisory to complement the DNS abuse amendments and provide guidance on the implementation and enforcement of the new requirements should they be approved. The advisory was developed with input from the contracted parties house to ensure there's a mutual understanding of the new requirements and how they will be enforced.

And you can check it out. It is published as supporting information in the public comment page, so please take a look if you haven't already. It also describes the new proposed requirements while reiterating that all existing obligations remain effective and will continue to be enforced and expands on key terms related to the mitigation actions that the contracted parties can take on or with respect to a domain name. Owen was explaining them before.

And we also included some examples of instances of DNS abuse and for each example the actions that the contracted parties can reasonably take to stop or to contribute to stopping the domain name from continually being used for DNS abuse or to disrupt or contribute to disrupting the course of the DNS abuse in relation to the domain name.

We were saying this before. There's no one-size-fits-all here. The circumstances surrounding each instance of DNS abuse do matter. This is why we included [illustrated] examples with specific facts linked to actions and how those actions were compliant according to the new proposed requirements.

We also explained how ICANN Contractual Compliance will conduct a comprehensive review of each case under these new requirements and what would be expected from the contracted parties to demonstrate compliance with any obligations if we initiate a case with them. The next slide. Thanks.

Explains that we will enforce these new requirements if they are approved through the processing of external complaints that we receive via our dedicated webforms but also through proactive monitoring and our audit program.

We will conduct a comprehensive review of all the information including complaints including records and also any other relevant available information that pertains to the case such as the data displayed in RDDS for the specific domain, DNS lookups to check the domain [inaudible] DNS, etc.

And any case initiated with the registrar or registry operator will include a list of what's needed from the contracted parties to the [inaudible] compliance with the specific and by when.

And we will generally expect an explanation from the contracted parties regarding the specific mitigation actions taken to stop or to contribute to stopping or disrupting, how those actions were prompt and reasonably necessary for the case at hand. And this includes any applicable explanation related to the disproportionality of actions and the possibility of collateral damage if that applies.

And if the contracted party does not take any mitigation actions because they determine that there was no actionable evidence for the case, we will also require an explanation regarding why and how they reached that determination and, of course, we will assess it.

And like we do today for [inaudible] allegations ICANN Contractual Compliance will publish metrics related to the enforcement of these new requirements if they are approved to keep the community informed.

This is all for the slides. Happy to take any questions.

CHRIS DISSPAIN: Do we have any questions specifically on the advisory at the moment? No, we don't.

RUSS WEINSTEIN: I think Steve had one.

STEVE DELBIANCO: I put it into the chat. I just wanted to ask that ICANN would readily receive and welcome comments on the advisory, not just comments on the amendments. But during this public comment period we may have suggestions for Org we respect to the advisory. And if we do those comments, is it solely within Jamie's shop to accept those or does that end up being something that the whole CPH agrees to? Thank you.

RUSS WEINSTEIN: Thanks, Steve. Great question. I think the focus of the public comment process is on the amendments. I think if you have helpful suggestions for the advisory, we're willing to listen. It is an ICANN advisory. It's not something that requires approval from contracted parties in order to move to the next step. We've been working on it in consultation with them, but it is our product and it's how we would enforce these agreements and how we understand them. So hopefully that answers your question. Jamie, I don't know if you need to add.

JAMIE HEDLUND: Yeah, so just two quick things. One, I would really encourage everyone to read the advisory. The textual changes to the amendments are fairly concise, but the [advisory] itself is 15 pages and it contains a lot of information about how we interpret the amendments, what the obligations are, and how we will enforce them. If you think it can be improved, we in Compliance are definitely open to that feedback. We just thought it made sense to include the advisory to try to give more

color to what the amendments actually require and how we'll enforce them.

STEVE DELBIANCO: And just one follow-up. Over time if it's discovered that the advisory itself can be improved, clarified, and given examples, Org can continue to evolve that document. It doesn't require this kind of a consultative process. You can improve the advisory over time.

JAMIE HEDLUND: We can improve the advisory over time. I think the bigger point is that over time we're going to get experience with these amendments and enforcing them and what we learn from that could go in the advisory but it would at a minimum be shared with the community.

STEVE DELBIANCO: Okay.

VOLKER GREIMANN: Yeah, that's exactly correct. I think the advisory is helpful for helping both us and the community understand what's meant by the new changes in the agreement, how we expect to live by those new requirements. And we also see that advisory as a living document that will evolve over time as we learn more. As we feel that certain parts of the agreement are interpreted maybe in a way that is not helpful, then the advisory can be changed to point in the direction that we feel is correct. And therefore, we expect that this advisory will become very helpful going forward as we live and learn.

CHRIS DISSPAIN: Thanks, Volker. The only other thing I would add is just to say that it is an ICANN document and nonetheless it has been a part of our discussions. And you don't have to be a rocket scientist to figure out that the CPH is comfortable with what the advisory says or rather than the negotiating team is comfortable with what the advisory says, otherwise we would have a problem. That said, let's be clear. We're about to start talking about the voting and how tight this is going to be. So we really do need to make sure that what we put forward has the best chance. I almost feel like saying take the win and let's pick it up afterwards and figure out what we need to do next. I just said it. Russ?

RUSS WEINSTEIN: All right, with that, let's go on to the process here. So next.

SUE SCHULER: [inaudible]

RUSS WEINSTEIN: Oh, we have more?

CHRIS DISSPAIN: So sorry, Sue. Carry on.

SUE SCHULER: No worries. We have a question in chat from [Hugo Arcuri], "Please, are there plans to make DNS more secure such as integrating blockchain technology to combat DNS abuse, spoofing, and other abuse?"

CHRIS DISSPAIN: No, and that's a subject for another time. But, John, if you'd like to comment.

JOHN CRAIN: This is John Crain, ICANN's chief technology officer. We are regularly looking at emerging technologies and how they can be used in the ecosystem, but that is not really relevant to this specific topic. Happy to take an offline question if you want to email me. I'm pretty easy to find.

SUE SCHULER: Okay, and then we have one other question from Brian King, "How do these requests for explanation and supporting records compare to what ICANN Compliance requests today under the 2013 RAA?"

LETICIA CASTILLO: Thanks, Brian. The request for explanation and records itself is not different. The process is not different. The obligations that we'd be enforcing are different. So currently there are no obligations to take steps to investigate and respond. If these requirements are approved, there's specific obligation to take mitigation actions with a target outcome of stopping or disrupting the DNS abuse. And this is what we're going to review if the requirements are approved.

CHRIS DISSPAIN: Is that the end of the questions, Sue?

SUE SCHULER: It is.

CHRIS DISSPAIN: Okay, super. So, Russ, back to you to go on to the next part.

RUSS WEINSTEIN: All right, so next. How do we go from here? These amendments are using what we call the global amendment process for the Registry Agreement and Registrar Accreditation Agreement. You may recall we've just done this as it relates to obligations related to RDAP, the registration data service technology, and implementing that technology in to the agreements, requirements for those into the agreements.

I'll take you through the process, but it requires a vote by all contracted parties. And we'll talk through that in a second. So important to recognize here also though is that not all registries are on the base registry agreement. Most notably .com and .net are not on the base registry agreement.

However, both .com and with the proposal out for .net there's a commitment from Verisign to ICANN to take the result of these global amendments for DNS abuse and incorporate them into the .com and .net agreements. And Keith will add on top of that when I finish. So I think that from a landscape perspective we have good coverage across the entire industry with these changes. And I'll go through the process in a second but, Keith, do you want to add on to that?

KEITH DRAZEK: Verisign has been sounded out. All right, that's better. Thank you very much, Russ. And, yeah, just to reaffirm, reconfirm, dispel any misperceptions or misunderstandings, Verisign is fully supportive of these proposed amendments to the RA and the RAA. Obviously, the Registry Agreement is the one that impacts us since we are not a registrar.

And I just want to note that I have been personally involved in the contracted parties negotiating team with ICANN. Samantha Demetriou my Verisign colleague is the current chair of the Registries Stakeholder Group, and we are fully supportive of these amendments and, as Russ noted, have committed in our letter of intent, in our existing agreements to take on these new terms as appropriate for our TLDs.

As Russ noted, we're still on legacy agreements, the registry agreement. We have not migrated to the base registry agreement as most others have. But we are committed to taking on these obligations and commitments at the appropriate time. So thank you.

RUSS WEINSTEIN: Thanks, Keith. Next. We talked about process. Essentially, the process is we have to identify a need a to negotiate. Actually, could we go two slides ahead? It will be easier to talk through it this way. We have to identify a need in the contracts, which the contracted parties did. We negotiated these changes which we've now brought to you all for public comment, and that's where we are now.

After public comment—could we go one more ahead, please? After public comment, we'll work to review those comments and provide a

summary and analysis report and decide if any changes are necessary to either the amendments or the advisory, as we talked about already.

And then we'll go into the voting process, and I'll talk about that in more depth, but the voting process essentially requires majorities of the registries and the registrars each independently to vote affirmatively yes to incorporate these amendments into their contracts. If we achieve those thresholds, it would go to the Board for consideration.

You can see a timeline up there of best case scenario how we get there from where we are today. Meaning if everything went as smooth as it could, we could have these amendments in place and effective by this time next year.

So how do we get there through the votes? I mentioned on the registry side—we can go back two slides—it's roughly a super majority, 66% or so. There are two metrics that we do to get there. And if we go back one slide, the registrars we need 90% of all registrars to vote affirmatively yes on these amendments in order to get them passed, which is an extremely high threshold. A lack of a vote essentially counts as a no vote. And so it requires a great deal on ICANN and on our colleagues and community members to help encourage registrars to participate in the vote and to vote hopefully yes for that.

Now it sounds overwhelming when you look at it on its face, but we've done it just recently which provides us good experience into how it worked, what to improve on. And also, we have recent contact with all of our registrars and have been preparing them for this.

So it's a challenge ahead of us. Steve, you asked earlier, what can you do as a community? I think it's really important to understand this context when thinking about what should go in these amendments, right? We talked about our objectives earlier. Our objective was to add a meaningful obligation to mitigate or disrupt DNS Abuse to both contracts. We think we've done that here. We think we've done it with great pace to bring it to fruition in five months and hopefully to bring it into real effectiveness within about a year's time.

I think what you can do is to support this process, to encourage participation, to encourage that let's take, as Chris said, let's align on what's important right now, what must be fixed right now, and what can be part of the community discussion for policy.

And so I'll let my colleagues join in on that, but I think that's the key.

OWEN SMIGELSKI: Thanks, Russ. I'm co-chair from the registrar side from the negotiating team, and one of the things that we kept in the back of our mind as we were doing this is this is not necessarily a negotiation for…it's not for the Registrar Stakeholder Group. It's for all of the ICANN registrars, and part of this is we need to get something that we're comfortable with. A lot of us who are here at ICANN are already doing these things. It's for those who are not.

But we still need to get the votes of people who are not here, and so a lot of what went into the wording as well as what's in the advisory was used as this is going to be an item that we can use to promote it. So it's

not just for the community but those that aren't here that we're going to try to get to vote.

So it was a lot of learning process with the RDAP amendment, but we've been working closely with ICANN on that as well as lessons learned about how we can improve this process going forward. And we're still giving ICANN that feedback, so I do hope that this next round, I'm not going to say it's going to be easier, but I think hopefully it may be less stressful. But, yeah, cautiously optimistic, at least from my side. Thanks.

CHRIS DISSPAIN: Okay, so I think that's the end of the slides. The floor is open to anybody to ask any questions at all. I can see Steve's got a question here for you, Keith, saying, "When you said 'at the appropriate time' would that be the time the amendment is effective as shown on the slide?"

KEITH DRAZEK: Thanks, Steve, for the question. Thanks, Chris. So typically we update registry agreements at the time of renewal, but I think it's a good question on this one. I think in our current .net agreement that's out for public comment there's a recognition that there's ongoing community work on this topic. And I will get back to you with a more concrete answer to your question, but the expectation is that as appropriate for the TLDs and on an appropriate timeline that we are committed to taking on those new obligations.

CHRIS DISSPAIN: Steve, do you have another question? Go ahead.

STEVE DELBIANCO: I recall in 2013 the RAA. The amendments that were done there were pretty well tuned to the new round if you recall, a lot of extra obligations. And I also recall that registrars had an incentive to sign up for the 2013 RAA since it was a condition to be able to market names in the new round. So refresh our memory on that. Did registrars vote on the 2013 RAA, or did they just simply adopt it if they wanted to sell new names? And if they did vote, how did that go? Thank you.

KEITH DRAZEK: So, yeah, you are correct. The registrars did not vote on that, and that was a requirement. In order to be able to sell the new gTLDs, you had to be on the 2013 RAA. And so for a while there were registrars on 2013, 2009, and also 2001 RAA. There was an incentive to move to the 2009 by reducing fees, but eventually all registrars are now on the 2013 RAA. And it's my understanding that they don't have a choice. If it passes the vote, it then becomes that for everybody. They don't have a choice to not be on it.

STEVE DELBIANCO: Right, but I was actually asking whether that incentive approach if necessary could be conceived in this instance.

KEITH DRAZEK: And I think part of that was we didn't want to overcomplicate everything. We didn't want to let perfect get in the way of the good. So what is something that we can do quickly to get positive changes in

there? That's something for discussing down the road. Should there be incentives and stuff like that? We can talk offline, but there's a whole host of issues and concerns, gaming the system, etc., stuff like that that can go into that. So this is something that's going to be an obligation on every registrar and registry.

CHRIS DISSPAIN: Volker?

VOLKER GREIMANN: Yes, and to add to that I think most registrars and registries that have agreed to this amendment that have been involved in the discussions that I've heard and not commented negatively on what we are proposing here is they believe that this is the right thing to do and we don't need a carrot to go with the potential stick that this includes. We believe that we want to raise the level of our responsiveness and responsibility that we're taking, and we feel that at least unless we don't get this passed there is no need for the additional carrot.

And to your question with the 2013 RAA, I think for us it's very important that all registrars come under this regime at the same time. That there are no hold outs of registrars that have their renewal date of their existing RAA five years in the future and that could hold out for that amount of time and therefore become a haven for bad activity. I think we need to make sure that any updates to the RAA are effective for all registrars.

And that's exactly why we, speaking as a member of the 2013 RAA amendment team or drafting team, we included this amendment

process in the RAA to ensure that we would not have to go the route of having a new RAA that becomes effective at different times for different registrars but rather have a process where the existing RAA becomes a more living document that evolves over time and that allows for a change that becomes effective for all registrars at the same time. That was very important to us at the time, and now we're testing this and hopefully it meets the requirements of the community. Thank you.

CHRIS DISSPAIN: Thank you, Volker, and very well said, I think. James, you're next.

[JAMES]: Yeah, I think Volker covered it. The whole design of the 2013 RAA with the amendment process is to synchronize the contracts so we didn't have these staged expiries and renewals. And the incentives are—look, I'm always in favor of incentives—but the goal here was to act quickly and not to tie this to something that's coming in three years or five years but to get the changes done quickly.

And there was a question in another session about what if a small registrar votes against. And just for clarity, if this passes, it immediately becomes effective on all registrars whether they voted for it or not. So it's not optional.

CHRIS DISSPAIN: Yes, Steve?

STEVE DELBIANCO: One small follow-up. I work in the world of politics, and sometimes you can encourage participation in a vote if it becomes clear that whether they vote yes or no, there's another wave coming by which they would have to adopt it anyway. So if there was an understanding that whether or not it's adopted immediately it will be a condition for selling any new names in subsequent rounds, something like that can just maybe nudge a doubter into participating and voting for it now.

CHRIS DISSPAIN: Interesting point for us to take back to our ongoing discussions, I think. We have ten minutes left if anybody else has any questions or comments. Happy to take them. Yes, question over here.

ANGELA MATLAPENG: Hi, everyone. My name is Angela. I'm new to this group. I'm from the ccNSO, but this is quite interesting. I've got two questions. The first one speaks to a couple of slides back. There's been mention on actionable evidence. So I wanted to know if there's any maybe reference to this. Would a registrar know what it means when you say actionable evidence? Is there a common maybe definition somewhere or maybe metrics that could help guide to say this is at least best practice where you can even have a least of indicators of compromises that helps?

And then the second one is on there was something on collateral damage. So I wanted to understand what would be the accountability that's faced by parties that do not comply. Are we looking into maybe penalties if those exist or if maybe we foresee those coming through?

Especially where DNS abuse then results in collateral damage which could have monetary implications. Thank you.

OWEN SMIGELSKI: Thanks for those two questions. The first one, actionable evidence, in the advisory my recollection there is a link to a document that the contracted parties put together which is about a guide to reporting DNS abuse. And there's some information in there about what types of evidence can help with that. I won't go into detail because it's all different.

And then as to the collateral damage, if a registrar or registry is not taking the action that's required to stop or mitigate or disrupt the DNS abuse, the consequence are ICANN can come after them. So that would really vary case by case, and I don't want to speak on behalf of compliance but there are obligations that have to be done and just can't be ignored. But again, for the collateral damage if, say, it's MySpace.com and there's some abuse on there, you don't necessarily shut down the entire site. You go after where that abuse is as opposed to that. So it's something that would vary case by case.

CHRIS DISSPAIN: Go ahead, Sue.

SUE SCHULER: From Kristina Rosette just to read this in. She wanted this to be on the record. "Apologies if I missed this point, and I realize this question was better raised in the first portion of the session, but will registry

operators be required to include in their monthly reports submitted to ICANN data about mitigation actions taken under these amendments assuming they're approved and become effective? Thanks." And then Volker did reply to her, "Currently, there is no requirement to keep statistics." So we just wanted to read that in.

CHRIS DISSPAIN: Just let Russ respond to that, Sue.

RUSS WEINSTEIN: Yeah, thanks, Kristina, for the question and Volker for your support on the answer. I think important to remember there are actually two different reporting requirements in the agreement. There are the reporting requirements in I believe it's Specification 3 or 2 which are two different sets of monthly reports. One around domain transactions is the basis of our billing system, and then there's one around activity reports. Things like how many RDDS queries or how many EPP queries they got in a particular month.

There's nothing about DNS abuse or abuse reporting in those reports. But let's not forget the requirements in Specification 11.3(b) which require registries to maintain reports related to this stuff. And so there we would expect it to happen. We don't collect those currently on a regular basis from ICANN, but they need to be available upon request from ICANN. Hopefully that clarifies.

CHRIS DISSPAIN: Thanks. And, Sue, do you have something else?

SUE SCHULER: Yes, we still have more questions. I have one from Mark Datysgeld, "Should members from the NCPH reach out to registrars we already use and ask them to consider voting yes? Would that be seen as a reasonable move?"

CHRIS DISSPAIN: Absolutely.

SUE SCHULER: I have another question from Kristina Rosette, "Will registry operators be required to include in their monthly reports submitted to ICANN…?"

CHRIS DISSPAIN: We've done that one.

SUE SCHULER: I'm sorry?

CHRIS DISSPAIN: It's the same question you've done.

SUE SCHULER: Oh, I'm sorry. Okay, I guess that was it. It was the same question. Thank you.

CHRIS DISSPAIN: No worries. Brian?

BRIAN CIMBOLIC: Yeah, thanks. Brian Cimbolic, PIR. And apologies for not knowing the ins and outs of the administrative process of this. But I guess from a transparency perspective will the names of registries/registrars that vote for or against the amendment be published somewhere just to see where people stand on the text of the amendments?

RUSS WEINSTEIN: I actually don't recall what we just did on the RDAP amendments. I know we did publish who had voted. I don't remember if we published directional. I think it's something we should talk about in this industry where transparency is such an important part of the things we do in this industry. Maybe it is appropriate to publish that, and maybe that helps encourage yes votes.

BRIAN CIMBOLIC: So just to re…I think that would be a good idea.

CHRIS DISSPAIN: Volker?

VOLKER GREIMANN: And to reiterate on that, I don't think we specify in our agreements the process of voting, how ICANN should go about it, what kind of publication and encouragement to vote there should be. So we are quite flexible in how we structure this. And having learned from the recent vote that we already did, I think that was perfectly timed to be a

learning experience for us to see how that went, where the problems were. We were able to identify a couple of problems that we could probably avoid this time going around the block and make it a much smoother and easier process.

CHRIS DISSPAIN: So I think we have another question in the chat. Go ahead.

SUE SCHULER: We have a question from Phil Marano, "Is there any intention to ultimately incorporate the advisory into the four corners of the agreement? There are a lot of helpful clarifying details in the advisory and it is great to hear everyone supports it. The advisory ideally could be incorporated by reference to help address otherwise ambiguous terms and help ensure the enforceability of these amendments."

JAMIE HEDLUND: The advisory is not part of the amendments. The advisory is an interpretive document, and it's intended to show how Compliance is going to—part of it is to show how Compliance is going to enforce the agreements. It was important for Compliance to be part of these negotiations to ensure that there was a clear understanding about what the obligations were and how they would be applied. So it is--I don't know that we have done advisories at the same time that we, in the past, with new obligations. But for a Compliance perspective it's very helpful for us to know that or to confirm that the obligations are clear and enforceable and that that understanding is shared not just by us but by the parties negotiating the agreements.

RUSS WEINSTEIN: Yeah, thanks, Jamie. Could I add one on that. I think also by not having those as incorporated by reference we gain the flexibility to evolve over time and learn as we talked about earlier. If it becomes part of the contract, we then need to go back through these voting processes versus having the ability to learn over time as we talked about to adjust and to make improvements. So I think there are big advantages to this being a complimentary document as opposed to a contractual one.

CHRIS DISSPAIN: Keith, go ahead.

KEITH DRAZEK: Thanks very much, Russ and Jamie. I was just going to say essentially what Russ said. And the really important point here is that on something like DNS abuse in this particular case it is a constantly moving target. And to hardcode an interpretive set of parameters or understandings or guidance into a contract would essentially tie ICANN's hands and contracted parties' hands in terms of being able to adapt and evolve and adjust to a constantly shifting landscape.

So good question, but I think where we are with this very, very detailed advisory—and again I would reinforce what Russ and Jamie said. Read the advisory if you haven't already. It is very, very good document. It has good examples. It's self-explanatory. But it is one of the things that can evolve over time. Thanks.

CHRIS DISSPAIN: Thank you, Keith. And we're at the top of the hour. Okay.

VOLKER GREIMANN: Sorry to keep you longer. One thing that we also discussed and that is probably helpful for the community to understand is that we had very deep discussions with Compliance about how they're going to enforce that. We chose not to include that in here because we feel that not specifying how Compliance will act on this will enable Compliance to learn new tricks to help registrars that may be lagging, that may be running behind the pack for whatever reason. We expect that a lot of registrars don't have experience with certain types of abuse because they've never faced them and that an educative approach might be better for Compliance than a punitive approach.

So one thing that we're hoping for here as well is that we are going to work cooperatively with Compliance. This is hand-in-hand as part of the community to see how we can best address this together, not against each other.

CHRIS DISSPAIN: Thank you, Volker. And so that's the closing comment, that Jamie is going to learn some new tricks.

JAMIE HEDLUND: I'm not that old.

CHRIS DISSPAIN: And with that, I'd like to say thank you very much, indeed, to everybody who came. Thank you very much to everyone who answered all the questions. Thanks to staff and everything, and we can close the meeting. Thank you all.

[END OF TRANSCRIPTION]