ICANN77 | Prep Week – DNS Abuse Contract Amendments Update
Tuesday, May 30 2023 – 14:00 to 15:30 DCA

RUSS WEINSTEIN: We'll give people another minute or two to come into the room. All right, Michelle, do you want to kick us off while we're waiting on something?

MICHELLE WILSON: No, I'm ready. All right. This session will now begin. Please start the recording. Hello, and welcome to DNS Abuse Contract Amendments Update. My name is Michelle Wilson and I am the remote participation manager for this session.

Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior. During this session, you must use the Q&A pod if you have questions. Any questions posted in the chat will not be read out loud on the microphone. Interpretation for this session will include French, Spanish, Chinese, Arabic, Russian, and Portuguese. Click on the interpretation icon in Zoom and select the language you will listen to during the session. If you wish to speak, please raise your hand in Zoom, and once the session facilitator calls upon your name, kindly unmute your microphone and take the floor. Before speaking, ensure you have selected the language you will speak from the interpretation menu. Please state your name for the record and the language you will speak if speaking a language other than

English. When speaking, be sure to mute all other devices and notifications. Please speak clearly and at a reasonable pace to allow for accurate interpretation.

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

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

RUSS WEINSTEIN: All right. Thanks, Michelle. Thanks, everyone, for joining us today. My name is Russ Weinstein and I'm the vice president of GDD accounts and services with ICANN. My team is responsible for our contracts and relationships with the Registries and Registrars, and I also lead ICANN's organization-wide DNS Security Threat Mitigation Program.

Today we'll be sharing information about an exciting new development, the much anticipated proposed contract amendments related to DNS abuse. This has been a collaborative effort across multiple functions at ICANN, most notably the Global Domains and Strategy Team which I belong to, our OCTO Team, Compliance, and Legal, along with Negotiation Teams each from the Registrar Stakeholder Group and the Registry Stakeholder Group.

To help me present today, I'm joined by Leticia Castillo from ICANN's Contractual Compliance Team, Owen Smigelski from Namecheap and the Registrar Stakeholder Group, and Chris Disspain from Identity Digital and the Registry Stakeholder Group. Next. You can go to the next slide, Michelle. We'll do a quick tour of an agenda today where we'll explain the background and intended scope of the amendments. We'll then do a high-level overview of the amendments themselves and what the new obligations are. We'll then have a short discussion around DNS abuse techniques and considerations from the contracted party perspective. We'll provide information about the interpretation and enforcement of these proposed amendments on Contractual Compliance. Then we'll provide some overview of the process and global amendment procedures to bring these amendments into effect, and then open it up for Q&A. We have 90 minutes total today for the session and we're hoping to have at least 30 minutes, if not closer to 45 minutes, for Q&A. We also have a session during the ICANN77 week. There'll be more time for Q&A and discussion there. So please join us in that session as well. Next slide.

The Public Comment period is now live. We opened the public comments on the proposed amendments yesterday. That will be open through July 13. It's about a 45-day comment period, taking into account some extra time for ICANN77. What you'll find is proposed changes to the Registrar Accreditation Agreement. Those are contained in Section 3.18. We'll see proposed changes to the Registry Agreement in Specification 6 Section 4 and Specification 11 Section (3)(b). In addition, we have a supporting document, a draft advisory

from ICANN, which helps provide expectations for compliance with the proposed obligations. So that's a contract setting document.

These negotiations kicked off in January and just completed in mid May, which is really fast in ICANN time for contract changes. It's a testament to the collaboration between ICANN and our CPH colleagues to bring this effort to fruition so quickly. With that, I'm going to pass it to Chris Disspain. He's going to provide some context for how we got here.

CHRIS DISSPAIN: Thank you, Russ. Hello, everyone. Good to see or rather know that there are lots of people watching. Hopefully, this will be informative and useful. I'm just going to go over three slides which talk about the background and how we got to where we are.

So just the starting point, basically, the contracted parties—well, you all know DNS abuse has been a subject of conversation in various different arena for a fairly long time and there are varying different views about it. Different parts of the ICANN community have been discussing it at different paces, and so on. And the contracted parties came appreciate the absence of strong enforceable obligation in the Registry Agreement, in the Registrar Agreement. Those are obligations that deal with a requirement to mitigate or disrupt DNS abuse. So we got together and decided that we thought it would probably be a sensible thing to start working on that. There's a bit of background on that particular slide that you're looking at right now. But I'd like to, if I

can, just move on to the next slide because that's the more interesting and important information on it. Thank you, Michelle.

So here we go. It's a two-stage process. We decided that we needed to agree meaningful and enforceable changes to the contracts in order to raise the floor. It's not about best practice. It is about raising the floor and trying to put in place a minimum standard that everyone understands and that is acceptable. We wanted to do that by creating an obligation to mitigate DNS abuse. The scope of the contractual changes is to deal with DNS abuse as it's previously defined by the contracting parties, house with no registration data disclosure topics, and no past or obligations. So those are the contractual changes and that's what we're actually going to be talking about today. While the comment period is open, and what we've been working on for the last 12 months, it was almost exactly 12 months ago that we got together and decided that we thought this was an appropriate thing to do. Those of you who've been around ICANN for a long time will understand that that's actually pretty quick to have got from that stage, just talking about it two months ago, to now is a fairly fast track.

Step two then is a community-driven process. So having dealt with step one, which is where we are right now, we move to step two, and that's acknowledging the work of the multistakeholder policy development process but the full involvement of the ICANN community in shaping the policy of DNS abuse is a key step, that there needs to be a strong scaffold and enforceable contractual obligations, as I said, a floor, then that's a prerequisite to making enforceable policy that people understand and can work with. And that the PDPs

must be grounded in clear practical goals that support DNS abuse, disruption, and mitigation. If I can go to the next slide, please. Thank you, Michelle.

So the guiding principles in the resulting amendments. To focus on the target outcomes of stopping or disrupting the use of gTLD domain names for DNS abuse. That's the focus. That's the target. The Registrars and the Registries must take prompt action to mitigate when a domain name is being used for DNS abuse. DNS abuse is highly contextual, the circumstances of each case are critical to determining the best approach to mitigate. There is no one size fits all. It is, in fact, a case of one size fits no one. At the end of the day, it's all about the context. Is it malicious? Is it not? We can come on and talk about that a little bit later on. The Registrars and the Registries need discretion for what action to take, and the action they take needs to be proportional and the possibility of collateral damage has to be taken into consideration before any action is taken. And finally, obviously, that it's important to recognize the different roles between Registrars and Registries. Yes, you'll see when Russ goes into the detail of the proposed changes, the two separate contracts, two levels of change, one set for the Registries and one set for the Registrars.

That's the background. The contracted parties' Negotiating Teams have been working closely together as a team with ICANN for just over 12 months. Both the Registrars and the Registries had support teams sitting in the background who were involved in most of the calls, were able to provide input and help. But obviously, for negotiating purposes, the number of people involved in the actual negotiation is

quite small. But we were consistently and constantly reverting to our colleagues in each of our respective houses to get their input and their views. Russ, I hope that covers the background in as much detail as you wanted. When we get to the end, I'm happy to answer any questions. Thank you.

RUSS WEINSTEIN: Great. Thank you, Chris. We can go to the next slide. So now we'll take you through a little overview of each of their proposed amendments. We'll start with the registrar obligations. So with that context, we'll dive in. Next slide.

Before we dive into what's new, it's important to remember what we have already. So the existing obligations related to abuse in the Registrar Accreditation Agreement are found in Section 3.18 of the RAA. They require registrars to take prompt and reasonable steps to investigate and respond appropriately to abuse reports, to maintain a dedicated point of contact for law enforcement or similar authorities to contact registrars of reports of illegal activity and to review those reports within 24 hours. To publicly display abuse contact information for how to submit an abuse report, where to submit it, and how those reports will be handled, and to maintain records of all the receipt and responses to abuse reports and make those available to ICANN upon request. So with that, we built on top of these existing requirements to tackle these DNS abuse obligations. Next slide.

Again, what we tried to do here was build on top and the existing obligations in Section 3.18. A high level overview of what we did was

we clarified information about the abuse contacts registrars must provide and where they must be displayed. We added a requirement to provide a confirmation of receipt of an abuse report, which was a pain point identified by many in the community and something we found in our own compliance tickets as well. We added a definition of DNS abuse for the purposes of this agreement so that we know what we're talking about, what the obligations are relative to these things. And then we added a new section in 3.18.2 and this is the core of the obligation to mitigate, to take mitigation action to stop or disrupt DNS abuse. We'll get into the detail in a little bit here now. Next slide.

So starting off with the new obligations is about reporting abuse to a registrar. So these are the requirements to clarify that the abuse contacts are readily accessible on the homepage and that registrar must provide that receipt of confirmation of report of abuse. We also clarified that registrars can use either an e-mail address or a web form to collect abuse reports as long as it's readily accessible from their homepage, and that the web forms must not require a login to submit abuse reports but can require things like e-mail or contact information so that they can get back in touch with the reporter. This address is a pain point that the registrars have identified for a while now, that the abuse report e-mail addresses as public often get diluted with spam and make it harder for them to identify real reports of abuse and take time away from fighting abuse.

Similarly, we added the confirmation that I've talked about before, so a registrar must provide a confirmation receipt the report of abuse. This helps reporters then be able to track their abuse report and if they

don't feel a satisfactory outcome or a satisfactory action has been taken, they can bring that report to Compliance. No changes have been made to the contacts of law enforcement agencies. Those obligations remain intact and unchanged. The only adjustment is they've been shifted from 3.18.2 to later in the section. Next slide.

Next, we have the definition for DNS abuse. And for the purposes of this agreement, as long as the Registry Agreement and the advisory that we have published, DNS abuse means malware, botnets, phishing, pharming, and spam when served as a delivery mechanism for other forms of DNS abuse. These are all defined terms in a SAC advisory 115 that came out a couple of years back, there in Section 2.1 of that as a helpful reference for us all. For the purpose of these agreements, these are the things we're talking about when we're talking about DNS abuse. Next slide.

Now, the core of the obligation is that a registrar, when they have actionable evidence that a registered name sponsored by that registrar is being used for DNS abuse, they must promptly take appropriate mitigation actions that are reasonably necessary to stop or otherwise disrupt the name from being used for DNS abuse. They recognize the actions may vary depending on the circumstances as Chris talked about, DNS abuse is highly contextual. We need to take into account the cause and severity of the harm from the DNS abuse and associated possibility of collateral damage. But this new obligation is meaningful and enforceable, and now for the first time requires prompt and reasonable action to mitigate when a domain name is recognized as containing DNS abuse or being used for DNS

abuse. So that's the summary of the Registrar Accreditation Agreement changes. Now we'll move on to the Registry Agreement.

So the Registry Agreement tracks pretty similarly. We'll first go through existing obligations, which are on two slides. First, we have Specification 6 Section 4. Registries are required to publish and provide to ICANN contact details for handling inquiries related to malicious conduct into TLD, and to remove orphan glue records when used in connection with malicious contact. Next slide.

Then in Specification 11 of the base Registry Agreement, often called the Public Interest Commitments, there are two obligations there, Specification 11 Section (3)(a) which requires registries to pull down a requirement to registrars which must be pulled down in their Registration Agreements, prohibiting certain activities and requiring consequences for the registrants if such activities are found. And then (3)(b) which requires registries to periodically conduct a technical analysis to assess whether domains in their TLD are being used to perpetrate security threats, and then to maintain statistical reports on the number of threats identified and the actions taken as a result of those analyses. So these are the existing requirements, and then again, we built on top to add DNS abuse obligations similar to what we put into the Registrar Agreement. Next slide.

Going back to Specification 6 Section 4, we clarified again for registries they may use e-mail address or a web form to collect those abuse reports. We clarified that a registry must also provide a confirmation of receipt of report of abuse similar to the registrars. Next.

We added the same definition that we used with the registrars and is applied to both to the whole agreement. Again, founded in SAC115. Next slide.

We added the abuse mitigation obligation for registries. So similarly to a registrar, when a registry reasonably determines based on actionable evidence that registered domain name and the TLD is being used for DNS abuse, the registry operator must promptly take the appropriate mitigation actions that are reasonably necessary to contribute to stopping or otherwise disrupting the domain name from being used for DNS abuse. Those actions at minimum should include referral of the domains to the relevant registrar with the relevant evidence or taking direct action themselves where they deem appropriate. Again, recognizing the actions may vary depending on the circumstances of each case and the severity and harm and potential collateral damage. Again, adding an obligation to mitigate DNS abuse when it's identified in their TLD and well evidenced. Next slide.

Then we made a minor change to Specification 11(3)(b) to replace the term security threats, which is undefined, although uses many of those same elements that we put into the definition of DNS abuse with the defined term of DNS abuse. This clarifies that the technical analysis that needs to be done by the TLD operators is being done to check whether domains are being used to perpetrate DNS abuse, and then that their statistical reports are based on identified DNS abuse. And now that they have the obligation to mitigate DNS abuse, once it's identified, anything they're finding here in these technical analyses

and identifying evidence for, they need to then go mitigate the roundabout step.

So those are the summary of the Registry and Registrar Agreement changes. I'm not going to pass it to Owen, who's going to talk a little bit about DNS abuse mitigation techniques and considerations.

OWEN SMIGELSKI: Thank you, Russ. Again, my name is Owens Smigelski. I am the domain name registrar of Namecheap and I am co-chair of the Registrar Stakeholder Group Negotiating Team. Next slide, please.

One of the things that Chris mentioned earlier is that DNS abuse mitigation is not a one-size-fits-all approach. It is highly based on context and each individual abuse complaint needs to be reviewed on a detailed level. It's not something that can be readily automated just because there is so much information either in the abuse report itself that must be reviewed but additional information that may be made available to a registrar or registry, such as customer information, age of the domain name, etc., etc. So there are a number of actions that registrars and registries can take to do that to mitigate DNS abuse. And quite often, it's not just something where we can flip a switch and then magically stop the DNS abuse. It's a bit more detail and complicated than that. So from the registrar and registry side, the one weapon that we can really do is we can suspend the domain name, and that can be done through a number of ways. What that does, that just basically takes it out of the DNS abuse. It doesn't resolve, it doesn't operate. So, e-mail, website, etc., not anything can function

there. This is also something that can be reversed as well too, that suspension can be undone. From a registrar side, that can be done by setting the EPP status code to client hold. And from the registry, they can set that to server hold. There are other ways to do that, but no need to go into all those details here.

There are some other ways also that a registrar or a registry can take action, which are a little bit more drastic. They can delete the domain name. That means it's totally gone. But then there are also some other ways that are a little bit less intrusive there as well, too. This would again be based upon the type of abuse that's being reported and the various circumstances in that situation. So some other appropriate ways to take action to mitigate, to stop or disrupt the DNS abuse is to contact the registrant or the hosting provider. Quite often, the hosting provider can see better what's on that network, what's going on there, or the registrant may not be aware of the abuse that's going on there. And it's important to note that quite often, while a registrar may also be a hosting provider, it's very quite frequent that the registrar is not often the hosting provider for a domain that is registered through them. Those are two different entities, which is why contacting a hosting provider, the registrant, can often be the best or the quickest way to get this resolved.

There's other steps that the registrars and registries can take, including locking out the domain name. That means that it can't be transferred to another registrar that might perhaps be a little bit less zealous with the way that they're approaching the abuse. Another thing that can be done is to redirect a domain. That can involve

modifying the name servers. This is often used in an approach where there is a way that we want to monitor what's coming in quite often with say a botnet or something like that. This can be used to identify and help people who might fall victim to this. Then there's also other escalation that can be done. If a registry gets, an example, of perhaps an egregious type of thing, they would reach out more directly to the registrar to expedite action to prevent ongoing abuse or collateral damage. Next slide, please.

You heard a couple of times we've mentioned compromised domains and collateral damage. Not all domain names that are involved in abuse are registered for an abusive purpose. There's actually a significant percentage of domain names—I don't recall off the top of my head the specifics—but a sizable percentage of domain names, what we refer to as compromised domain names, that is where without the knowledge of the registrant, somebody has done something in order to take over either all or part of a website or a domain name. In these scenarios, quite often, the suspension, such as client hold that I referred to on the previous slide, that may not be the appropriate action. What you may have is this may be a website that is part of a larger site. So it's quite possible it could be a university or a hospital or some other website that has a significant amount of pages and traffic, and only a very small percentage of that site is being used to exploit that. So in these types of cases, it's better to not suspend but to work directly with the registrant or the hosting provider.

An example that I can give is at the ICANN76 meeting in Cancún, the Registrar Stakeholder Group announced acidtool.com which is a site

that we put together, which can help look up not only registrant information but also host information, which is very helpful when trying to go after DNS abuse. Within a week of announcing this, that website was hit by a large number of denial-of-service attacks. And eventually, it had a plugin that was compromised on the website platform that we're using. So instead of just taking down the entire site, what we did was we worked with our tech team and our host team, and removed the plugin that was infected and had been compromised, and updated it and fixed it and took some other actions to protect that. That way, the website continued to operate and assist Internet users in finding other sources of hosting abuse.

Then also, another point where this might be applicable is when there's a third level subdomain in there. So when a registrar or registry is dealing with domain names, we work at the second level. So that would be example.tld. But it's often that there are third level domain names where it's sub.example.tld, and registrars and registries can only work with the second level domain names. If we suspend that, that takes down everything else below that, and that might not be a good solution for that. So quite often in these cases where we are dealing with these compromised domain names and not wanting to cause collateral damage to them will work with the registrar, the registrant, site operator, host, but there's a number of places where we can work there to do that to ensure that DNS abuse is mitigated and resolved. Next slide. That's it for me.

LETICIA CASTILLO: Yes, I think I am taking over. Thanks, Owen. Hi, everyone. My name is Leticia Castillo. I'm a director with ICANN Contractual Compliance. Next slide, please.

ICANN Org has produced a draft advisory to complement the amendments and provide guidance on the implementation and the enforcement of the new requirements should they be approved. The advisory which has been included as supporting information in the Public Comment page was developed with input from the Contracted Party House to ensure they see mutual understanding of the requirements and how they will be enforced.

In the advisory, we describe the new proposed requirements while reiterating that all existing obligations remain and will continue to be enforced. It expands on key terms related to the mitigation actions that a contracted party can take on or with respect to a domain name such as suspending the domain or redirect to a solution, and the other actions that Owen was just explaining.

It provides a few examples of different instances of DNS abuse and for each example the mitigation actions a contracted party can reasonably take to stop or to contribute to stopping the domain from continually being used for DNS abuse and to disrupt or contribute to disrupt in the course of the DNS abuse in relation to the domain name. We also explained the review that ICANN Contractual Compliance will perform to determine whether or not to initiate a case with the registrar or registry. And what will be expected from the contracted party to demonstrate compliance with the new obligations.

The next slide—next slide, please. Thanks—explains how as a part of our process, we will enforce these obligations via the processing of external complaints received through our dedicated web forms, but also through our monitoring and audit-related activities. The draft advisory explains how we will perform a comprehensive review of each case, including the information and records of complaints, and other available relevant information such as the data displayed for the domain through the RDDS, also known as WHOIS, DNS lookup to determine whether the domain name is active, etc. For any valid complaint, we will initiate a case with the contracted party which will list the information and records that are needed to demonstrate compliance with respect to a specific case and by when.

We will generally expect an explanation of the specific mitigation actions taken and how these actions were prompt and reasonably necessary to stop or to disrupt or to contribute to stopping or disrupting as it pertains to the case at hand. This includes any applicable explanation related to the disproportionality of actions and a collateral damage. If the contracted party determine that the evidence provided obtained was not actionable and therefore no mitigation actions were taken, we will also require an explanation as to why and conduct an assessment to determine compliance. As we do now, for different complaint types, including for existing abuse obligations, ICANN Contractual Compliance will select metrics related to the enforcement of this obligation should they be approved to keep the community informed.

This is all for the draft advisory. I am going to hand it over to Russ.

RUSS WEINSTEIN: Thank you, Leticia. Now I'm just going to wrap up with just a few more slides. These are the slides describing the process it takes to bring these negotiated and proposed amendments into effect. This is the process we call the Global Amendment Procedure to both the Registry and Registrar Agreements. It may sound familiar as we just used this procedure and are still in the throes of finishing it up or changes to the base Registry Agreement and the 2013 RAA and the Registration Data Access Protocol obligations, RDAP. We also used it once prior on the Registry Agreement back in 2017.

In a nutshell, the procedure calls for a negotiation to occur, which has occurred, a Public Comment which we've now launched. A vote by the contracted parties where we need majority approval from each of the registries and registrars. Board consideration approval, and then a notice making the changes effective. The Registrar Agreement is a little cleaner and that every registrar is on the same RAA. The Registry Agreement is mostly like that. We have the base Registry Agreement where most of our registries are a party to it. In a few legacy agreements that are still not using the base Registry Agreement, most notably, .COM and .NET are in that case. But both of those have already committed to take these changes as appropriate by way of the letter of intent that's included into their agreements. Back in 2020, as part of Amendment 3 of the .COM Registry Agreement, we agreed with Verisign on a letter of intent to accompany that agreement. And part of that was around helping develop and supporting and including DNS abuse obligations. That same obligation is now being proposed in the

.NET contract that's currently up for renewal and just finished Public Comment. All of the major TLDs will be covered by these changes should they go through, which is great because it covers almost nearly every registration in gTLDs. Next slide.

So I don't need to bore you with the details, but just a reminder that both registries and registrars have one voting threshold that must be approved. So they must review and approve these proposed amendments. We need essentially a two-thirds majority vote based both on fees paid and total TLDs. The fees paid are a combination of both the total TLDs and the registered names within those TLDs. That's from the registry side and you'd roughly have a two thirds vote of approval. Next.

From the registrar side, it's a much higher threshold. Almost 90% or roughly 90% of all the registered names and almost 90% of all registrars must vote yes to get these amendments approved. So we'll be doing a big outreach effort in conjunction with our Registry and Registrar friends to ensure that we can drive the votes to approve these proposed amendments as they're good for the Internet ecosystem. Next slide.

So overall process, I mentioned it at the beginning, but we did our negotiation, we're now in the Public Comment phase. We wanted to put this process into a timeline for you as well. I see my slides didn't quite work so well in the conversion here. But we'll do the Public Comment phase now between May and July. We'll review those comments both as ICANN and with our contracted party colleagues to determine if any changes are necessary before finalizing them. We'll

then bring them to a vote. And the target for that vote is in the fourth quarter of this year, October through December. And if we get to that majority threshold on both houses, as mentioned, we'll bring those to Board consideration, for the ICANN Board in the first quarter of 2024. If those are approved, we could be looking at these amendments on contract before this time next year, which would again be lightning speed at ICANN for such changes. So really exciting that we're here already and onwards and upwards from here. Hopefully, we get great feedback from you all in this Public Comment phase. Last slide.

So our last slide for today before we open up the Q&A—I know there's already been some active Q&A going on in the chat pod—is we have a DNS Abuse Amendment Outreach session with the contracted parties at ICANN77. So please come join us there if you're in attendance or are participating remotely. It's a 13:45 local time on June 13. That's on Tuesday. We'll be available for more discussion and Q&A at that session. So with that, I'd like to thank all my presenters here. Thank you all for attending. We'll open it up for any additional Q&A.

Bear with us as we take the chat. The questions are already coming into the pod. We're working through those. We're trying to get you guys answers and can also take them verbally.

YUKO YOKOYAMA: Russ, at this point, if I may suggest that we answer your questions verbally.

RUSS WEINSTEIN: Certainly.

YUKO YOKOYAMA: Okay. Then I will start reading from the top. This question is from Sivasubramanian M. Does the role of registry end with taking down a malicious domain as a mitigation measure when warranted by the degree of abuse if it is DNS abuse? All that is needed for the malicious party is to take a new domain name from the same or different TLD space. Wouldn't it help if the registry or registrars share information to identify patterns, fingerprints of the abusers, and help one another in identifying or dealing with abusive registrants malicious actors? Who would like to take this question?

RUSS WEINSTEIN: I can take this one for us. Thank you for the question. It's a good one. As we talked about up front, the core of this effort was to define a floor for DNS abuse obligations. For the purpose of a floor, what we did was create an obligation to mitigate the DNS abuse being observed on that domain name, whether in the registrar or in the TLD. We considered something like this to be outside the scope of what we were doing right now, but there is room for discussion along those lines in the policy discussion that could come later. So I encourage you to hold that thought. Thanks for the question.

YUKO YOKOYAMA: Thank you. The next question is also from Sivasubramanian M. Does it in any manner reduce the responsibility, accountability of the

registry/registrar if the abuse is spotted on the third or a deeper level of the domain name?

RUSS WEINSTEIN: Leticia, did you want to take this one?

LETICIA CASTILLO: Sure. Can you please repeat the question? Does that remove responsibility if the abuse is in the third or another level?

YUKO YOKOYAMA: Third or a deeper level of the domain name.

LETICIA CASTILLO: Well, the responsibility is to take the mitigation action when they obtain evidence that the domain name is being used for DNS abuse. So we will review all the details of the case. It is possible that the abuse is at the third level, the level we require the registrar to provide their assessment if we have obtained enough evidence that the domain name is being used to conduct the abuse. So it does not necessarily remove any of the obligations. But as with any other case, we will review all the details that pertain to the case at hand. And it's really hard to say yes or no as we keep saying not all size fits here.

RUSS WEINSTEIN: Thank you, Leticia.

YUKO YOKOYAMA: Thank you. The next question is from Brian King. Thanks very much, Russ. This was partially answered in the pod in writing.

That sounds like a welcome and refreshing change of approach. As a follow up, could you or ICANN please share the rationale behind the apparently different standards in the RA versus the RAA? Specifically, why in the RA the obligation turns on the RO's reasonable determination versus in the RAA the requirement is triggered when a registrar has actionable evidence? Would it be Russ to respond to Brian King?

RUSS WEINSTEIN: Sure. I'm happy to take this one. Thanks, Brian. So the language is slightly different. The main difference is recognizing the role of the registry and the registrar. We'd like to think of the registrar as the tip of the spear in combating DNS abuse. And so they have the direct relationship with the registrant. And so when they have actionable evidence, they can make that determination. The registry, they'll have reasonable evidence that they have actionable evidence and will either take action directly or may refer that matter to the registrar for them to take the action. So very slight nuance in the language but little difference in terms still requiring mitigation action by both the registry or the registrar.

YUKO YOKOYAMA: Thank you, Russ. Perhaps next two questions, we can bundle them together. Both are from Alan Greenberg. First one is when do the RAA changes take effect? Immediately or when the next RAA is signed up to

five years from now? And the second set of question is when do the RA changes take place for each registry?

RUSS WEINSTEIN: I'll take this one again, Yuko. Thanks, Alan. Good questions. I tried to cover this towards the end of the presentation there. But if everything goes as smoothly and according to plan, these could be on contract with the registries and registrars as early as the second quarter of next year. So this time next year, we could be looking at these amendments into effect. It's obviously dependent on getting through all of the steps in the process successfully from here on out. But like I said, best case scenario, we're looking at second quarter next year.

YUKO YOKOYAMA: Thank you, Russ. Next question is from Rick Lane. What percentage is Verisign's vote based on that criteria for registry passage?

RUSS WEINSTEIN: I'll take this one as well. Thanks, Rick. Sorry if I confused matters a little bit there. Verisign would only vote for the TLDs they have on the new base Registry Agreement, which is the TLDs they applied for in the 2012 round of the TLD program. Their legacy contracts don't vote or don't participate in the vote on the base Registry Agreement. But as I was saying, they've committed to taking these amendments via the letter of intent that's applied to both of their contracts. They've been a part of this process throughout, they're part of the negotiation teams and been fully supportive.

YUKO YOKOYAMA: Thank you. Next question is from [inaudible]. How is the registries and registrars able to effectively differentiate between technical DNS abuse and content-related abuse? At what level should DNS abuse be fought and prevented? Who should be in charge in defining this boundary?

OWEN SMIGELSKI: I will handle responding to this question. Thank you for this inquiry. So quite often, it's something that you can tell it when you look at it. So as we mentioned or Russ mentioned earlier during the presentation, this is a narrowly tailored definition of DNS abuse and what's going to be actionable in here. It is for phishing, pharming, botnets, and malware. Those are not content-related abuses. Those are something that's completely different. We're making these types of DNS abuse, ones that should be actioned by contracted parties, because this is something that everyone agrees upon. This is a widely used definition. This is something that is done around the globe, whereas content-related abuse can vary based upon jurisdiction and region and type of parties.

So again, it's not something that we're just ignoring, but it's not necessarily the focus of these abuse amendments. There will be additional action by the ICANN community. Again, this is just the first step. There's step two and beyond. And these types of issues can be discussed and considered by the ICANN community as we move forward.

Who's going to be defining these types of boundaries? Again, this is something for the ICANN community. But speaking as a registrar, certain types of abuse is content-related, we will take action, but sometimes we won't. Again, it's very specific based upon the type of content and the abuse. Thanks.

YUKO YOKOYAMA: Thank you, Owen. Does anybody from ICANN side wants to add anything? If not, I will go to the next question.

RUSS WEINSTEIN: No, I think Owen did great. Thanks.

YUKO YOKOYAMA: All right. The next question is from [Nojusad]. Isn't this detailed and comprehensive DNS abuse review and mitigation process within the ICANN community too slow to stop serious malicious attacks by cyber criminals? What strategies are there to ensure prompt spotting of abuse and action against it?

RUSS WEINSTEIN: Thanks. I can try and start with this one and maybe some colleagues can jump in. I'm not sure I would describe this processes as overly slow. What registries and registrars do on a regular basis, they have designated points of contact where they can receive reports of abuse from the community, from users, and are required to promptly take a review of those and then mitigate. They identify DNS abuse with

actionable evidence. Also, many registries and registrars also subscribe to various security feeds that provide information and intelligence about threats and DNS abuse occurring across the Internet space and look at those reports on a continuous basis and react to those as best they can.

Then additionally, both registries and registrars have requirements related to law enforcement and criminal activity. So when they have dedicated channels for law enforcement or other similarly situated agencies to report abuse or malicious conduct to them and they'll deal with those on a near real-time basis within 24 hours.

So I think what we have here is not a slow and overly complicated process for this DNS abuse. These are things that registries and registrars can identify and act on at the DNS level should it be necessary and they're prepared to do so. I don't know if Chris or Owen or any others wanted to add on to that.

OWEN SMIGELSKI: Yeah, Russ. I will follow up on as well. It's good to point out, yes, this is not necessarily something that is slow. But one thing I would like to highlight is it's difficult to predict what will be abusive. That's a big concern, especially from registrars and registries, is we don't want to assume that somebody's guilty before they've done anything. It can be very disruptive to stop a domain name. From a registrar side, if we are suspending a domain name, we're actually breaching our contractual relationship with our customer. So it's something that is often by the nature of it has to be reactive as opposed to predictive. So that's why

there are a number of ways to report abuse and to have people report abuse to registrars and registries. But it's not something that has to take days, weeks, months. It's something that can be measured in days, hours, if not minutes, depending upon how the abuse is identified, how it's reported. And it is something that I think what we're doing here is we're all working together, we're trying to figure out ways to take action. And then also make sure that all contracted parties must take these actions. The things that have been identified in this presentation are actions that a lot of the registrars and registries are already doing. And what we're doing is we're kind of codifying those and putting those in so that it'll be an obligation for all registrars and registries to take. So hopefully moving forward in the future, there'll be a more industry-wide approach to being able to stop DNS abuse quickly. Again, this is just the first step. There's much more for us to do in the future. Thanks.

YUKO YOKOYAMA: Thank you, Russ and Owen. I don't see any other questions in the Q&A pod. So I'm going to kick it back to Michelle.

MICHELLE WILSON: Thanks, Yuko. If there are any other questions, if you'd like to speak, please raise your hand in Zoom. And once the session facilitator calls upon your name, kindly unmute your microphone and take the floor. Before speaking, ensure you have selected the language you will speak from the interpretation menu. Please state your name for the record

and the language you will speak if speaking a language other than English.

YUKO YOKOYAMA: Thank you, Michelle. I do see Jonathan Zuck's hand. Jonathan, please unmute your microphone and please ask your question.

JONATHAN ZUCK: Thanks a lot. Jonathan Zuck here from the ALAC. My question was in the pod and got answered, I guess, in text in some way. But I feel like it's sort of misses the mark. And I haven't read the advisory, and so there's homework for me to do as well.

But part of what I believe drove this change is, as Owens said, to try and get some sort of normalized reaction to DNS abuse complaints. There had been conversations in the past that those that fell outside the norm or that were more habitually slow or whatever the best term is, sometimes we've used the term bad actors but that's fallen under misuse, but the ability for Contractual Compliance to take action on contracted parties that, for one reason or another, refuse to respond promptly. I guess my question is does Contractual Compliance believe that these changes in the discretion offered to the registrars and registries give them sufficient tools that given a pattern of disregard, I guess, for this normalized process have the ability to suspend or revoke a contract for an offending registrar or registry? I hope that question makes sense.

YUKO YOKOYAMA: Thank you, Jonathan. Who would like to take this question?

LETICIA CASTILLO: Sorry, I was talking on mute. I can start, and then Jamie who is also with us can add if he sees fit. So the amendments allow for sort of flexibility and recognize that the appropriate mediation action may vary, but all actions should aim to either stop or disrupt the name from being used for DNS abuse. So when we initiate a compliance case, we will request evidence that those mitigation actions have been taken and properly taken, taking into account all the details that's around the case at hand. And if that evidence is not provided, we will use our standard process and use it to enforce it.

I'm not sure if I am answering, and like I said, Jamie can chime in. But we will enforce the requirement to take those mitigation actions when the circumstances that are explained in the RAA and RA take place. That's explained more in detail in the advisory.

JAMIE HEDLUND: This is Jamie. Thanks, Jonathan, for the question. I don't really have much to add to what Leticia already said. But if you have any further questions, I'm happy to take those now or offline when there is a lot of information in the advisory on how we're going to enforce these new amendments. This is from a compliance perspective. This is a significant change or would be a significant change if these amendments become effective. It is, as others have recognized, a first step and one in which we will gain experience over time and report

that experience to the community in addressing DNS abuse and implementing these new obligations, assuming they get approved.

JONATHAN ZUCK: Thanks.

YUKO YOKOYAMA: Thank you, Leticia and Jamie. I am not seeing any other hands. Should we give it maybe 30 seconds before we close out? Still no questions in the pod? No hands. Russ? Oh, actually, one question just popped in in the Q&A pod. Yes, this question is from Steinar Grøtterød. Will any evidence be checked towards the DAAR data?

OWEN SMIGELSKI: I can start up and then pass off to John. So thank you for the questions, Steinar. And certainly the DAAR data in the reporting that ICANN does is very helpful and can help show what the context of DNS abuse is. But speaking of as a registrar, I don't have access to DAAR. I'm not looking at that. It's not something that we consider … An abuse complaint should be well-evidenced and actionable. We should be able to look at that complaint and be able to take the action that's needed. We shouldn't have to go look up stuff elsewhere or consult something else or whatever. So that's why we put these requirements in there to make sure that there is this evidence that's provided because sometimes it's difficult to see what something is. It may be geo location specific. So that's why we want that. Now, I guess I'll pass off to John so he can speak more about DAAR. Thanks.

JOHN: Thanks, Owen. So the Domain Abuse Reporting tool, DAAR, is based on reputational data. It's what people are saying about domain names. It's not necessarily backed up by strict evidentiary data. Each of these reporters have different evidentiary standards, some stronger than others. So no, it won't be directly connected. DAAR as reputational data is indicative. It gives you somewhere to go look, to follow up looking for evidence is not evidence of itself. We have other projects within the office of the CTO, something we call DNS TICR that has been running for a while and actually reports things to registrars based on evidence that are pretty much always actioned. But DAAR in itself will not be a major tool for presenting evidence.

RUSS WEINSTEIN: Thanks, Owen. Thanks, John. Sorry, Yuko?

YUKO YOKOYAMA: I was just going to say there is no more questions in the pod and I still don't see hands. So handing it back to you, Russ.

RUSS WEINSTEIN: All right. Well, thank you, everyone. The Public Comment is available for you. So please go take a look at the documents and give them a review and share your feedback with us. If you're going to be in D.C. or attending the meeting remotely, please join us for the session on Tuesday the 13th where will again go through this material and have a discussion with you all. But thanks again and have a great ICANN77

Prep Week. Safe travels to those traveling to D.C. We'll see you there. Bye now.

MICHELLE WILSON: Thank you. Please stop the recording.

[END OF TRANSCRIPTION]