ICANN78 | AGM – GNSO CPH DNS Abuse Community Outreach
Sunday, October 22, 2023 – 1:15 to 2:30 HAM

SUE SCHULER: Hello, and welcome to the CPH DNS Abuse Outreach session. 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. Questions and comments will be read 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.

To view the real-time transcription, click on the Closed Caption button in the Zoom toolbar.

To ensure transparency of participation in ICANN's multi stakeholder model, we ask that you sign into the zoom sessions 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 Brian Cimbolic.

BRIAN CIMBOLIC: Thank you, Sue. Hi everyone. Welcome to the Contracted Party House DNS Abuse Working Group Outreach session. I'm Brian Cimbolic with

PIR. I'm also one of the co-chairs of the Registry Stakeholder Group Abuse Working Group, along with Alan Woods.

And next slide, please. Today we are going to go over the pending amendments both to the registry agreement and the registrar accreditation agreement to create a higher floor on DNS Abuse. So we're going to hear from several of the co-chairs of the working groups as well as some members from the amendments team. We're also going to hear an update on ACID Tool, which is a tool that is put out there by the Registrar Stakeholder Group. And we very much want to have this be interactive. There's been a lot of engagement amongst registries and registrars about these amendments, but we want to hear from the community and we want to save plenty of time for questions.

So with that, I will hand things over to Owen to walk us through the amendments. Owen, take it away.

OWEN SMIGELSKI: Thank you, Brian. My name is Owen Smigelski. I am the Register Stakeholder Group co negotiation lead, along with Catherine Merdinger over there. And I will be leading this part of this presentation.

Next slide, please. So what are the amendments? The contracted parties wanted to …DNS abuse is a big topic in ICANN now and we wanted to do some action that we could do quickly, which would not have to go through the whole PDP process. That's not to say that this wasn't something that came out of … It was just the contracted parties. This is based upon the GNSO Small Team's recommendations about how there could be some contract changes to help the contract parties

address DNS abuse. So the goal was to make some meaningful baseline obligations so that the contracted parties had to take reasonable, appropriate actions to disrupt or otherwise mitigate DNS abuse. So this was done within the ICANN processes and boundaries and remit and it was kind of a first step for subsequent action by the community.

Next slide, please. So the amendments focused on DNS abuse definitions that have been used within the community. It was cited in SAC 115 and it highlights several areas of things that are very clearly identifiable as abusive actions. And it's one of those black and white things as opposed to a gray thing.

So the first area that is covered is malware, which is malicious software. It can be installed from a website directly or on there. It's generally without your consent or you can click something. It can also be spyware, ransomware, a number of things on there. But basically it's bad software that's coming from a website in some manner.

Another type of DNS abuse covered by this is a botnet, which is where it kind of takes over computers either without permission or sets up a network of computers which then can infect malware and do other things there on behalf of a remote attacker.

Another one (and this is at least from my side) is I see a lot of in my registrar is phishing, and that's where an attacker is trying to get sensitive information from somebody, whether it's corporate information, log-on credentials to systems, financial institutions, bank accounts, things like that. And they can be sometimes done just via directly via website or sometimes these are also used through email and sometimes text messages or SMS. And then also phishing

campaigns can sometimes try and convince you to install software as well too.

Next slide, please. And the fourth main type of DNS abuse that are covered by these amendments is called pharming, and it's a little bit different than phishing but often has the same thing. Instead of modifying a website or utilizing a domain name, it is changing the DNS records. So it kind of redirects you. You think you're going to a particular website. It looks like that, but however it's been changing the name servers or something along those lines. So it is similar but technically different than phishing.

And then the final and the fifth area of DNS abuse covered by these amendments is spam. And it's not all spam because one person's marketing letter is another person's spam message. We're focused on spam that is associated with the four other types of abuse. Quite often that's a main point of delivery; to entice somebody to click a link or go to a website or something like that. So I would cover spam only to the extent that it is being used for those four other types of DNS abuse.

Next slide, please. So I'm going to speak just of the RAA because I'm on the registrar side and I will defer to a registry colleague when we get there. And we're focusing on the RAA first because generally registrars are at the front line with this more. We have a direct relationship with the registrant, so it's a little bit easier for us to act and get in contact with the registrant. We have the contact details, et cetera.

So the definition of DNS abuse is put in there. There's also change-to-request methods. Right now the RAA is very broad in terms of how abuse is reported and not very specifics. And then there will be required

action there as well too; the registrars will actually have to do something as the current wording is open to interpretation.

Next slide, please. Sorry, I just need some coffee here. So this is actually the, I would say, red line, but it's actually a blue line, I guess, of the changes to the RAA. And we wanted to very narrowly focus on section 3.18, which is the section of the RAA that deals with DNS abuse. There are other sections of the RAA that could have been touched, but we wanted something that was quick and narrowly focused and could accomplish this goal. So that's why the only changes were made to 3.18. I know some public comments that said they wanted other changes and edits elsewhere. Those are things for later on down the road to be considered, whether those would move forward or not.

So again, like I said, nothing was removed. So any obligations that are currently in the RAA, such as a registrar having to take action for illegal activity or a registrar having to respond to law enforcement requests for abuse, are still in there. They're not on the screen because that's in a different section. I think it's 3.18.3 now. So just realize anything that is already in the RAA that can already be done and dealt with is going to remain.

What we've done is increased what's in there. So we do say that the registrar needs to take response to DNS abuse, which is that fine term there. We include those in there and then we link to the SAC 115. Those were the exact definitions from SAC 115 on those previous slides that I went over.

And then also what it does is it does allow for a registrar to use a web form for requesting DNS abuse complaints. Quite often reports that are

received through email are not of the highest quality. Sometimes it just says “please take down this website” and that is it. There's no more information. They're slow to respond. Also sometimes if somebody is emailing you a complaint about an alleged bad domain name, sometimes it's going to be on a block list and it's going to go missing. So allowing the ability to provide that web form ensures that the registrar will receive that complaint in the format that is best for them and also provide the opportunity to provide attachments and things like that and to route it to the appropriate team as opposed to just an email.

In addition, it's going to require a registrar to confirm receipt of the report and there's additional explanations in an advisory which I'll get to later. So it doesn't exactly specify what the confirmation means, but it's just that the reporter will be able to track the fact that they submitted a complaint and then define it.

And then this section 3.18.2 specifies what the registrar must have to do and we're trying to make this as broad as possible, meaning that a registrar can take several different actions but making it clear that the registrar has to do something to disrupt or mitigate that. And the reason why we want to do that is because not every type of abuse is the same. Sometimes DNS abuse takes the form in a website or a domain name that is registered specifically for the purpose of committing DNS abuse. An example might be a squat or a typo of a famous bank's name or Facebook login XYZ or something along those lines. That is a domain name that was intended specifically for that purpose.

A large part of DNS abuse can be what we call a compromised website or a compromised infrastructure. And that's where somebody has a website that is being used for a legitimate purpose and for some reason a plugin is exploited or they get access to the password, they change some content. It even gets as obscure as they can hack the favorite icon that appears in the browser window. So there's a number of ways that sites can be compromised and the way you would approach that is different than doing that because I remember when I was working at ICANN Compliance once I saw a university's website had been hacked and there was a page or two on there and the appropriate response was not to take down that entire university's website. What you want to do is give that registrar the opportunity to contact the host or contact the registrar to make sure that is fixed and patched. So registrars generally only have one tool, registries as well: to suspend a domain name. We can't really just go and take down a file. We need to work with the registrant or the host in order to get that there.

And a fun example I give about why you don't want to take down those sites is at the Cancun meeting, the Registrar Stakeholder Group announced … or was this maybe it was Cancun or was it DC? We announced Acidtool.com, which is an abuse contact Identifier, which we'll talk about later. The week after we announced this, we were subjected to a DDoS attack. A plugin was hacked and it came down for a week or so. And the appropriate response was not for the registrar to take the entire website down because it was still usable to a degree, but to work to fix and patch and update and stuff like that and make sure that there was additional security. So ACID Tool is doing a lot better now

and we'll talk about that later. But that's just a real world example about how you don't want to just take down an entire domain name.

Excuse me, next page please. And now I will pass to somebody for registry stuff, Alan Woods.

ALAN WOODS: Thank you very much. Alan Woods, one of the co-chairs of the Registries Stakeholder Group, DNS Abuse … Working Group? Subgroup? I don't know. So yes, luckily I do not have to talk quite as much because one of the expectations in this entire process was to ensure that there was a synergy between the registrar and registry expectations. They needed to meet in the middle, make sure that we were working together, not in opposition to each other. So you'll see that an awful lot of the actual wording found in the registry amendments would be very mirrored of that which is found within the registrar amendments. So I haven't put up the actual wording. I'm sure you're all sick to death, those of you who've seen. [It's the natural words.] So this is just kind of a high- level overview of what were the changes.

So the first one is we added to our specification six, section 42, and we made a very slight amendment to Spec 11-3B which is one of the specs that most people would have in the past associated with the DNS abuse obligations on registry operators. But we found that new specification 642 was just a good place to put it.

As with the registrars we were given and we took a positive obligation to take an action. And that action was where there was a reasonable determination of DNS abuse can be made by the registry operator.

And just to clarify, I suppose the DNS abuse definition is also found now within the new registry amendments. I see Farzi has put in some comments in the chat room and to confirm, yes, it was mentioned in SAC 115. I was also one of the people who was collaborating with the SSAC on the creation of SAC 115 and it was used as a definition that has been used, it was referred to that wasn't necessarily defined in SAC 115.We need to make that clear.

However, for clarity within the contracts and making sure that this is something that is enforceable and readily actionable by both registry registrar and ICANN alike. It was important from a contractual point of view to have that clarity of a definition.

Another important aspect was the inclusion of the requirement of actionable evidence (again, Owen has talked about this); actionable evidence being ensuring and enshrining where due process, in the process that we are looking at … A lot of people will talk about things like the Digital Services Act in the EU, where it talks about non arbitrariness of action, and therefore having a link to a registry and a registrar where appropriate, taking action based on real evidence, an evidence based escalation in effect to ensure that that evidence supports that determination and supports that action. And it was important that we got that into the amendments to make sure that there was no arbitrariness in it and we enshrined due process.

The action, as I have put it, in inverted commas, is has to contribute to stopping or otherwise disrupting a domain from being used for DNS abuse. Again, that is mirrored language from the registrars and I do not need to go into that. But specifically, I think it is important for us to

understand that it is in that same vein. An action to suspend is not always the appropriate action to take. Therefore, we were giving that positive obligation to take an action that is appropriate in the circumstances.

And again, going to the last bullet point, that was the whole concept that was also enshrined within the amendments. And that is we must provide clarity as to why we believe that that action is reasonable. And this is about us making sure we have the proper audit trails and records, making sure that when an action is being taken, w we can show why in the circumstance that action was deemed the appropriate action. So in the amendments, you will see words such as "taking into account the severity of the harm," which is an obvious reason the circumstances of the case; i.e., what are the expectations? What was the circumstance of the abuse? Was it something that was compromised? Was it something that was potentially registered for an abusive purpose? And also the important aspect is the potential for collateral damage. And I know Brian, you're going to be talking about this later, but the potential for collateral damage is indeed making sure that our action does not do more harm than the actual abuse that is being perpetrated.

And that is really kind of the high-level of what the registry amendments and the raising of that floor that we have rallied around in effect in both registries and registrars.

Go to the next page. I think …

OWEN SMIGELSKI: So one other thing that was done in addition to the amendments which the contracted parties negotiated with ICANN was that ICANN Org, in consultation with the contracted parties negotiation team, drafted an advisory. And I'm not going to read the whole name because it's really long. We just call it the advisory. And what that does is that provides guidance a little bit more onto what is DNS abuse, potential responses to DNS abuse, and how that would impact ICANN Compliance investigations. This is not a binding thing. It's not part of the contracts, but it's intended to give some guidance on how ICANN and the contracted parties do envision this. I think it's like seven or eight pages. It's rather long. It took quite a bit of discussions. But I think it kind of gives some clarity and some more explanations about what is in there and what both the contracted parties and ICANN expect there it will be.

It also does give some examples on how registrars and registries can respond to certain types of DNS abuse complaints and how they could be actioned. So it kind of gives a little more clarity and guidance in there.

So this is intended to be envisioned as a living document. We're making some changes to the contract that we hope will go a certain way. We're not sure what it's going to do or what it's going to look like or how it's going to be in real life. So this is a document that we do intend to revisit periodically and to update and kind of give some more clarity and guidance to the community.

The link is there on the slide. Also, if you go look at the DNS abuse amendment page that ICANN has created, it's there along with all those other documents as well too.

Next slide, please. So I'm also going to put out a big vote out there or a big push to vote yes. I know there's some contracted parties in the room, some maybe who have not voted. There's some of us … We've got stickers. If you have voted, come up here. We've got lots of "I voted" stickers. Thank you ICANN for getting those for us. Some of us have more stickers than others. It's not a competition. We want everybody to get their stickers. So please do vote.

And we're also encouraging registrars and registries to vote yes. I know previous times we just encouraged them to vote. This time we want to encourage yes, because this is something that came out of the contracted parties, the Registrar Stakeholder Group and the Registry Stakeholder Group. We do want these to go through as a first step in tackling DNS abuse within the ICANN community. This will show that we do want to take meaningful steps to combat it. This will mean that every registrar and registry will have that baseline. And we also think that will reduce the likelihood of people outside of the ICANN community trying to take action to do DNS abuse. Sometimes it can be done better within ICANN, we think.

And a really big thing at least from the registrar's side is this will really help improve DNS abuse report quality, because, boy, before I went to a registrar, I just assumed that they got all the information they needed. And again, sometimes they will just come in and say, "Please take this website down," and don't even mention the domain name, which is somewhat helpful when you're trying to process an abuse complaint. So if we don't get this doesn't pass the voting thresholds, it will lead to delays in addressing DNS abuse, and then any future outcomes could be less predictable and what might come out of there further.

Next slide please. So for those who are contracted parties, just do know voting the way that ICANN works. Abstaining is not like the rest of the world. In the rest of the world, when you abstain, it lowers the voting threshold. That is not the case in ICANN. There is a voting threshold that's based upon for the registrars and registries, that it differs slightly. But if you don't vote, that's the same thing as voting no. So we really do encourage everybody (registrar, registry) to vote yes. An email should have been sent to the registrar and registry primary contacts from noreply@eballot.com. Just do check. It may have gone into a spam folder. If you haven't received that, ICANN will certainly help you sort that out. The voting period opened on October 9 and is open through December 8th, a 60-day vote. And so we do hope that everybody votes yes on that.

Next slide, please. So these voting statistics … I do apologize. This is as of the 21st. We actually have updated numbers from the 22nd, so you can go check. And we have them directly, as opposed to ICANN's website, which is a little bit of a delay of them processing that. So you can see the voting totals there. They've gone up a little bit since I don't have that directly on the screen here, but this is going a lot quicker than we'd hoped. There was a lot more [yes] votes happening at this phase than we've seen with the previous, the RDAP vote that we had … earlier this year? Late last year? I don't recall the specific timing of that.

So that link there is to the global amendment page, and I think ICANN will be updating the vote totals weekly on there. Russ is nodding yes, so every week they'll be up there on there.

Next slide please. Again, if you need any help for those kind of things, please do contact globalsupport@icann.org or if you have a direct contact with your ICANN account manager, they can help you out there as well too. And I know ICANN definitely wants to help. If you don't hear anything from them, reach out to any of us. And we can help as well too, because we do want to push this over the finish line and get these approved.

Next slide. So this is just a general timeline of where we are, and we are in stage four where we're voting. Again, the first was the negotiations, and then we had a reasonably fast negotiation period, which we were all kind of surprised by, but it was a very good collaboration between ICANN and the contracted parties. There was a public comment process, and then ICANN did a really good job of going through and reviewing and summarizing the public comments. And again, that public comment report does that because there were some important points raised by certain members of the community, some concerns, and those are discussed and addressed in there. So assuming that the vote goes ahead, then the next thing would be the ICANN Board to vote and then the effective date. So in theory, I think it would be around this time next year ish when the effective date would come in. I don't recall specifically on that, but that's kind of the general timing on that.

Next slide. Am I turning this over? Okay.

ALAN WOODS: Back to Alan Woods then, to kick this one off. So now that we've gone through what the amendments are, the process, everything that's going through, we want to take maybe a second or maybe even a few minutes to bring this back away from the legal language, specifically, and give it

a little bit more insight into what this actually means for the people who are not contracted parties. What is this going to mean? What is the actual impact? So we're going to do what we kind of coined little vignettes of little aspects of what the words within the contract amendments mean to us, practically speaking, and what you can look to.

So the first one (and I'm going to deal with this one) is the concept of the actionable evidence. Now, of course, in setting up the registry agreements, I went a little bit into this, so you won't have to listen to me too long in this one, but to maybe restate because it is vitally important, the concept of having actionable evidence has come from an awful lot of experience about reports that both registries and registrars get or reports that are made not directly to us but are just existing out there in the ether of the internet where it is saying "X is bad. X is abusive," without any reasoning, any understanding or any evidence. And there's an expectation that there is an action against that on us.

So we're given "Here's a domain name. It's bad. Take it down." So it was very important for us to set that expectation. Not only as a registry and a registrar do we need to make sure that we are taking the right action in the right circumstance, but when that action is being taken, that it is attributable to some form of evidence, that there is a reason for us, that we can record and demonstrate and display and show that we have taken an action that is reasonable in that circumstance, based on the evidence that we see.

And I use the word (and I don't use it lightly): we need to ensure that there is due process. A lot of people expect action without

understanding that what we need to do is pay attention to not only the rights of our registrants, but also the rights of everybody else. We need to be above board, transparent, and making sure due process is taken into account.

So a good example would be in the phishing example, where we are able to show that, for a domain that has been (and this is in the advisory as well) been flagged for phishing, we see the elements of that phish. We can see where there is an attempt to use a trust to obtain some form of data that is not being and should not be shared with a third party; so a login, a password, a bank account, a bank account login, things like that. If we have evidence that shows that, then that it makes it easier for us to make an assessment in that circumstance as to whether the action (perhaps it's suspension, perhaps its escalation) is not appropriate in that circumstance.

So it is important that we set that balance at the floor, that for us to even consider taking an action, there is evidence that supports us taking that action, and that should be recorded. And that is in the interests again for the registry, the registrar, the registrant, but also for ICANN in helping to enforce these expectations which we welcome.

That's kind of all about actionable evidence.

REG LEVY: This is Reg Levy from Tucows and co-chair of the Registrar Stakeholder Group DNS Abuse Subgroup. And I'm going to make some comments about what reasonable action, what reasonable mitigation, might mean. There have been some concerns about the fact that this is

undefined, and “reasonable” is in fact a legal term of art. That means it depends. It depends.

So the problem with defining an action is that everybody has a different business model. Tucows’ business model happens to be a reseller model. And so very often the action that we take is to forward the report to our reseller, to give them the first option to make a fix. That is reasonable. It isn't that we are not doing anything. It's that we're doing something that maybe another registrar wouldn't do because they don't have that intermediary between the registrar and the registrant. For other registrars who have hosting companies, they might be able to take direct action to remove the content from the website in a way that another registrar, that my registrar, simply doesn't. So the reasonable action is unfortunately undefinable because in each case it's going to depend on the actual situation.

Owen raised an issue where there was a compromised site and simply suspending the domain would have taken a university completely offline.

So in each case we need to look at the situation and make a decision and each of your registrars needs to do the same. And when ICANN comes to you and says, “What did you do?”, you can say, “I acted reasonably,” and then explain what it was that was done and why that was reasonable in the case that you took that action.

And now I'm going to turn it over to Brian for compromised websites.

BRIAN CIMBOLIC: Thank you, Reg. I think we've actually probably covered how the amendments deal with compromised sites, noting that a registry or registrar isn't forced to take a clumsy action in that case and suspend the entire domain name. And I think that at a higher level, that kind of goes to a thread in the amendments. While we all wanted to do something about DNS abuse (the negotiation teams were committed to that), we wanted to make sure that it wasn't just an action; it was the right action. And so the compromised websites is a great example of that. It's not that we're required to suspend the domain name, but we are still required to do something. We're required to notify, perhaps the hosting provider, do something where you get closer to the registrant to notify them, to the reseller, to take some step to try and help.

And so for those registries and registrars that are thinking about these amendments, please do take a look at the advisory because that's the common thread. It's not just that we're doing something, it's that we really try to understand and approach DNS abuse with all the nuance and thought that it deserves.

With that, I think I hand it back to Reg for webforms.

REG LEVY: Thank you, Brian. And I just wanted to reiterate that the registrars have an explainer about webforms, which I'm putting into the chat right now, that you can check out if you have concerns. If you are here in the room and are not a registrar but are a potential reporter and you have concerns about web forms, we have some tips about how they can work properly.

The reason that we use webforms is because it gets the request to the right place. So I know that I use webforms for phishing, which are different web forms than the ones for malware because each of those is going to require perhaps a different set of evidence, actionable evidence, as Alan was discussing earlier. And my team will look at the evidence in the context of the report so it gets to the right team. If you just send it to an email address, who knows where it goes.

And also the web form can help craft the report in a way that is helpful for us because there are some cases where someone thinks there is a phishing attack, but in fact there is not an actual phishing attack. It's just a typo squat. So the forms are very useful for registrars to make sure that we are getting reports in a correct form. That makes it easier for us to act quickly. If we have to go back to you and ask for additional information, then the DNS abuse continues to be implemented before we can take action.

And then I'm going on to raising the floor. Just a reminder that these contract amendments are not intended to change anything. They have not taken away any rights or any obligations from the way that the contracts initially read. They are raising the floor and allowing ICANN the tools that it said that it needed to enforce the contracts against contracted parties that don't do anything about DNS abuse in their namespace. So going back gently to the reasonable action conversation, you have to do something, but what you do is going to depend on your business model, on the domain name, on your relationship with the registrar, and on the type of abuse specifically reported.

And now I don't actually know what's after the next slide or who I'm turning it off to.

Oh, and this is me again. Next slide, please. Okay, so we have acidtool.com. It is excellent. We have lots of people using it, which is great. It gives you contact information for the hosting provider. So if you have a concern about content, this tool will help you get that complaint to the right party.

It has information about email, so if there is unsolicited email that is not technically spam under the DNS abuse definition, you have the information to contact the email service provider directly.

It also has information about the creation date, which can be helpful in terms of whether or not the DNS abuse that is occurring on the domain is recent and perhaps the result of a maliciously registered domain. Or if the domain itself is old and the abuse is recent, there might be a compromised site situation happening.

To the extent that registrant data is available, it will be displayed here. To the extent that reseller information is available, it will be displayed here. For us wholesale registrars, you're always welcome to start at the reseller if that's something that you'd like to start out with, because that's what we're going to do.

And of course, it will also provide contact information for the registrar. But note that very often the contact information will say, “Can you please use our forms?”

So that's acidtool.com. I am saying it again in a public forum. I anticipate that we will potentially have another DDoS attacked attempt

in the coming weeks, but generally speaking, it is up and running as long as we haven't talked about it recently.

I'm going to hand it over to—what?

UNIDENTIFIED FEMALE: [inaudible] explaining.

REG LEVY: There are explainers available at those links above, which I will ask Sarah to copy and paste into the chat. Thank you.

About how to use it. We've had requests from ALAC to explain how to use the ACID tool. It is just a website and you put in the domain name. You do have to put in the domain name itself. If you prefix it with dub, dub, dub, or any subdomain, if you put in HTTPS or if you put any file path after a slash, it will fail. So just put the domain name in. And it works for ccTLDs and gTLDs alike.

Okay, now I'm turning it over to Owen for some stats. Thank you.

OWEN SMIGELSKI: Thank you, Reg. And so just before I read the stats here, I just want to say, while we did have the DDoS and other attacks in March, we've since moved to a more robust platform and other sorts of stuff in there, so we should be able to weather other stuff there. But we've got a dedicated team now to work on that, so we're more responsive in that, so hopefully we can promote it without bringing it down next week.

So these are the stats since June. I'm only doing June, because, again, we had the DDoS attack in March, and we changed hosting providers and server and stuff like that. And the data from them included the DDoS access. So those were kind of messed up. But as you can see, in June is when we first transitioned. And since then, every month we've had over 4100 unique visits; that is, per IP address or whatever, how it's being counted. And then the number of total visits are showing that a number of those people do when they come to the site generally at least more than one search as well, too. So it is something that is getting quite a bit of traffic there. So we're pushing sometimes almost 10,000 searches per month. So we can certainly (fingers crossed, because it's hosted by Namecheap)be able to take more usage on there. So I do encourage anybody to use that. And as Reg said, it does give you the hosting provider information in there. So it's a lot more than just doing the RDAP lookup, but it also does include that as well, too. That's it.

BRIAN CIMBOLIC: Okay, I think with that, we're actually ready to move into Q&A. So please do me a favor, especially those of you in the physical room, because I can't actually see you. If you can, please raise your hand in the Zoom room, but I'll try and keep an eye over my shoulder if someone comes up to the mic.

We got one coming.

UNIDENTIFIED MALE: I'm very sorry for hovering. Many apologies. I'm not on Zoom right now.

BRIAN CIMBOLIC: Go ahead, Mark.

MARK DATYSGELD: Thank you. Mark Datysgeld, speaking on my own capacity as a small business owner from Brazil. So thank you again for leading this effort. And having just come out of the IGF and looking into all the processes that are going to come still next year and the year after that, there's certainly a lot of appetite from other actors to start, regulating our industry or start acting upon the domains, the names and numbers space. They are certainly not making it subtle. So the approval of this vote would definitely be a very good affirmative step towards signaling to them that, "Yeah, we have this together. Don't worry, this is under control."

So thinking about this from a broader perspective, this is very important not only for DNS abuse, but I think for the industry as a whole. It's a signal that we care because the impression that they seem to have is that we don't have a grasp on this, but we do. We know we do. We just need to get things together, right?

So just giving some extra encouragement for us to think about the broader picture outside of just the abuse aspect but on showing that the industry is strong and ready to react and ready to get a handle of itself instead of needing external forces to come down on us. So thank you very much.

BRIAN CIMBOLIC: Thanks very much, Mark. First of all, I think I can speak for us that we collectively agree and think it's a point very well taken.

I also wanted to specifically thank you and the work of the GNSO Small Team on DNS abuse because while this was a bilateral negotiation, really the path was laid out by the GNSO Small Team. So really, thank you again for the great work of you and the team.

I see Keith has raised his hand. Keith, go ahead.

KEITH DRAZEK: Thank you very much, Brian. Hi, everybody. Keith Drazic with Verisign. And I want to +1, Mark on your comments just now and also Brian's comments in response. I think what you said is spot on. And I think that your work on the GNSO Small Team was a really positive thing that helped frame and guide and reaffirm in many ways the work that we've done here on these contract negotiations. So thank you.

I did want to just take the opportunity to sort of reassure everyone who may be listening and may not have been following along that these bilateral contract negotiations between registries, registrars, and ICANN on the registry agreement and the registrar accreditation agreement are the first step in this ongoing conversation on DNS abuse mitigation within ICANN's, remit within the role, responsibilities and capabilities of registries and registrars.

So going back 18 months or 20 months now, whatever it is, as we started talking about initiating these bilateral negotiations and creating new commitments and new obligations to mitigate DNS abuse, as has been described, we acknowledge that we are in a multi-stakeholder community, that we rely on the bottom-up consensus based policymaking and the GNSO policy development processes to ensure

that we have community input and the full range of views of community input when it comes to developing new policies. And we are committed to that. As contracted parties, we are contractually obligated to take on new requirements that come out of a policy development process. And so we are certainly open to, and I guess in some ways expect, that these conversations will continue. It could be that we have a follow-on PDP at some point.

And just wanted to let everybody know and just reassure everybody that this was the first step. This was what we could do bilaterally with ICANN quickly and that would deliver meaningful and material new requirements that will change and enhance our ability to mitigate DNS abuse. We think that's a very positive thing, but it is only the first step. So thank you very much.

REG LEVY: Thanks, Keith, and I appreciate both of those comments. Just briefly, on the first one, we are very pleased by the results of this and are looking forward to everybody voting yes. If anyone in the room is a registrar and is not yet sold, please don't hesitate to ask any of us. Happy to talk you through it and make those explanations and make you more comfortable.

BRIAN CIMBOLIC: Thank you, Reg. Thank you, Keith. We have Steve and then we have Farzi in the queue.

Steve, go ahead. Thanks, Brian.

STEVE DELBIANCO: Steve DelBianco for the Business Constituency. And as you know from the comments we filed on the amendments, [we're] very appreciative and supportive. We had some suggestions that may not have been accepted, but our sentiments were very clearly in support of this direction.

I also was in Japan last week with Mark and many of the other people here where the United Nations is gearing up for a two-year roadmap, as they call it, leading to the United Nations General Assembly, fall of 2025, a resolution on where they want to go for the next phase of UN involvement on the Internet and also, specifically on domain name system.

I don't think that audience will be appreciative enough of voting results and approval of amendments. And in order to demonstrate results, I can't always go to Graeme's reports because the statistics may reflect not a significant reduction, simply because there are more bad actors involved.

So the real question is this. What do you think you can do once it goes into force to track the requests that come in, the reports that come in, as well as the actions taken within whatever bounds privacy law would permit? Detailed data would be so instructive for those governments to understand that their role here contributed to actual tangible action against DNS abuse. Thank you.

BRIAN CIMBOLIC: Thank you, Steve. So I would note that registries, at least in the RA, have to maintain statistical reports of whatever action is taken that actually exists in the current agreement without the actual requirement to refer to the registrar. So registries at least will be in a position on a TLD-by-TLD basis to see what effect this has had.

But point well taken that there needs to be some sort of more collective measurement, collective support, of how these amendments get administered. And in the end, was there a meaningful reduction in DNS abuse? Because that's the goal here.

I see Crystal has raised her hand. Is this in response? Okay, Crystal.

CRYSTAL ONDO: I just wanted to point out also that part of the RDAP contractual amendment that went through not too long ago as well was giving ICANN the tools to use registry data to map registrations to registrars in a way that they aren't scraping who is and running into throttling issues. So ICANN will also be tracking this on a per registrar basis, not just on a TLD basis. So I think we can expect strong data out of their OCTO team as well. So I think all of us would love to see meaningful, tangible results from this effort.

BRIAN CIMBOLIC: Thank you, Steve.

We have Farzi and then Graeme and then Michele. Oh, actually, sorry, I guess Farzi … Just one second. Graeme, was it in response to Steve?

GRAEME BUNTON: I've got two, but I'll respond to Steve and then get back.

BRIAN CIMBOLIC: Okay, great. And then, Farzi, we will come right to you.

GRAEME BUNTON: Sorry. This is Graeme Bunton from the DNS abuse institute. Steve was referring to our compass reporting that we put out monthly which tracks rates of DNS abuse over time. We think right now that we're very well positioned to measure the impact of the amendments. So key figures for that from our perspective right now are going to be not just volume of DNS abuse, but actual mitigation rates and time to mitigation. And my hunch is that we will see mitigation rates increase and time to mitigation decrease. We're already collecting that data. We're figuring out how to make it available and we're really going to commit to providing that to the community over time. After the amendments come out, you should see a blog post from us about how we're planning on doing this in the near-ish future. Thank you.

BRIAN CIMBOLIC: Thank you, Graeme.

Farzaneh, go ahead please.

FARZANEH BADII: So one of the issues that I see multiple times in these outreach sessions is … So the contracted parties in a way is doing something innovative.

Now, I might not agree with the whole process and how it was done, but you're doing something innovative. And I think that we should be careful in how we handle receiving comments about this issue and also how you respond to the comments and just like, arguing that these are like bylaw … And I know and understand that you are here to take comments, but then in these outreach sessions and when you receive comments, I just feel like we just come here, we provide you with comments, and then you go and do your thing, which is fine, but we still need to see what's going to happen to those comments. And I got it from Keith's comments that this is like an ongoing thing and after the negotiations are done and bilateral amendments are done, then we can continue the conversation.

But I'm just saying that instead of having outreach sessions that are more like about telling us what you're doing, I would have preferred to also have an outreach session that tells us how you manage the comments that you received on the bilateral negotiation and the text and how you're going to tackle some of those concerns. And it doesn't matter … Sometimes you can just say, "Hey, we cannot address these concerns at ICANN. We can go and address it somewhere else." And that would be enough. But I think that it would be great to hear responses to our comments in these sessions.

And another thing that I just want to disagree with Steve is about the importance of the UN. And I think that we should take as much time as we need to tackle these issues. DNS abuse has not gone up, and if we want to make the political issue, that's another thing. But the UN at the moment … I think that the registries and registrars can just monitor the processes, but it is not a very urgent matter to look at, to be honest. And

a lot of the issues don't even relate to ICANN, per se—the ICANN mandate. Thank you.

BRIAN CIMBOLIC: Thank you, Farzi.

Russ raised his hand, hopefully in response. Russ?

RUSS WEINSTEIN: Yeah. This is Russ Weinstein from ICANN, and it's me and my team who are responsible for the negotiation on the ICANN side. And the public comment process is our process, the ICANN process.

So, Farzi, I take your comments on board. I think we attempted to provide all of that rationale. We didn't necessarily bring it here, given timing. We thought that was sort of behind us at this point. We were already into the voting stage, so it didn't quite make sense to be talking about the comments we received and how we analyzed those and provided input back to the negotiation on those.

But I recognize we didn't do a big public session about those. We do a lot of public comment sessions at ICANN. There's probably, at any given time, five or six things that are open for public comment, and we put out public reports about how we summarize those comments, how we analyze them, and what, if any, changes we made to the documents. We did that for this one. I think we categorized the feedback received from the community into five or six key themes and addressed those one by one, both at the comment level and thematic level.

So please, we can drop that link in the chat here for you. We can talk about how we do comments going forward in terms of, if we do another negotiation in the future, what the right way to address the comments with the community is if we need to do outreach sessions and that sort of thing. But our standard practice is what it is, which is we do analyze the comments and produce a summary report that's open to the public. So if there's anything you found in that report that wasn't satisfactory, please feel free to come talk to me about it. Thanks.

BRIAN CIMBOLIC: Thank you, Russ.

Sam?

SAM DEMETRIOU: Thanks, Brian. This is Sam Demetrio, Chair of the Registry Stakeholder Group. And just to add on to what Russ said, I also want to call back to what Brian and Alan and Reg set up at the beginning, which is that from the beginning, before we initiated the negotiation process for these amendments, we always viewed these amendments as the first step in a larger process. Keith just spoke to this as well.

And so we did, as Russ very cleanly just stated, consider all of the public comments that came in. And we really pushed ourselves to ask the question of did the amendments, as we drafted them, still meet the purpose that we were trying to achieve, which was to set this kind of new bar for the entire industry to take mitigating action, appropriate mitigating action, on well-evidenced cases of abuse.

And we discussed amongst the team and our stakeholder groups that the answer to that was yes. and that all the other great content that was provided, all the great feedback that came in through the public comment process, was exactly why this is something that we want to work on with the community going forward.

So this is just to really reiterate our commitment as contracted parties to continue to engage in that outreach. We can always make these sessions better and I'm happy to take feedback from Farzaneh and anyone else on how we can.

We're also talking about using our respective CPH working groups on DNS abuse to do more outreach and engage with more parts of the community more frequently than we have been in the past to get this kind of feedback, to get this input, on how we as a community can tackle this topic and continue to move the ball forward as it comes to addressing DNS abuse.

So I just wanted to make very clear that this is something that we're not signing as done just once these amendments get over the line and that, yeah, we're definitely committed to working with the community on this going forward.

BRIAN CIMBOLIC: Thanks a lot, Sam and Russ.

Michele, over to you.

MICHELE NEYLON: Thanks. I was just kind of picking up on something Steve was asking and I think it's something he's asked a couple of times in the mean. I think essentially what he's looking for is a greater level of transparency. And I suppose part of the problem with that is when you look at phishing, you can have many URLs but only a single domain. So I think in some ways some of that data probably will never really match up because you're comparing apples to oranges in some respects. A single domain could have millions and millions of URLs, so you're only going to see one domain was acted upon, as it were.

But I think something that might change things in terms of the level of transparency would be the GSA, because we do have transparency reporting obligations there. Speaking on behalf of my own company, I mean, we've never published a transparency report, though we have been collecting a lot of the data, though, as I've said many previous occasions, most of the requests we get from law enforcement and others is not related to domains. It's usually related to IP addresses.

But I suppose the thing is that you will see more data flying around. But ultimately, statistics are always manipulated. People will push them around to fit whatever it is that they're trying to get to. So I'm not sure exactly if you'll get what you're looking for.

BRIAN CIMBOLIC: Go ahead, Steve.

STEVE DELBIANCO: Thanks, Michele. I appreciate it. This is a case of "audience plus purpose drives the design." [Audience, governments, the UN purpose

]convinced them that our industry, our multi-stakeholder model, actually gets results. Therefore, the design isn't transparency. It's performance data, performance statistics that are digestible. Too much transparency will completely overwhelm that target audience.

So the idea is reporting. And I honestly think that Graeme's DNS Abuse Institute does the best job of high-level reporting. But in reporting the statistics, you can't reliably say that mitigation statistics are up if we don't know if those mitigations were connected to reports that came into the DNS abuse system and exercised through the new contractual obligations.

So I think that if it's possible to compile statistics on how many reports came in and how many of those reports resulted in mitigation actions that stopped it. That may or may not connect with the data that Graeme is tracking, because he's tracking it now, and you're not even accepting these reports yet, but knowing that the purpose of this is to demonstrate performance, it doesn't have to be perfect. Whenever possible, the performance should expand and aggregate to include the number of URLs under a digital domain, which were in fact, responsible (better still, the number of phishing attacks that had been going on on a daily basis on all of those URLs). If that data were available, the performance of a takedown of a mitigation looks better and better in the eyes of the target audience. So it's more of good marketing and communications than of just transparency. Thank you.

BRIAN CIMBOLIC: Thank you, Steve.

We have Graeme next in the queue. Graeme?

GRAEME BUNTON: Thanks, Brian. I had a couple other pieces, but I'll bring a piece back around the measurement of abuse and something that we're very thoughtful of, which is that focusing only on rates of mitigation is difficult because different types of abuse have different outcomes that they should have, especially as it relates to compromised abuse reports where mitigation at the DNS is inappropriate. And so you need to be able to bifurcate those abuse reports and then measure mitigation rates for malicious only, work that we're engaged in right now but is difficult to do. And so be cautious when you're looking at abuse reports and measurement that's not making that distinction.

A couple other pieces that I wanted to add, mostly for the registrars in the room, is that we operate and anybody who has abuse reports that they want to get to registrars. The institute runs a free service called NetBeacon that tries to provide a simple conduit for abuse reporting that takes abuse reports from anybody who has them and gets them to gTLD registrars.

The forms that we provide via NetBeacon are embeddable and/or you can use our API if you would like to take advantage of the enrichment and standardization that the platform does. So if you're struggling with figuring out how to get those forms in place, please come talk to us. We're happy to help you with that. Again, there is no charge for any of that.

One of the other pieces that we're working on right now is reporting abuse directly to hosts simultaneously to registrars so that we can begin to close the circle in a way that has yet to be done in this space and I think is going to be extremely powerful. So if you're interested in that piece of abuse reporting, either as a reporter or a registrar, please reach out. Let's talk. Thank you.

BRIAN CIMBOLIC: Thank you. Graeme. One thing, just coming back to something that Steve said, is I did just want to note that while the contractual amendments obviously aren't in effect, a lot of us, especially around the table, are already doing this. So when you talk about accepting reports, so many actors in this space are already really diligent and meet the level that's set forth in the agreements. The effective bit with this amendment is just making sure that everyone else lives up to their end of the bargain too. So I just wanted to note that.

Sophia, please?

SOPHIA FEND: Hi, everyone. Sophia Feng for ZDNS. And first of all, thank you to the [inaudible] working group for drafting this amendment and advisory documents, which, as I think personally, is very important and helpful for the industry to grow more healthier as we are a Chinese registrar. And according to the official crime rate report by China, the crimes related with DNS abuses rose by 300% and consist of 70% of all crime that happens within the Chinese mainland.

So I do think we do have shared responsibility here as a collaborative group of registrars and registries to act on these DNS reports.

And just a question probably for the registrar and registry side. And as mentioned in a revisory, the appropriate mitigation action to stop or disrupt an instance of DNS abuse will vary depending on the specific circumstances. So the appropriate amount of time to investigate and take actions will also be varied, making it very impossible to probably prescribe a fixed amount of time for action to consider as prompt. So is there a threshold of processing time to define whether a registrar's behavior is prompt or, maybe in the further advisory where there will be also contractual compulsory to define what will be appropriate time of [p]rime? So that would be my question.

BRIAN CIMBOLIC: I see Russ has raised his hand respond. Russ?

RUSS WEINSTEIN: Sophia, thanks for the so. I think in the advisory, what we tried to do was identify several examples of instances of an abuse report and examples of how the registrar or registry would respond to that abuse report, including the time they took to do that investigation and response, and give examples of where it would be found to be in compliance most likely, and really noting that these are really contextual situations, and so the examples are only as good as the detail in that example and not necessarily a universally applied threshold.

So I think the way it's going to play out is that reasonableness will be held for ICANN to determine based on the complaint we get and the information we get back from the registrar when we do our investigation. And ICANN's committed to making sure that those are valid complaints, that they went to the registrar first, that the domains exist, they're under your sponsorship (and if Leticia or one of my other Compliance friends are in the room, feel free to correct me), and doing the thorough, valid assessment that it's a valid complaint worth passing on to the registrar to get feedback about what they did and how they did it. And then a reasonableness determination will be made from there. So I think there's not a clear bright line, and it's going to be a learning process, too, for the industry as a whole.

BRIAN CIMBOLIC: Alan, go ahead.

ALAN WOODS: Thank you very much. I just want to add that I suppose that one of the things that we are going to have to grow together on as well is making sure that we get good at record keeping as well when it comes to dealing with these things. So I completely agree that having reasonable thresholds might be important, but also having reasonable records of why you made a decision in a particular abuse and why it took that long or took that short is also going to be vitally important information so that when ICANN gets that complaint or when they're doing an audit under this, they will be able to readily get that.

And I think we need to just increase … And this is about transparency. This is about statistics as well. It all melds into one [so] that we're able to provide that level of detail so that we can all move the bar forward.

OWEN SMIGELSKI: just kind of following up, also, the advisory does take into consideration that not every registrar is the same as every registrar and not every registry is the same. Some registries are for specific industries, some are larger, some are smaller. There's new gTLDs and legacy. There's a lot of varieties of registrars. My goodness, when I joined a registrar, I thought they're all the same. But no, we sell directly to customers. Tucows uses resellers. There are corporate registrars, there are registrars that focus on domain names that are caught after expiration, and stuff like that. So trying to get together examples that work for all of them or could apply to all of them was a difficult task. But it's not comprehensive, it's not everything. There's a lot of flexibility and stuff built into there, understanding that there's a lot of different business models and structures and local requirements and stuff like that as well too. And I think that document can evolve over time to reflect those changes. Thanks.

BRIAN CIMBOLIC: We have Michele then Ashley.

MICHELE NEYLON: Thanks. Just kind of going back to this kind of thing, I think some people seem to be laboring under the myth that this is suddenly magically going to change things dramatically. And I think you're going to be kind

of disappointed because most of the larger operators are already doing a lot of this. The ones that are problematic are the outliers. So I don't think you're going to see a huge change overnight.

What would be interesting to see would be the ones who were doing things like when they got a report of something involving a domain that [was] on their creds, but if it wasn't pointed to them, they automatically closed the ticket and they were able to get away with that. That, I hope, is what we will see—those kind of companies.

UNIDENTIFIED MALE: [inaudible]

MICHELE NEYLON: You're fixated with breach notices. Okay, fine, you can be fixated with your breach notices. I never agree with you.

I think it's going to be interesting to see what will change, but I don't think you're going to see some kind of magical difference overnight because most of the larger players are already taking action. If GoDaddy is taking action, Tucows is taking action, Google, a few of the others [in general behave], then it's not going to change anything overnight.

SOPHIA FENG: I just want one thing. As a [copper] registrar, as we are practicing these mitigations, what we find out is a lot of DNS abuse website links are changing from time to time. Maybe in five minutes it will be [inaudible] for website and then in next an hour it will be a malicious website again. So that's how we're going to do it in terms of the data collection. And

also how can we track the behavior of those websites and link? And that would be a much bigger questions there.

BRIAN CIMBOLIC: Thank you, Sophia. I just want to briefly also respond and maybe respectfully disagree with my Irish friend in that I don't think that … Don't get me wrong, I'm not naive enough to think that these amendments are going to pass and then DNS abuse is solved. But I think that they will have a meaningful impact potentially right away. You're right. All the big actors are doing responsible things for the most part. But there are pockets of registries and pockets of registrars with an outsized footprint when it comes to DNS abuse. And so for the first time, they are going to be contractually obligated to really "do" something about it.

So when we talk about sort of the actors not at the table, those sort of old cliches, for the first time, ICANN Compliance is going to have clear tools to really do something about those actors with outsized footprints on DNS abuse and force them to change their ways. So that's my own two cent.

We have someone behind me. Bertrand, please go ahead.

BERTRAND DE LA CHAPELLE: Good afternoon. This is Bertrand de la Chappelle from the Internet and Jurisdiction Policy Network. Two quick points. One, what is being attempted here is both to create the floor, as has been mentioned, but also to progressively improve the workflow of notification management of the notices and action upon notices.

And here I want to support what Graeme was mentioning regarding the accessibility of a new platform and a new set of tools for reporting abuse. And this is a direct answer to the fear that a certain number of actors may have that it will create an additional burden for them. The purpose is here to raise the floor, but also to lower the barrier to managing the reporting. That's one.

Quickly, the second one is, as I wrote in a Circle ID blog a few months ago after Washington, this is a litmus test for the ICANN community in both directions positively because if this is adopted (and I strongly encourage all the actors to actually vote favorably), this will be a very strong message to an external community both inside, to the Governmental Advisory Committee, that this community is willing to take its full responsibility and only its responsibility because it doesn't have a responsibility for absolutely everything. This is a narrow scope. This is dealing with very specific issues. And it is to say there are things that the DNS operators can and should do and things they shouldn't do.

But towards the external world, without necessarily worrying about the UN in general, there is a message that is if this organization doesn't reach the threshold of voting to adopt this, this will not only reflect badly on this community itself, but it will have a huge impact on how ICANN is being perceived externally.

So I want to really emphasize, as somebody who's been from the outside and came into the ICANN community, to say be mindful that if this is not passed, it is not only going to harm the community itself. It's going to harm ICANN because it will be too easy for a lot of actors externally to say, you see, if they're not even able to accept this, then

they cannot pass any policy that is meaningful. So I really encourage this well balanced effort to pass and to couple it with the new processes for reporting that people are working on.

BRIAN CIMBOLIC: Thank you very much, Bertrand. I appreciate that.

We have three minutes left if anyone has one last intervention before we break.

Not seeing any. I think we can wrap. Thank you very much, everyone, for participating—oh, sure. Sorry. Actually, we do have one last one. Sarah, please?

SARAH WYLD: Thank you. I want to say a big thank you to all the members of our negotiating teams from both the registrar and registries. You've done a lot of work and I really appreciate it. Thank you.

BRIAN CIMBOLIC: Hear, hear. And with that, I think we can end the recording. Thank you so much.

[END OF TRANSCRIPTION]