ICANN77 | PF – GAC Capacity Development Workshop on DNS Abuse (2 of 3)
Sunday, June 11 2023 – 13:45 to 15:00 DCA

JULIA CHARVOLEN: Tracy, this is Julia. We're ready when you are.

TRACY HACKSHAW: All right, everyone. We're back. I'm going to start with a quiz. Just one question. Let's see who has been paying attention. All right. So, the last session, it was said that since 2019, the GAC has filed a total of how many public comments? In the last session, since 2019, it was said that GAC has filed a total of how many public comments? The prize, see those notebooks I gave you here, the public comments on DNS abuse will automatically fill out if you get it right. I see a hand, two hands. Anyone else? Let's see. Who knows? Who knows? So, I saw Zeina first.

ZEINA BOU HARB: 32?

TRACY HACKSHAW: 32. That is incorrect.

ZEINA BOU HARB: Incorrect?

TRACY HACKSHAW: Oh, my goodness. Egypt.

ABDALMONEM GALILA: Yes. This is Abdalmonem. I think if I remember well, Benedetta said that it is 7 per year, I think it's around 23.

TRACY HACKSHAW: 23?

ABDALMONEM GALILA: Yeah.

TRACY HACKSHAW: Incorrect.

ABDALMONEM GALILA: Yeah. Sorry.

TRACY HACKSHAW: All right.

UNKNOWN SPEAKER: Was it 33?

TRACY HACKSHAW: 33. That's the correct one. Wow. You win the prize. Okay. Here's another one. Hang on a sec. All right. Of course, I'm killing some time

for GAC members to come back in, in case you wouldn't realizing. What was the highest number of public comments filed topic? Which one?

ZEINA BOU HARB: ICANN Governance.

TRACY HACKSHAW: ICANN Governance. And how many were there?

ZEINA BOU HARB: 15.

TRACY HACKSHAW: Oh, my goodness. Excellent. 15. Followed by what's the next highest topic? They were equal. All right. So, the next highest two topics then? Next highest two topics? I've got a hand there. Yes?

UNKNOWN SPEAKER: One is the New Round of the gTLD, Then the other one is like something with like registration data.

TRACY HACKSHAW: WHOIS and data protection matters. How many were they?

UNKNOWN SPEAKER: And the is number is six, right?

TRACY HACKSHAW: Six. Exactly. Followed by?

UNKNOWN SPEAKER: Oh, I don't remember that.

TRACY HACKSHAW: Followed by? Paying attention, taking notes. Current TLD policy was four, and DNS abuse, two. Which brings you to my segue into this particular topic. So, welcome back to all GAC members in the room and online. Good evening, good day, good night, good morning. And as you're back in the room now, as you can see we have a full table, a full house ahead of us. So, it's very, very interesting session lined up.

What we're going to be doing now is discussing the substance of the issue, DNS abuse, and what I would like to do is introduce us all to the starting two speakers, our colleagues from the Public Safety Working Group, PSWG. Gabe. Not me not say necessarily. Gabe from the United States and Chris from the UK. And they will introduce us to the overarching issue of DNS abuse, what it means, why it's important. And then following that, I will hand over to my colleague, Susan, who will do the introductions of the rest of the team. All right? So, let's go. DNS abuse. Go ahead guys. Let's move.

CHRIS LEWIS-EVANS: Thanks, Tracy. Hi, everyone. As Tracy said, Chris Lewis-Evans. So, I work within the National Crime Agency and also a co-chair of the Public Safety Working Group. And then, Mr. Gabe.

GABE ANDREWS: Gabe Andrews. I am a member of the Public Safety Working Group and a law enforcement officer in the United States.

CHRIS LEWIS-EVANS: Perfect. I mean, we can move on to the next slide. Brilliant. So, what we're going to do is recap over some statistics that we showed to this group last time in Cancun. That doesn't mean you can go to sleep straight away. And then we'll go over some case studies and then say why the DNS abuse is important. The statistics that we've got are really hard for us to collect, so we will only be updating them every year. And then just a small call out, that if any other country has any other statistics, then please feel free to give them to your PSWG rep or to one of us directly.

So, the first slide here shows an increase in the reported type of crimes that we're getting from the public within the UK. And as you can see, whilst the sort of malware side stays fairly equal, it's the hacking and social media and email compromise that is a definite game. And that also contributes to the total number increasing. And I think it's fair to say that generally, cybercrime is one of the most underreported types of crime that we receive as well. So, by no means is this the full extent.

So, from those statistics you saw on the previous page, we also break it down into what was one of the causes of that. And within business breaches, the data breaches, a large percentage, so 80% have identified phishing as a cause for that breach. So, you'll quickly see that that links up very nicely with a definition of DNS abuse that's agreed by all parties.

And then just for some scale and some numbers, 800,000 reports of fraud and fraud related to cyber aspect or cyber-enabled fraud and £2.35 billion loss and 80% of that loss is cyber-enabled. And as with that previous slide, phishing has been one of the key enablers for criminals to be able to initiate that attack. So really linked to DNS abuse and a massive impact on the UK and its economy. And then on to the next slide and on over to Gabe.

GABE ANDREWS: Okay. And then from a US perspective, and I want to reiterate my colleague, Chris' offer, if you have perspectives from your own nations, if you have friends and colleagues in law enforcement in your own nations that can bring statistics here, we want to hear from places other than just US and UK. We want to incorporate that as much as possible. From the US perspective, we often collect complaints from victims via our Internet Crime and Complaints Center, IC3.gov. These are the stats from the last five years that I showed in Cancun. Just as a refresher. Last year, we got just over 2000 complaints a day.

We would look at the category of the complaints. We don't see DNS abuse as a category of crime that's reported to us. We don't track it that way. But we do see phishing as one of the categories that we put into a bucket called phishing. And if you look at the amount of crimes that are

reported by categories over the last five years, these are the top five. Phishing is by far the most commonly reported crime. And as Chris just said, phishing is both something that is universally agreed upon within ICANN circles as being DNS abuse and it's simultaneously one of the most common vectors that bad guys use to cause all sorts of additional downstream crime.

CHRIS LEWIS-EVANS: And then over to me. So, we heard in the first session about some SMS phishing and I just want to prove or go through a case study where that was used as an attack vector. So, the UK received reports that a victim's social media account had been hacked and carried out an investigation on that. The victim said that they were asking for more passwords, for more access to their accounts and loss of all their normal social media accounts, so Snapchat and Instagram, etc. We were able to identify the suspect and found that they had history of hacking social media and carrying out social engineering attached to that.

And on doing several warrants on his address, we found I think it was about 11 phones, all used to carry out the SMS phishing different numbers to maintain different victims and mass amount of phishing on all of those devices. We'll go on to the next slide, please. So, you'll see from here this is an extract from one of-- Sorry, Tracy.

TRACY HACKSHAW: We're going to be asking questions throughout. So, I hope that's all. People will be going to be asking lots of questions throughout. So, Chris, you've mentioned SMS phishing, and we spoke earlier about the

idea of mobile phishing, SMS phishing, smising, wild phishing, is there a difference and what is it? And is it related to the DNS abuse, all of them?

CHRIS LEWIS-EVANS: Not necessarily. However, so one of the good things, bad things about SMS phishing or Smising or whatever you want to call it, as we now all have smartphones, we all have portable computers with us. They are made to make going to places, clicking on things as easy as possible. Normally, that means some of the protective advice that you would give to someone that's on a computer to protect themselves from that, doesn't really happen. And also, on a phone, you tend to be very reactive. You don't think about what's going on, you'll just click something, see what comes up. That's generally how people use their mobile devices.

So, in an SMS phish, it could be send some money to this bank account. Is that DNS abuse? No, not at all. So, they're trying to do it. But in a lot of cases, as is the case with this one and the bottom chat window, there was a link provided that utilizes a domain name. So, in this case, this was a compromised domain, but in some cases, it could be maliciously registered domain. And in which case, 100% DNS abuse has been used to commit further things. So, there's definitely a differentiation between those but a lot of the time with these attacks, they have embedded domain names that want you to click on something to do something else, whether that's to download malware or to extract passwords out of you, but all of those where it has a link to click on

where it's using the domain name system to fool you into clicking that, 100% DNS abuse.

Perfect. That answers your question? Brilliant. So, that pretty much goes through that slide. So, you can see a bit of social engineering going on. The first two, the victim actually asks for a link. A link is provided. This this one, I've obviously redacted parts of it because it is a compromised domain. But you can see how believable it is for the victim, they would want to click on it. And if we go on to the next slide. So, this one's a bit small because we were trying to get a lot of content in. But they were then supplied with a page that tells them to log into their Snapchat. They're sort of expecting that because they've said they've got images on their social media, they've been extracted and put somewhere else. And then they are extracting those and using it extort them even further or to get data from the—So, there is numerous reasons.

So, in this case, there was two aspects to the DNS abuse side. One was that compromised domain, which were able to contact the host to say you have a compromised domain. You want to fix that. So, that's on a host base. And then on the right-hand side of the screen, you have a phishing service. So, this is a website that is set up just for creating phishing pages. So, on that front, that was domain that is just for phishing, which is criminal. So, were able to take that down, citing DNS abuse on that front. So numerous cases there. And obviously for us as an investigator, even finding out who uses that site, we're able to then stop further DNS abuse from happening. So, there's a lot of investigatory stages there, where we rely on the WHOIS and also the

ability to take stuff down or suspend it. And on to the next slide, and over to Gabe.

GABE ANDREWS: Okay. Here's a different case study. This is something that we had to deal with maybe four weeks ago. This is a real domain, but you'll note I redacted the portion in the gray box there. I'm hiding the name of a software vendor that provides secure login services. That's when you log in to a portal for, say, your employer. It's noteworthy that this particular login portal was for my own employer, the US Department of Justice used this this vendor. And beneath this, here's a phishing domain that I've also redacted, where the redacted portion is identical. Even if I've hidden it, take my word, it's identical.

This was a domain that emulates. It looks just like the real domain above. This is a phishing domain that is targeting the collection of login credentials for Department of Justice employees. This is a non-trivial matter from our perspective that we had to contend with. You can imagine your own departments of justice and your own prosecutors in your nations the kind of information that they have to protect and the impact on your own criminal justice systems if that kind of information was let loose due to collection of login information.

So, let's take a look at this phishing domain in particular. You can see here WHOIS information, that's registered data information associated with the phishing domain. And like before, I've redacted some of this. Everything in a gray box, I've blocked out intentionally just to not identify the registry nor registrar. But within this data, I as an investigator can easily identify the registry and the registrar to make an

abuse complaint. I can also identify that this domain was registered on May 11th. That's the creation time for this domain. We caught it within 24 hours of being registered.

And so, our complaints went to the registrar, the registry, Cloudflare. You might not be familiar with them. They provide security services and so forth to companies and so that's why their IP shows up. But we identified Cloudflare, and then they helped us identify the host of the content. And we made notification to the host as well, all within 24 hours of the domain being registered. This is a best-case scenario for a victim that's identifying an ongoing attack on their systems and trying to notify the various parties that can actually take action to help.

And so, in the summary effects, we have a domain that looks almost identical to the important login portal for a federal agency. We have the software vendor that we know is being targeted in an ongoing fashion for phishing attacks. The domain is just created, it has no history of legitimate use. This is purely created for this mission attack in our view. And you have the coming from an actual federal law enforcement agency that's part of the targeted entity. And so, we were optimistic that we could take some swift action to alleviate the threat.

I see Bertrand here in the audience conveniently. I'm going to call out. At the last ICANN, he mentioned that there's a limited number of options that a registry or registrar can take in response to an abuse complaint. And I think that he called out that what I call suspension is also called a hold and when the registrar holds it, it's called a client hold, when a registry takes this action, it's called a server hold. It suspends the domain and prevents it from going anywhere. It makes it

safe. And were hopeful that's the action that could have been taken. What actually happened is we made this abuse referral. It came in, let's think, the 11th was a Thursday, thus our referrals were on a Friday. This unfortunately happens a lot in the world of cybercrime. The bad guys have learned that doing bad stuff on the end of a work week often buys them a whole weekend.

So, what happened then was Cloudflare took immediate action to add an interstitial kind of a pop-up warning to anyone visiting this site, "Hey, this is probably really bad and you need to be extra careful". And really were very appreciative that Cloudflare took that immediate action to help mitigate the harm. We heard back from the registry on a Sunday actually, so kudos to them. We're grateful that they're responding to us even on the weekend. But unfortunately, the response came in the form of, "Well, as you know, we don't host this domain, we're not the registrar, and thus we're not in position to act unless you provide a court order." They did not offer to take action with this registry hold that we were hoping for.

The registrar responded a day later in the work week, on the 15th on Monday, that, "Hey, we're merely at the registrar. We don't control use of the domain, but we'll notify our reseller." Which kind of begs the question, why didn't I as the law enforcement immediately notify the reseller in this instance? And if you look at the WHOIS information, there is no field for the reseller in this information. This has been a topic of GAC advice in the past that we've suggested that reseller should actually be in the WHOIS records to help with this exact scenario of trying to immediately notify the parties that can take action. Unfortunately, this was how we learned that there was a reseller. And

so, there's another 24 hours then of communication going from the registrar to the reseller asking for additional help.

Again, the registrar has a lever that they can pull, called a client hold in this case, that would suspend the domain. But again, they're asking the reseller now to take action. Right about this time on the 15th, I recalled and I made a reminder to my colleagues. There's this thing called NetBeacon stood up by the DNS abuse Institute that helps triage abuse complaints. Please make sure that something is submitted there too, and that was done on the 15th. I don't know if that was critical to causing the next action that happened or not. It certainly didn't hurt. But then on the 16th, we were notified by the registrar that the reseller did delete the domain. And so that was four to five days after the registration and the initial report.

This is a mixed result I would view. I think that we viewed this as the best use case. The most clear instance of targeted phishing targeting a very important system in which case there would have been very minimal risk associated with suspending the domain while action is taken to investigate. And unfortunately, we did not achieve that outcome. It's still better than it could have been. It could have been no one did anything, and that's not what happened. Eventually, the reseller did delete the domain. But for clarification, for those of you that are perhaps not very familiar what that means in in security terms, that means the domain is deleted from the record, and anyone can come back and pay $10 and re-register it, which doesn't always happen. Maybe it could happen. I don't know. If it happened in this case, after it was deleted, but it's not quite the same ideal best-case scenario of suspending the domain as we had hoped.

And so, all of that I guess this calls the importance of having GAC advice to such things as why the reseller information is important, why we expect there to be action taken, and what kind of action I think really is most effective in combating a threat versus not.

TRACY HACKSHAW: We just need to wrap this section up. So, as I'm hoping that maybe in next two minutes, we can wrap this up.

GABE ANDREWS: Copy. I think we're almost done too. We'll go through this very quickly then. So, in this case, I'll just very quickly hit this. Why not get a court order? Court orders are great tools for investigating things after the fact. In my agency, it takes 2 weeks to 30 days to get one, not a great tool for mitigating harms in real time. If the domain is suspended by a registrar or registry, is it still dangerous? No. Done. Dead. Killed. If we acted at the host level, as we also tried here, and the host deletes the content, is the domain still dangerous? And the answer there is all too often it still can be. And this is just a repercussion waiting for it to click. Of the fact that the domain can point anywhere, any number of IPs hosts across the world, you can have two, a dozen, a hundred, a thousand. As long as the domain still resolves, it can still be a threat.

Thank you. And here's the closing takeaway. Phishing as we've both discussed is DNS abuse. It's the top reported Internet crime to my agency, and it enables, as you heard from Chris, a wide variety of other fraud and crime. 80% he said, of fraud is associated with phishing as the initial vector. And when we ask for swift action to be taken against

maliciously registered domains, we ask because it can have such a big impact on DNS abuse and, by extension, on cybercrime. Next.

CHRIS LEWIS-EVANS: And this is the last slide and it's just a recap on some of the prior advice that is important to DNS abuse. So, considering we're running out of time, I will let you read those at your leisure, but I think the big one is the six safeguards at the bottom to refresh yourselves on. And thank you very much.

TRACY HACKSHAW: Thank you, Gabe and Chris. And I'd just like to pause here, see if we have any questions from our GAC members who have been listening. Any questions online? Let's have a look.

JULIA CHARVOLEN: Tracy, we have a hand up from Nigel.

TRACY HACKSHAW: Nigel.

NIGEL HICKSON: Good afternoon. Nigel Hickson, UK. Thank you so much. This is always incredibly valuable. And the reference back to the Beijing communique is also pertinent, I think. The amendments that have been drafted on contracts, the draft amendments. In your view, how far do they go to

meet some of the concerns that the GAC has previously identified in this area, not least in the Beijing communique? Thank you.

TRACY HACKSHAW: Perhaps, I think, Nigel, that question is going to feed directly into the next session. So maybe we could thread it through, right? So, I would suggest we hold unless you have a very rapid answer.

CHRIS LEWIS-EVANS: I was going to say we've got ICANN presenting just on that fact. Maybe, Nigel, if you repeat that question after that, we can both answer. It would be great.

TRACY HACKSHAW: All right. Excellent. Yes. Are there any other questions related to the substantive DNS abuse topic? Yes?

GEMMA CAROLILLO: Thank you. Gemma Carolillo, European Commission. First of all, really congratulations for the excellent presentation. A question concerning the case study, I would say, that Gabriel presented this last. It seems that the appropriateness of the action is key, but also the speed. How much do you think that the clear chain of information between all the actors involving, including the hosting providers is key in reducing the time to action? Thank you.

GABE ANDREWS: It's a good question. Thank you. Very quickly. I think it's essential because when we're trying to make abuse notifications, if the people that we have information for in the WHOIS system, the registrar and registry, are not themselves willing to pull the levers, then we need information for those who are. And if that's the reseller level, if that's whatever we as an ecosystem are deciding is the appropriate place for that decision to be made, then they need to have their contact information right there so that they can receive the first notification of abuse and not waste time. Given that especially when these domains go live, it's usually used immediately.

I don't know when the first phishing messages were going to be going out with this particular domain, because we don't know necessarily if they're being sent by email, there was an ongoing campaign where there were even phone calls being made to employees and this domain was being conveyed over the phone. When you're responding in real time, you don't necessarily have all of those facts, but what was presented, I would still suggest was sufficient for action, and sufficient for immediate suspension pursuant to further investigation. And whoever has to make that call, we need to be able to call them, simple as that.

TRACY HACKSHAW: All right. Thank you very much. And in the interest of time, I think we'll have the other questions come in in the next session. So, if you have any further questions, please take note of them and let's have them in the next session that will start now. So, I'm going to toss to my colleague Susan from the United States government who is going to

introduce our next panel. And thank you very much, Gabe and Chris from PSWG field, wonderful inputs. And please stay there because I'm sure that more questions are coming in the next session. Thank you. Susan?

SUSAN CHALMERS: Thank you, Tracy. And hello, everybody, good afternoon, after lunch. Hope you had a nice lunch. As discussed earlier, the focus of today's session is really the primary focus is on the public comment process and how the GAC would like to go about that, but now we are delving into subject matter of the next public comment that we'll be focused on. And so, we're very fortunate to have folk from ICANN org, ICANN Compliance, the Registry and the Registrar stakeholder groups to walk us through the proposed amendments. So, thank you to all of you. If you could just introduce yourselves as you take the mic. Much appreciated. Thank you.

RUSS WEINSTEIN: Sure. Thanks, Susan. Hi, this is Russ Weinstein. I'm with ICANN. I'm in the role of GDD accounts and services. My team is responsible for all of our contracts and our relationships with the registries and registrars in this industry in the gTLD space. I also lead ICANN's organization-wide DNS security threat mitigation program and where we have a regular meeting across functions to discuss issues and topics related to DNS security threats and DNS abuse and things that ICANN can do in the ecosystem to help combat those.

So, this particular project has called to both of my roles within ICANN being the responsible for our contracts as well as responsible for furthering our combating of DNS security threats and DNS abuse. So, with me today, we have Jamie Hedland from Contractual Compliance, we have Owen Smigelski from Namecheap and the registrar stakeholder group. We have Chris Disspain from Identity Digital in the registry stakeholder group. We have Ashley Heinemann, the chair of the registrar stakeholder group, and Sam Demetrio, the chair of the registry stakeholder group.

This effort is a really cross-functional within ICANN and collaborative exercise with the registries and registrars who will tell you the story, but came to us and volunteered to step up and increase their obligations in their contracts relative to DNS abuse because it's a real problem and they recognize that just like you do. And so, within ICANN, this was something that was highly supported at the Board and CEO levels and was a cross-functional effort from myself in the GDS team, John Crane and his Octo team, Jamie and the Compliance team and our legal team was deeply involved as well. The product we developed with the collaboration of the registries and registrars I think really will be a big, meaningful, important step for this industry. I think it addresses a lot of the concerns Gabe and Chris put on the table, and will be a real advancement for this industry.

So, with that, we'll get into the agenda. Chris is going to provide some background about how we got here, what we are trying to accomplish. I'll talk through the detail of the contracts and help you explain what we did accomplish. Owen will talk a little bit about DNS abuse and that will build on some of the sessions you've had leading up to this in the

webinars to help build on the capacity. And then we'll talk a little bit about what the amendment procedure is for the contract, where we are and what it really takes to amend a contract, because I wish it was as easy as just agreeing with these guys. But it's a little bit more complicated than that is everything in ICANN is.

So, with that, let me go to the next slide. So, again, where public comment has opened. We did this-- For ICANN really quick speed, we really began negotiating in earnest in January and were able to complete those negotiations and deliver this for public comment in the end of May. Here, so less than five months' time to bring this to fruition. What you'll find is changes to the Section 3.18 of the Registrar Accreditation Agreement. In the registry agreement, you'll see the changes predominantly in specification 6, Section 4, and then a small change in specification 11 3(b).

In addition to those contract changes, we've also worked to develop what we call our draft contractual advisory. That provides more explanation and context to what these terms and provisions mean. We provide examples of how they would work in practice. And hopefully, it's a helpful supporting document. The advisory itself isn't really out for comment. The comment is about, I think, the best thing you can do is direct your comments, more focused on what the amendments say than the advisory, because the advisory will adjust if there's necessary changes to the amendments. But the comment periods open through July 13th, and we're here to help you guys think through that and provide good input from the GAC, which is really important. Next, I think we'll go to Chris. We'll talk a little bit about how we got here.

CHRIS DISSPAIN: Thanks Russ. Good afternoon, everybody. I'm Chris Disspain. Nice to see you all here. My job is to give you just a very brief overview of the of the background to how we got to this stage. Many of you will know that DNS abuse has been a topic of discussion that ICANN in the GAC and various other for quite some considerable time. And the contracted parties have been working on this issue also for quite some considerable time. And in fact, probably the first clear step was taken in 2019 when the DNS abuse framework was published and signed onto by significant number of contracted parties. But last year, some contracted parties got together and started thinking about what more what we could do. And I think it's very important to get clear what the goal was.

The goal of these contractual amendments is not to provide best practice. I'll explain why in a second. The goal is to provide a floor, to provide a higher level of floor in the RRA in the contract so that there is a baseline from which ICANN Compliance can enforce any policy in respect to matters that are covered by DNS abuse. And so, we decided that we felt the best way of dealing with this was twofold, one is to deal with the contractual amendments, and then to look at a series of very narrowly scoped and focused policy development processes to build upon the work that we will have done putting these amendments into the contracts.

There is an acknowledgement that, in respect to DNS abuse, there is a role for the policy and there is a role for the community in making that policy. But we felt that the critical starting point had to be a floor in the

contracts that meant that there was an obligation on the contracted parties to do something about DNS abuse to mitigate it or to stop it. And those obligations were clearly enforceable by ICANN. And so that was our intention, that was our goal. And as Russ has said, over an extraordinarily short period of time, those been in ICANN for as long as I have will recognize that doing anything in five months and ICANN is really quite extraordinary. We've managed to get to this point. So Russ, I don't really have anything else to say. We can take questions later, but back to you, I think.

RUSS WEINSTEIN: Do we want to pause, Tracy, see if there's any questions before we get into the substance?

TRACY HACKSHAW: Yes, let's definitely see if there are questions now throughout. Are there any questions? Please feel free to raise your hands. And, Julie, help if I can't see anyone else who has any questions?

JULIA CHARVOLEN: Thank you, Tracy. We have a remote participant, Kavouss Arasteh from Iran delegation raised hand.

TRACY HACKSHAW: So, let's take Kavouss.

KAVOUSS ARASTEH: Yes. Good afternoon to you. Good evening to the others. Yes. I think what I saw or what I heard is promising. It's promising that we have to at least-- I don't know the content of that issue that will be disclosed or will be available on 13th of July, but I hope that would be useful. What I'm asking whether if all these things that I hope will be done properly and timely, would be done. To what extent at least guesstimate the abuse, DNS abuse will be mitigated?

Point one, and point two, having heard the Chris Spann. I know he is one of the most competent persons working on the matter. I saw one of the very good works of him lastly, and that was an IGEO, which he successfully completed and resolve the issue of years. I hope that his contribution if he continues to contribute to this matter with all seriousness. But to what extent all these things would mitigate and reduce the DNS abuse? Thank you.

CHRIS DISSPAIN: Thank you. Hello, Kavouss. I hope you're well. I'd like to be able to give you a very simple answer to your question. It's a really hard question to answer. I mean, the truth is, we have no idea how much DNS abuse will be mitigated. What I think we can say for sure is that there will be-- Whereas now, a large number of contracted parties will probably be doing the stuff that's already in, that we've proposing to put into the amendments, there's no obligation to do so, and putting that obligation in and helping ICANN to making it simpler for ICANN to enforce has to have nothing other than a seriously positive effect on the amount of DNS abuse that is out there.

But that said, I want to acknowledge that there is still more work to be done. No one is suggesting that these contract amendments are the end of the matter. As I said before, the intention is to run a number of focused policy development processes to do more work and to make things even better if at all possible. So, that's the best I can do for now, but thank you for the question.

RUSS WEINSTEIN: All right. Thanks, Chris, and thanks, Kavouss. So, we can go on to the next part and we'll get into the substance of the amendments now. So, the approach we took in these negotiations and the amendments was to be sure were adding to the existing agreements and provisions. So, it's not something where were attempting to take something away from the community, but on the new obligations add on top to what already exists. So, thinking about that, it's important to start with what do we have today.

So, the current registrar obligations related to abuse are in section 3.18 of the registry-registrar accreditation agreement. They basically take a reasonable impromptu step to investigate reports of abuse, publicly display abuse contact information and the abuse handling procedures, maintain records and receipt of how you handle abuse when it's reported. And importantly for law enforcement and for governments, providing a dedicated point of contact for law enforcement reports or quasi law enforcement and government-related reports that needs to be monitored in 24/7 and needs to be responded to within 24 hours. So, Gabe, that issue you described that seems like an escape on that front

and wish it got routed or got handled appropriately because I think you already have that protection in the agreement.

So, in summary, what we did with these negotiations and what the result is we added, as I mentioned, we added the existing provisions. We clarify some information about the abuse contacts and making sure that they're very readily accessible from a registrar. Add a requirement to provide confirmation of receipt of an abuse complaint because that was something that we heard quite a bit about in the ICANN discourse that you submit an abuse report and you don't know what happened to it and you don't really have a good way following up on it and some registrars are registries. So, we added this requirement to provide confirmation of receipt.

We use a definition for DNS abuse for the purpose of these agreements and it's based on some work the SAC has done as well as several others in the industry. The core of it is we added an obligation to take a mitigation action to stop or disrupt DNS abuse when it's well evidenced reports. And that's the big meaty one that we'll get into in a few minutes.

So again, these are information about the abuse report and trying to make lower the barrier or make the reporting process better than it is today. And so, we clarified how the abuse contacts to receive reports need to be published on the website and provide that confirmation of receipt. We also addressed a long-standing issue that registrars and community members have identified that when you publish an email address on the web, that becomes a spam trap and overloaded. And so,

we allowed registrars to instead of using an email address on their website, publish a web form.

And what this hopefully will enable them is to get to the relevant abuse complaints faster than having to filter through high volumes of spam to get there, enabling them to take action faster. So, we think that's a positive development and something the community has been talking about for a while as well. We talked about the confirmation of receipt. And then just a clarification that the rules in place related to law enforcement agencies remain the same. There's been no changes made to those from a sensitive perspective. They've just been shifted down a section in the agreement.

So, the definition of DNS abuse for the purpose of these agreements. So, this is something that's been talked about quite a bit across the community. And as Gabe and Chris were mentioning, phishing is really the number one thing out there that I think these guys are worried about and many from a cybercrime and safety perspective, along with malware. But these are the five dimensions of DNS abuse and these are within ICANN's remit. And there are things that are actionable by the registries and registrars and that's why we've locked in on this definition and it's based on work the SAC has done as we referenced in SAC115.

So, the media obligation is, again, this obligation to take mitigation actions. So, we go from receive a report and investigate and respond to when you get an 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 stop or otherwise

disrupt that name from being used for DNS abuse. So, we recognize as we've talked to you about in the past in the lead-up webinars. I think Graham did some presentations on compromised militias. We'll talk a little bit about that. But this does take into consideration that not every case is handled exactly the same way.

DNS abuse is highly contextual. And that it needs to be dependent on the facts of that case. What action is the right action to take? And Owen will talk a little bit more about this when he goes. But keeping in context this concept of collateral damage and again we'll talk about that a little more. But this is a really meaningful obligation. It's clear, it's enforceable, and it changes the dynamic quite a bit from where we are today.

So, I will go through the registry obligations. And it's important to remember, we did these together collaboratively with the registries and registrars. We basically mirrored the same requirements from the registrar agreement into the registry agreement with some consideration for the difference in roles that a registry and a registrar play. Registrar being closest to the customer and having that customer relationship compared to the registry. So, the existing provisions in the registry agreement are specification 6, Section 4, where registries are required to publish contact details for handling abuse reports and to remove orphan glue records when used in connection with malicious conduct. That's the current baseline today.

And then there's the requirements in specification 11, sections 3(a) and 3(b), which have their origins in that Beijing communique from all the way back in 2013. And those requirements are that a registry must flow

down in their agreements with registrars. You must flow down in their agreements with registrants that certain actions and activities are prohibited and certain uses of the domain name are prohibited. And there must be consequences for violating those provisions that the registrar can enforce. That's in 3(a). And then in 3(b) is the one that gets talked about quite a bit, where a registry must periodically conduct technical analysis to assess whether domains are being used to perpetrate security threats in their zones. And they must maintain reporting on what the security threats were that were identified and any actions they took and be able to provide these reports upon request. So, that's where, again, the current requirements that we built on top of this.

So, what did we add to the registry agreement? Very similar, as I mentioned, to the registrar agreement. We clarified some information about how to submit an abuse report and providing the confirmation similar to the registrar. We use the same definition so that they're the same and can be floated across the industry. And then we have a very similar media obligation here. So, it uses most of the same words, but again, recognizes the context of a registry versus a registrar. So, I'll just read it for ease of use. For the registry.

"Where a Registry Operator reasonably determines, based on actionable evidence, that a registered name in that TLD is being used for DNS Abuse, the Registry must promptly take the appropriate mitigation action(s) that are reasonably necessary to contribute to stopping, or otherwise disrupting, the domain name from being used for DNS Abuse." And at a minimum, that should include either referral of that information and that actionable evidence to the registrar, so

they can investigate and respond and their obligations would kick in, their new obligation would kick in, or they can take direct actions themselves and do the mitigation options that Gabe was talking about earlier. And Owen will talk about as well.

So again, taking into account the role of the registry versus registrar, and again, not every case is the same DNS abuse being highly contextual, that you expect different actions to be taken based on different reports. So, it's really a helpful improvement to the agreements there.

And then in Specification 11 3(b), because we had added this definition of DNS abuse. We replaced the term, the undefined term of security threats within those sections with DNS abuse and we think that adds clarity and adds meaning importantly that the things they're doing registries are required to do on security threats is being done for DNS abuse and I think that will provide us a better position to have good conversations based on data and things.

And that's the summary of the two agreements. And as I mentioned, there's an advisory that you should all read as well and hopefully provides really helpful context about what these words mean in a little bit less legal jargon than in the contracts, and provides examples of how the obligations take shape in practice and provides a little bit about the compliance process as well, and how we would address them from a compliance perspective. So, that's the summary. Maybe we can pause now again and open up for questions.

TRACY HACKSHAW: Thank you very much. I just want to remind everyone, we have just about 10 minutes left in this particular block of activities.

CHRIS DISSPAIN: Tracy, can I suggest that actually if you let Owen just fill in some of the detail then the questions? He may answer some of the-- preempt some of the questions. It's up to you.

TRACY HACKSHAW: DRC, is your question specific to the what was just spoken about? Okay.

BLAISE AZITEMINA: Okay. Thank you, Tracy. Our comeback, I'm taking as evidence the definition that we just had about DNS abuse according to the slides that we went through. And this morning, we are the kind of interesting session covering the mobile phishing. I'm just making a follow up based on the question of Tracy and the very exhaustive and clear answer from Chris. And we understand that SMS, USSD platforms might just be those or channels to get in to abuse, and still, I don't really like. And in the morning, we talk about it, abuse is a little bit soft. Let's talk about crimes. Because these are really crimes. I do not know if that's a legal perspective or we can choose a better way, a better word, I mean.

And we know that the infrastructure behind will lead somewhere to financial institutions or to database, or even to registrar and then we fall to the normal or classic DNS abuse that we are talking about. So, my question is just a kind of a call. So, it's a concern and I'm a little bit frustrated. For this to be addressed, of course, it's not standard DNS

abusers we understand, but ICANN can't come with strategies, warnings, guidelines so that's either, we talk only to regulators, mobile operators or somehow ICANN as a role or something to do to assist in this? Thank you.

OWEN SMIGELSKI: Hi. This is Owen Smigelski. I can handle this one. So, if it's being used for phishing, if it's an email, if it's in a website, if it's via SMS, if there's a domain name that's being used for phishing and it's a gTLD, absolutely, that's within the scope of the phishing identified in this contract. I mean, there are other types of phishing that may go on with mobile devices that are things outside of a domain name, but to the extent it's within ICANN's remit, yes, this will cover that.

NIGEL CASSIMIRE: Yes. Good day. Nigel Cassimire from Caribbean Telecommunications Union. Just on this last slide here where we've seeking to replace security threats with the exact DNS abuse. I'm just wondering if we are comfortable that we are not leaving out any security threats, by only focusing on the honest abuse in terms of the contract because I'm wondering if there might be there might be some other type of security threat that mightn't exactly be DNS abuse, that could warrant some sort of action from registries and registrar as well. So, have we thought through that and are we comfortable that we're not leaving anything out?

RUSS WEINSTEIN: Yes, thanks. It's a good question. So, I think that comes back to where we started on these agreements, which is the existing provisions are related to abuse generally and those haven't gone away, those stay where they are. And so, registries and registrar still have some obligations related to undefined abuse which relates to security threats.

In the context of this provision in Spec 11 3(b), I think it does add helpful clarity around what is to be reported on. It doesn't change what needs to be acted on.

Again, there are there are provisions related to malicious conduct with the TLD or the little abuse in the registrar agreement that still remain, but when we're talking about defined DNS abuse, we've increased the obligations and the requirements. And that's because it's something we understand, we can box it, and really drill down into what is the expected behavior on those. And that's the amendments we produced.

OWEN SMIGELSKI: If I can just add one more too. This is not it for DNS abuse action within ICANN. This is something that we identified contracted parties and ICANN is something that we can get done quick now five months for the amendments. We'll keep forgetting that there's also a 15-page advisory we all agreed upon. So, there was a lot of work that went into it. But next steps after this are for the community. And so, those other things that may not be addressed now, we can address them later.

CHRIS LEWIS-EVANS: And just to add from my viewpoint, I think this is a key thing for the GAC to think about in its public comment. As Russ has said, add some clarity in the discussions they've had, it allows them to take better action. But from a GAC perspective, does it cause any public safety risk that they might not have thought about? And that's the purpose of that public comment is to provide them with any information that we might see. But what we're hearing, they believe it provides a more clarity, more ability to act. So, we need to consider that and we may need to think about that on the public comment front. Thank you.

NIGEL HICKSON: Yes, thank you very much. Nigel Hickson, UK, GAC. And thanks so much for this session. It's incredibly valuable. No doubt we're going to come back to this later in the week in various other sessions, but to have the ICANN org and the other parties explain what this is about I think is valuable. And congratulations on achieving such a rapid turnaround. Really, I just had a question on the language and if we're going to come back to this later, then that's understood.

And the linkages between 318(i), 318(ii) and 318(iii), I think a very understandable. Just the thing that I didn't quite understand and that might be because English is not that good sometimes, but is where you were saying a couple of places that the mitigation that the registry or the registrar—and I know it's in both sections—should take the appropriate mitigation actions that are reasonably necessary. And I just didn't quite understand reasonably. I know that the taking action has to be subject to certain criteria, but once you've decided to take the

action, I didn't know what reasonably necessarily meant, so to speak. Thank you.

OWEN SMIGELSKI: So, this is Owen Smigelski. Nigel, that's a perfect question into segue into my slides. So, if we can move that, go onto the next slide, I think we're done here. So, one thing to keep in mind when dealing with DNS abuse is there is no one solution to every single thing. They're all different. A lot of this will require review manually by humans, investigations internally, access to additional information. That's not required, but certainly certain things. And as the example that Gabe gave earlier about a domain name being registered very close to that type of attack that highly suggests that it's being used specifically for that. Also, on a side note, the DNS abuse amendments in my opinion would actually have made that registrar be able to take action for that. So, I think that would be good that that would be addressed.

So, there are different things that registrars have to do and a lot of that are registries and a lot of that has to do upon whether or not it's compromised or maliciously registered. So, I'll go quickly through here. There's really only the nuclear option that registrars and registries can do. They can turn a domain name off or let it continue to function. They can go out and take out the little tiny bit of content or something like that. So, that's why there's very quiet often a need to work with a hosting provider or the registrar registry can do with that. So, those are usually done through some sort of holds or changes to name servers.

Other ways that these types of DNS abuse complaints can be addressed is actually contracting the registrant or the hosting provider sometimes

depending upon what that is. A perfect example, I know we've heard about acidtool.com, which is a resource that the registrar stakeholder group put together, which if you put a domain name into acidtool.com, you can see the registrar information if available as well as hosting provider. When we announced that at the Cancun meeting, within a week, we were receiving a DDoS attack and multiple hacking attempts and everything. Apparently when you do stuff to help stop DNS abuse, people get angry about that.

So, what they did was they actually got in and exploited a plug-in vulnerability. They were using WordPress and so the correct action wasn't to stop that domain name, it wasn't to suspend the domain name because people were using it. What we ended up doing was working with our tech team to update the plug in, remove the content, and continue to function, as well as do some other mitigation things, put on Cloudflare. We would move it to a dedicated server, etc. So, there's different things that can be done. Domains can be deleted. I think I heard Gabe mentioned that. That can have to do with the AGP limits policy, why they got deleted as opposed to just left there.

Or sometimes another type of effort that we happen is someone from like a law enforcement agency will come and say this domain name is being used in some type of malware or phishing attempt, and we want to see who's being harmed by this. And so, rather than stopping the abuse, we will allow it to continue, but coordinate with law enforcement so they get the information along with that. So sometimes it's not always the proper thing to stop the DNS abuse. That's how we kind of disrupted or mitigated.

The thing also is not all DNS abuse is the same as a compromised domain name and that's where like I described with the acidtool.com, somebody came in and they hacked it. That can happen other ways. There can be a password compromise or other things like that. And in that kind of scenario, you're not going to want to shut down the whole site. We've seen sometimes where it's a college university or a medical facility has a page somewhere that gets hacked, you don't want to take that down. So, there's stuff that can be done in the background either through resellers or the registrant or hosting provider webmaster. There's a number of things that we can do and the changes that are in this contract do allow for that so that the only thing you do is just shut down an entire website, that collateral damage can be huge and potentially very disruptive to that.

There can also be times where it's not necessarily domain.tld where the abuse is occurring. It could be secondlevel.domain.tld or sorry, third level, those third level TLDs are not necessarily something that a registrar registry can deal with. And if those are taken down, if the main domain is taken down, then all of those other third level sites go down as well too. So, there's a number of situations on how to respond to that, but there is flexibility in the wording of the amendments for that and if you take a look at the advisory, we go through and explain those and how that can be affected. I think that is done. Deck slide, just in case? Okay. That's it.

TRACY HACHSHAW: All right. And we have a couple of questions coming in from the Zoom room. Kavouss' hand was up, is up. It's put down now, so I think we can move on to--

KAREL DOUGLAS: Tracy, sorry. We also have some questions on this side.

TRACY HACHSHAW: Yes. So, let me just deal with the remote please. Jorge is asking, how is the correctness of the choice of the corresponding action assessed and who monitors that? That's Switzerland, Jorge. How is the correctness of the choice of the corresponding action assessed and who monitors that? And Kavouss' hand is also up as well. Kavouss', can we take your question now? Yes. So, let's just take the question from Kavouss' as well.

KAVOUSS ARASTETH: Thank you very much. My question was-- Excuse me. Do you hear me?

TRACY HACHSHAW: Yes. Yes.

KAVOUSS ARASTETH: Sorry. My question was on the first slide, we're talking of the issue of enforceable. I think in addition to the enforceability, we need to add or consider two more objective, enforceable and measurable. Without measurable, we don't know whether to what extent this action has

been positive or contribute. This is one. The other one, the content of the report. What would be the content of the report? The content would be, for instance, include category of abuse, include the nature of the abuse and something like this.

And then the last question or last comment is that, when we say obligations, for critical cases, obligation is a mandatory language in the agreement, but sometimes it may not be sufficient. We need to add to that one accompanied with a firm commitment to undertake, to implement or comply with that obligation which still, as I said before, should be objective, measurable and enforceable. So, I think a simple obligation on the language-wise is not sufficient. It should have a firm commitment that the action will be done and the side question is that the frequency of the report, how many reports per year or so on so forth. Thank you.

TRACY HACHSHAW: Thank you. So, we can get the response to Jorge's question and then Kavouss'.

CHRIS LEWIS-EVANS: Yeah. So, thank you, Jorge and thank you, Kavouss. I think those questions are actually fairly related, so I'll try to answer both of them from my compliance perspective. So, first of all, the amendments, they add a significant obligation to what's there right now above the basic requirement is particularly in 3.18 of the RAA to investigate and respond. It's not just to investigate and respond, it's also to take action.

So, to Kavouss' question, there is an obligation to mitigate or otherwise disrupt the DNS abuse.

When compliance initiates on whether or not a report of DNS abuse has been acted on appropriately, there's a number of things that we will look to ensure that the obligations are complied with. This is assuming, obviously, that the amendments are adopted. First of all, we will look to see that there's actionable evidence of one of the forms of DNS abuse. And for reporters out there, this is absolutely key. It's compliance, not just for DNS abuse, but for abuse reports generally, there's often 70% to 80% of the complaints that we get, we can't do anything about them because they don't have evidence of the abuse. They don't have evidence. They don't demonstrate that they reported the abuse of the registrar or it's really a complaint about a ccTLD or they're telling ICANN to take down content.

So as these amendments are implemented, it's really important that people that reporters who are not happy with the response they got from registrars to registries include evidence of the abuse. And I would refer you to the CPH guidelines, which I think there's a link in that somewhere.

GABE ANDREWS: Yes, it's in the advisory.

CHRIS LEWIS-EVANS: It's for sure in the advisory, I was just wondering if it's also in the presentation. But that has a good explanation of the types of evidence

that would satisfy for the registrar as well as the types of evidence that compliance would look for. The language does continue some of the language from-- the amendment does have some of the language from the existing 3.18 about reasonable and prompt and appropriate. And as Russ and others have tried to explain, the circumstances of a particular instance of DNS abuse vary tremendously. So, whether an action is prompt, whether the evidence provided to the registrar or registry was actionable, whether the action that they took to mitigate or stop was appropriate are all individual items that are almost impossible in advance to prescribe. But that doesn't mean that the registries or registrars when presented with actionable evidence have discretion to do nothing.

If we get a report or if we determine on our own that there is actual DNS abuse and an appropriate action wasn't taken, we will ask the registrar or registry to demonstrate why they don't think the evidence was actionable or why the response that they took was reasonable under the circumstances, was appropriate, and was prompt. It would be a lot easier if we could come up with black and white rules with specific timelines and actions to be taken in every case, but that just doesn't fit the world of DNS abuse. But again, that doesn't mean unfettered discretion to blow it off. It means you have to investigate, respond and take the appropriate action in promptly.

And just to flesh out again a little bit on the promptness. There are lots of examples. I really encourage everyone to read the advisory because the amendments themselves, the textual change in the amendments are fairly short. The advisory is 15 pages long and includes lots of examples of different scenarios as well as more detail on the approach

that compliance will take. But there may be instances where it is appropriate for a registry or registrar to have taken a longer period of time. Some of the examples say two days, sometime it is possible that it would take five days in a particular circumstance to understand exactly what's going on. It's also possible that the harm that's being created by the DNS abuse is so impactful and has so many victims that if the register comes back and says, that we waited a week, we will say that's not appropriate. That does not comport. Given what you knew at the time, you should have taken action sooner.

And then the last thing I just wanted to touch on and somebody asked earlier about how will we know and how will we measure. In compliance, we are going to report on what we see and what we've done with granularity. And as everyone said, this is a significant first step, this is a significant new obligation. And at least from a compliance perspective, we will provide granular reporting so that the community will see what's been going on and we'll report on any challenges that we find that could be the subject of further community discussion, contractual negotiations or policy development.

TRACY HACHSHAW: All right. Thank you very much. I know the time has completely run out on us. This is a capacity development session, so I want to make sure we get the questions in. So, I know there are a few questions coming still. Let's ask the questions and then toss back to the panel to continue and to feed that into their presentation if possible. Let's take it for five minutes.

BERTRAND DE LA CHAPELLE: Hi. Good afternoon. My name is Bertrand de la Chapelle from the Internet and Jurisdiction Policy Network. Two quick comments in response to what has been mentioned. When Nigel was asking about reasonably necessary, it's a typical implementation of the concept of necessary and proportionate. And as has been mentioned often on the panel, each case is a specific set of parameters and the choice of action pending the information that is provided is exactly what needs to be done to act at a proportionate level. So, the expression reasonably necessary is a good concise expression to combine the two elements.

The second thing is as was mentioned by Gabe before, speed is essential and the shift that a lot of people are not necessarily going to pay enough attention to is the mention of web forms because not only is this something that is going to reduce the amount of potential spam on the email abuse points of contact as was mentioned. It is also something that paves the way towards better automation of the workflow that accelerates speed at which the information is going to be provided to the different actors in the dispatch mode.

And NetBeacon was mentioned and the work that the DNS Abuse Institute done in that regard is very important also because in the future, one might consider that smaller registrars and registries who do not necessarily have the capacity to automate their workflow easily are going to be able to access this kind of tool to automate their process for the distribution of abuse reporting, not decision making. But workflow is essential and the work of the DNS Abuse Institute has been really good in that regard.

TRACY HACHSHAW: Thank you very much. There's a question I can't see.

NOBUHISA NISHIGATA: Thank you very much for the presentation. Quite helpful. And one favor to ask, could we get back to Gabe's slide about showing the exchange between the law enforcement and the registry-registrars? My question comes from that deck. Then then I got some question with the registry-register as well.

TRACY HACHSHAW: So, can we get that question first? Because I think we can't go back too far now because time has run out on us.

NOBUHISA NISHIGATA: Okay. So now my question, the first question is that looking at Gabe's deck showing the exchange between the law enforcement and registry-registrars, my first question is, is it normal reaction from the registry or registrar to answering the inquiry or the question from the law enforcement?

And then the second question is, if so, then I would like to know more rationale to act like this because it I think it is not only Japan. I'm working under the government of Japan. It's a little bit frustrating from our side. But still, this is only maybe government side to be frustrated in there. Of course, there are registry and registrars, good companies and listed in there who do have the good corporate governance and the etc. So, we would like to know more rational to understand the behavior from the registry/registrar side.

So, then my third question if possible. It is about the amendment. And then just I mentioned about some reactions shown by the Gabe's deck. How the amendment going to change the behavior at the registry or register's side if the current amendment is adopted or implemented as it is? Thank you.

TRACY HACHSHAW: All right. So, we can cut straight back to the panel and you can finish off as well.

OWEN SMIGELSKI: And I can answer probably all three of those. So, short, these new proposed amendments would absolutely 100% require the registrar to take action to stop or otherwise disrupt DNS abuse. Perhaps it might still have to go through a process of just one report to the registrar and then it's done. The registrar may need to reach out to a reseller, etc. However, with an efficient example such as that, 100% a registrar would be obligated to stop or otherwise disrupt that phishing. So, it's very positive moving forward.

Right now, that is not a requirement for registrars to do. Those that have signed the DNS abuse framework, my registrar, the ones that generally participate in ICANN, we're already doing this stuff for the most part. This would make sure that every registrar and registry in the world using gTLDs will have to action that type of complaint that Gabe highlighted earlier.

ASHLEY HEINEMAN: So just to tackle on -- Ashley, sorry, with the registrar's stakeholder group. That is the intention of this exercise in creating a baseline. Because we've heard one example, that is not reflective of the entire industry, but our hope is that by having this contractual language, a requirement to take action, the ability for Compliance to step in when necessary is exactly what we're trying to achieve here. So, I appreciate the example because that's what we're trying to address and make sure that we're all living at the same standard, because that is not a reflection of the entire industry. Thank you.

GABE ANDREWS: Sorry. And just to add, I think the other thing and Ashley just mentioned it there, but it's worth probably highlighting, is it if it does happen, it also gives compliance the ability to act. So, I think that's the key point. One is it gives the registrars a compliance part to do and then it gives compliance tools to act if it doesn't. So really big change really in how we are at the moment. Thank you.

TRACY HACKSHAW: All right. And let's take two minutes to just wrap these slides up if possible.

RUSS WEINSTEIN: Sure. So, this is Russ again. And I mentioned at the top, it's not as easy as just agreeing here with the negotiating teams. How do we actually bring these to fruition? So next steps here. So, you may recall, we actually just did amendments to the base registry agreement and the

registrar accreditation agreement related to RDAP and implementing new obligations related to how they provision the RDAP service, which is related to registration data. So, we just got some really good experience because we're going to need it for the next step.

So, the short answer is the process. We can go to the next step on the next slide. The short summary of the process for this is identify a problem, initiate negotiations, which we've now done and completed, put it out for public comment, which is where we are now. Next steps, we'll review the public comments, discuss with the contracted parties, if anything should be adjusted, and we'll finalize the amendment proposals. And hopefully, that will occur in the July to September timeframe. And then we go to the voting.

And so, every registry and registrar has an opportunity to vote on these amendments. And in order to get them into effect, we need a majority of registries and registrars. And on the registrar side, it's actually 90% of the registrars essentially need to vote yes for this to pass, which it's a big hurdle to climb. It's in the agreements. It's been that way since 2013. We've just proven successfully we can do it on RDAP. It takes a lot of effort, but it's something to factor in when we're negotiating these, when we're thinking about how to describe them to the community. And it'll be a big effort from both ICANN and their contracted parties to encourage the votes. Yes. Because we think this is the right thing, this is a good thing for the industry and where we want it to go. But it is a big factor and something to keep in mind. It's not as simple as okay, we've agreed. Let's get it on contract.

Following voting by the contracted parties, it'll go for the Board, the ICANN Board for consideration and if adopted there, we'll go into implementation. The timeline shown here is kind of the best-case scenario timeline. We've met the milestones so far to stay on that best-case scenario, but what that means is by this time next year these things could be effective in contracts, which would again be really at lightning speed for ICANN. And a really good step forward. So, with that, I think we can close it out. Thanks.

TRACY HACKSHAW: Thank you very much and thanks to all of the panelists and everyone who came today, we really appreciate it. I know time has been problematic, but I think it was good information shared. And I would encourage people have questions, put them in the chat now because I think there are folks still looking at the chat in the Zoom, and they can maybe get them answered there. Also, and Russ is going to say something about that, questions?

RUSS WEINSTEIN: Yeah. We have a session on Tuesday in the afternoon where we're going to explain these amendments again to the whole community and take questions. And so, really if it's possible for you to attend that and ask more questions, that's another good opportunity for dialogue on this.

TRACY HACKSHAW: All right. Thank you, Russ. So, we're going to take a break now. So, we had Susan planned to present something, so we're going to shift that to

after the break at the start of the next session. And what I want to do before we go to break is just ask another question. Who speaks French? Who speaks French in the room? All right. Who speaks Spanish? Who speaks Arabic? Who speaks English? All right. The reason for all of this is because you're going to break on to groups by your languages after the break.

So, when you come back in the room, be prepared to break out into groups, move around from your tables into groups. We're not coming back in plenary. Be prepared, right? We're not coming back in plenary. We're going to move to groups in your languages to discuss what we just had today, to answer some questions, group work after. Okay? Don't run away. Come back for the groups. Okay? Thanks very much. Thank you all. 20 minutes. We're back in 20 minutes.

[END OF TRANSCRIPTION]