

---

ICANN73 | Prep Week – Contractual Compliance Update

Wednesday, February 23, 2022 – 13:00 to 14:00 AST

MEDHI KURDMISTO:

Hello, everyone. My name is Medhi and I'll be moderating this chatroom today. In this role, I am the voice for the remote participants, ensuring that they are heard equally with those who are in-room participants. I'll post these instructions in the chat as well, but when submitting a question that you would like addressed in this session, please provide your name, affiliation if you're representing one, and start your sentence with the word <QUESTION>. When submitting a comment that you would like me to read out loud on the microphone, please provide your name, affiliation if you have one, and start your sentence with the word <COMMENT>.

Text outside these quotes will be considered as part of the chat and won't be read out loud on the mic. We'll address all questions and comments at the end of the presentation for fluidity's sake. Any questions or comments provided outside of the session time will not be read out loud. With that being said, we can kick it off with Jamie.

JAMIE HEDLUND:

Sorry about that. Having technical issues with the mute button. My name is Jamie Hedlund. I'm Senior Vice President for Contractual Compliance and US Government Engagement. Thank you for joining this pre-ICANN73k webinar on contractual compliance.

---

***Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.***

---

First, I'd like to give a quick overview of the agenda and the presenters. Jonathan Denison (or JD) is Director for Contractual Compliance based in Los Angeles will introduce new reporting that we will be publishing soon.

Leticia Castillo, Director for Contractual Compliance, also based in Los Angeles, will then provide an overview of registrants complaints, protection and enforcement notices since the pre-ICANN72 webinar. She will also discuss our efforts to enforce existing abuse obligations.

Yan Agranonik, Senior Manager for Risk and Audits, will then discuss recent audits of registry and registrar compliance with DNS security threat obligations.

Finally, JD will close with a summary of some of our recent outreach activities. Next slide, please.

Before we get to the [inaudible] presentations, a brief summary of what we do at Contractual Compliance. ICANN has agreements with domain name registries and registrars. Among other things, these agreements incorporate the policies developed by the ICANN community to help preserve and enhance the security, stability, and resilience of the Internet's domain name system.

Our role is to ensure that registries and registrars comply with the commitments in their agreements. We enforce the agreements through resolution of complaints through proactive monitoring and through audits.

---

We also engage in education and outreach activities around the globe to help ensure that there is a common understanding of the obligations and agreements among contracted parties and interested members of the community.

With that, I will turn it over to JD to talk about our new reporting. Thank you.

JONATHAN DENISON:

Hi. Thanks, Jamie. We can go to the next slide. So, I'm actually sitting in for Pamela Howard today. She's our Metrics and Reporting guru and we've been working with her to come up with new types of metrics and reports.

If you've been following us for a while now, you'll know that compliance has moved into Salesforce in the naming services portal, which we call NSP Compliance for our section. Basically, moving into the system has allowed us to capture data at a more granular level, and as a result, we can provide more information publicly in our metrics and reporting pages on our compliance site.

So, what we did is we came up with a few new reports. Basically, it's going to give you an idea of the complaint volumes and related compliance actions. As mentioned, it'll be launched shortly, and essentially it'll be a 12-month rolling series that we'll be updating monthly, beginning with January 2021.

The three new reports are registrar and registry overview activity across all complaint types. So this will give you a bit more information

---

on the overall volume across all the complaint types, and you'll see volume of complaints closed due to those having fallen outside of ICANN's contractual scope and those will be the ones that were never forwarded to the relevant contracted party.

Then you'll also see the volume of notices compliance did send to the contracted parties within the informal and formal resolution stage of our processes.

If you don't know, the informal is where compliance contacts the contracted party and resolved issues in a non-public manner, and the formal resolution stage is when essentially these issues are not resolved within the informal phase and are escalated and become public and those are the things you'll see where we published our breach notices, termination suspensions, those kinds of things.

Then another type of report is the top five complaint types and reporter type. So these will detail the top five complaint types for the same time period. These are generally the majority of the complaints that compliance receives, and along with those numbers, we'll provide a brief description of the obligations that are enforced with each complaint type. So you'll get to know a little more detail about what exactly those complaint types mean and the types of contractual issues involved.

Also, you'll see details about the reporter type or the complainants, and those are selected by the reporters when they submit the complaints, so that way you can see whether it's coming from a

---

particular community or whether it's a registrant, those types of things.

Then, finally, we have a new abuse complaint type report and that will be like two tables. It'll be the volume of abuse complaints received and it'll kind of detail the alleged abuse activity associated with a domain name. Those are also selected by the complainant when they submit the complaints. So essentially it's more or less what the complainant has selected as what they think the type of abuse the domain name is engaged in.

Then, the second table will be volume of closed abuse complaints. It will detail those that are closed without having to contact the contracted party because it was out of scope. It will also show those closed after obtaining evidence of compliance from the registrar.

That's kind of the gist of those new reports there. Again, it'll be published shortly, so keep an eye out and, of course, we'll be announcing when it does get published. So, thank you.

JAMIE HEDLUND:

So, before we get to the next section, I just want to mention, I just want to add on to what JD just described. One of the reasons we're doing the new reporting is to take advantage of the great amount of data that we have access to through NSP Compliance.

The other is because we recognize that a lot of our prior reports, which will be retired, had very little viewership, at least according to Google Analytics. So we're trying to do two things. One is to show the data

---

that we have, to show it over a period of time so that if there are trends that can be identified, those will be easy to see and could be of interest to the community.

When we do come out with the new reporting, which will be shortly, there will be an announcement in the blog and a description of what's in the reports. So I really encourage, if you are interested enough in compliance to show up for this webinar to check out the new reports and let us know if this information is interesting, it's not interesting, if there's different information you'd like to see. There will be in a blog information on how to provide that feedback, but of course we are always interested in community feedback and we're interested in providing reports that we hope will be of use to the community. Thanks.

LETICIA CASTILLO:

Hi, everyone. This is Leticia Castillo and during this part of the update, I am going to talk to you about the main type of complaints that we have been receiving from registrants since our last update using these new metrics that JD and Jamie were talking about.

The actions that we have been taking to enforce some of the contractual obligations that most directly protect registrant's rights and some details regarding the former notices of breach, suspension, and termination and have issues since ICANN72.

---

With that, let's move to the next slide, please, and talk about complaints that we have been receiving from self-identified registrants from September 2021 through January 2022.

It is very consistent with what we saw in prior updates. Domain name transfers and [renewal matters] continue to be in the top three in volume of the complaints that we have received.

You can see part of the 4,923 complaints received in this reporting period, 938 the person filing the complaint indicating that at the time of submission he or she was the registrant of the domain name subject to the complaint, and 305 he or she was the former registrant. This happens often with domain renewal issues or unauthorized transfer issues, for example. And in 282, the person submitted the complaint indicated that they were the authorized representative of the registrant, either current or former. And you can see that most of them were submitted through the transfer form.

Within the transfer complaint, we do enforce the contractual obligations are enforceable under the transfer policy, and a common example of this is a scenario where the registrant wants to transfer the domain name from one registrar to another, and for that meets the AuthInfo code, which is a password that is technically needed to enable the transfer and also needs to remove any transfer lock that may exist on the domain name. We contact the registrar and indicate that registrar did not [inaudible], so they come to us.

But there are also other types of complaints that we address under this complaint type. Those related, for example, to requests to change

---

the registrant information, also unauthorized transfers of registrar and/or registrant, and also other less common matters, like those related to the transfer emergency action contact (or TEAC) which is a contact registrars must have for use of ICANN [inaudible] registrars and registries that require a fast response in relation to transfer matters.

Examples of renewal matters are complaints where the registrant indicates that they have paid for the renewal or the redemption of the domain name but the domain name has not been renewed or has not been redeemed. But also other obligations that are, for example, related to ensuring that the registrant knows that the domain name is about to expire with enough time for the registrant to act on it.

When it comes to complaints submitted by self-identified registrants and abuse, these are mostly invalid complaints. As you can imagine, people do not report their own domain names for abuse. These are normally closed as invalid or recategorized.

For instance, it can be a complaint filed by a self-identified registrant, an abuse complaint saying the registrar is being abusive because they are charging me double for a hosting package that I purchased. This is an invalid complaint. It doesn't fall within the abuse report handling requirements within the RAA and there is no ICANN policy or agreement that relates to hosting services. So what we do is we close the complaint, we inform the complainant why, and other avenues that he or she may wish to pursue through to have their issue resolved.



But it can also happen, they're saying, "I paid for the renewal of my domain name. The registrar took the money and did not renew. This is abuse." So it will not fall within the abuse complaint type in our system, in our metrics, but we will move it from the abuse queue to the renewal queue and we will address the contractual compliance matter within that correct queue, and of course we will inform the complainant about it.

We also added some other interesting information here to provide a little bit more context. Most of the complaints received during this period had the reported type "other". This is an option in our forms where there is no specific [criteria] for the complainant. For example, someone submitted an abuse complaint to us, to the [inaudible] user—maybe it's not a registrant, it's now law enforcement, it's an information security professional. So that person will select the option "other" within our complaint form.

And the second type is actually us, where we detect non-compliance and we do not wait for an external complaint to come to us. For instance, if we see registration data displayed for a domain name that is redacted per temp spec that does not include a webform or the email address, we create the case and we initiate the matter with the registrar or if we see that a registrar is not providing a WHOIS service, again we will initiate the complaint ourselves if we only see the case ourselves without waiting to receive an external complaint.

---

And there are other cases that we saw from ICANN’s own monitoring of contractual obligations, such as data escrow that I will explain a little bit more in our next slide.

So, to all these complainants—not to ourselves, of course—but to all these external complainants, we will either explain why the complaint is not within scope. Like I said, we will provide other pertinent information and other avenues they may wish to pursue. Or if the complaint is fully form, we have all the evidence and all the information that we need and it refers to an obligation that is within our policies and agreement, we will start the process with the contracted party, which takes me to the next slide, please. Thank you.

So, this slide includes notification sent to the registrars for three complaint types that most directly address the protection of registrants and how they were resolved. These do not include oral notifications sent across all complaint types.

By the way, we have approximately 30 complaint types, just to give you an idea, and they do not include those [inaudible] that we sent to complainants where valid complaints without information and additional [inaudible] were needed.

As you can see, for the transfer cases that we closed from September 2021 through January 2022, we closed them because the registrar demonstrated compliance with the applicable contractual requirement. That’s the [inaudible] cases that we closed.

---

And for 28% of the cases, they were closed because the registrar provided the AuthInfo code—the password that I was talking about before—removed the lock and/or the transfer was actually completed after we contacted the registrar, and at the time we were closing the case.

An example of registrar demonstrated compliance here, because I know it's kind of a broad code, could be where it's a complaint about completing a change of registrant—change of registrant information. We get evidence and an explanation from a registrar that the steps are required within the policy were taken, that parties were informed, that they got the confirmation from relevant parties and the changes were performed.

For renewal cases, you can see that we closed, again, 60% of them—the vast majority because the registrar demonstrated compliance with the requirement.

For instance, the registrar provided a copy of all the renewal reminders that must be sent to the registrant, that the website resolution was interacted, which is the bigger warning for the registrant to see that there's something going on that they need to take action and renew the domain name to prevent [it's lost].

An example of corrected its non-compliance could be the registrant informing us that a technical issue prevented them from sending mandatory renewal reminder, and at the same time confirming that the issue had been remediated and that they had reached out to all

---

affected registrants to let them know and make sure they were aware of the expiration, etc.

And in 12.5% of the cases, the domain had been renewed by the time we were closing the complaint and after we contacted the registrar and it was because the domain name, was about the domain name needed to renew.

As I briefly mentioned before, we also enforce the obligations that are related to data escrow. According to the Registrar Accreditation Agreement, the registrar must deposit the data associated with the gTLD domain names that it sponsors with a data escrow provider, a formal [certain] schedule and formal requirements. This way, if the registrar is terminated or stops operating, the domain name can be recovered as the domain names themselves and the data associated with them is safely stored by third-party by the data escrow provider.

So you can imagine how the lack of [deposits], the lack of compliance, for one registrar depending on the number one domain name it sponsors can affect hundreds or thousands—sometimes even more—domain names and registrants.

You can see on the slide, 98% of the cases that we closed were closed because, upon being contacted by us where we addressed the cases, the registrars made the deposits and those were closed. Can we please move to the next slide? Thank you.

So, most cases are closed within the informal resolution stage, which is generally the stage—JD was mentioning it before as the confidential

---

part of work. Generally comprises three notification and a couple of phone calls through which we communicate to the contracted party a list of items that are necessary to demonstrate compliance. We also provide a copy of the complaint and any evidence that we have regarding the complaint. And most cases are actually closed, resolved with the formal stage because the contracted parties do timely provide evidence of compliance at that point.

But if the informal resolution process is exhausted and there's no resolution, we escalate the matter to the formal resolution stage of our process where a Notice of Breach is issued to the contracted party. This notice is published on our website, states the specific areas of non-compliance, what is needed to be done by the contracted party to cure. In most cases, it is related to the specific complaint that resulted in the breach, but also to prevent future failures as well and by when. And failure to fully and timely address this notice results in a suspension or termination of the accreditation for registrars or termination for registry operators.

You can see there that, since September 2021, we have issued six formal breach notices. The notices include failure to comply with several obligations, such as providing WHOIS service, escrow and data, implementing UDRP decisions or investigating and responding to these reports. One breach was not cured and escalated to termination of the registrar's accreditation. Two were partially cured [inaudible] and they escalated to suspension of the registrar's accreditation for three months.

---

And for those that don't know, during the suspension period, what happens is the registrar is not allowed to get new registrations or accept in-bound transfers. It must cure the remaining violations by a deadline to maintain the accreditation. If that doesn't happen, it can still escalate to termination of the accreditation.

That bottom of the slide, you have a link to our enforcement page that includes all of our published notices, in case you want to read them.

Now we can move with the next part of our agenda. We have the enforcement of contractual obligations related to DNS abuse. Can we move to the next one please? Thank you.

This is in Section 3.18 of the Registrar Accreditation Agreement. This [resolution] are to take reasonable steps and prompt steps to investigate and respond to abuse reports that involve domain names that the registrar sponsors and that are submitted by any user. There are also requirements related to review reports within 24 hours when they are submitted by law enforcement or consumer protection or similar entities within the registrar's jurisdiction. Also, the obligation to display abuse contact and a description of the abuse procedures for [inaudible] how to submit an abuse complaint to the registrar and how those abuse reports will be handled.

There are also obligations to maintaining records related to the investigation of the response to the abuse reports and provide them to ICANN upon reasonable notice.

---

So, when we investigate an abuse complaint, in general we request an explanation and evidence records concerning how the registrar addressed the specific abuse report as required by the RAA and consistent with registrars on the domain name use and abuse policies.

We will request as much information and clarifications as needed to ensure that this was done and that we have evidence of it. However, it is important to keep in mind that our enforcement authority is limited to the requirements in the RAA. We have no authority to, for example, ask the registrar to suspend a domain name or remove its content or transfer the domain name from one registrant to another in response to an abuse report because those are not actions that are mandated by the RAA.

Here are some metrics concerning our enforcement of these obligations from September 2021 through January 2022. We received 1,426 abuse complaints and sent 273 abuse notifications to registrars that requested the evidence and the explanation I mentioned before.

We closed 254 cases with registrars because they demonstrated having taken the steps to investigate and respond to the abuse report. In 37% of the cases, they suspended the domain name or domain names that were subject to the complaint. It's very common for us to have an abuse report or abuse complaint that includes a list of domain names.

And in the rest, they took other steps, contemplated by their abuse policies. For instance, they contacted the registrar who removed the abusive content from the website or they contacted the registrant who

---

took whatever actions were needed to remove the domain name from a blocked list [inaudible].

We also closed 1,216 out-of-scope complaints without being able to initiate an investigation with the registrar and you can see here in 73% of the cases because the complainant did not provide the evidence needed for us to initiate the process, meaning there was no evidence that an abuse report was ever filed with the registrar prior to submitting a complaint to us.

We're talking about the first requirement was to investigate and respond to the reports, so there must be an abuse report filed with the registrar to trigger this requirement.

However, many complainants misunderstand ICANN's role and authority and they believe that they can report the alleged abuse or illegal activity to us and they actually ask us directly to delete domain names or to remove certain content. Sometimes they ask us to transfer the domain names to them, etc., something that is not within our scope. We do provide all types of clarifications.

And in 5%, the domain name was already suspended at the time we [inaudible] the complaint and 10% involved country code top-level domains or ccTLDs, which are not within our scope because ICANN does not accredit registrar or set policy for ccTLDs.

The remaining smaller percentages were cases like the case was already ongoing, it's a repeated complaint, or it was about a domain name that was not even registered, etc. And what we did is, like I said



---

in all these cases, we provide any explanation that can help the complainant find the right way to proceed. We provide means on how to find the registrar and find their abuse contact information in case they want to submit a report to the registrar, etc. Let's move to the next slide, please. Just very quickly. Thanks.

In addition to addressing the external complaints concerning abuse obligations under the RAA, just to provide a few examples of how we also practically enforce requirements in this area, not including the audits that Yan is going to explain in a few minutes.

For example, where we do not see the abuse contact displayed on the registrar website or in WHOIS response, like I mentioned before with other cases, we will address the matter with the registrar in a proactive manner.

Yes, this is all for the enforcement of DNS obligations [inaudible]. We have included in appendix. At the end of this presentation, it will be posted to the website that includes some more metrics about abuse, also about access to registrant data that comprises a longer period of time in case you want to review [it as well].

That's it. Yan?

YAN AGRANONIK:

Yes. Hi. This is Yan Agranonik. I am responsible for compliance audits and I'm going to talk a little bit more about the most recent registry audits and the DNS abuse registrar audit.

---

First, registry audit. Basically, what we've done is we looked at obligations related to Spec 11 (3)(b) for all the registries, specifically the questionnaire in the RFI—request for information—that was sent to them is published. You can see it on our website, as well as the report that shows the results of the audit.

The idea behind the audit was to see what, if anything, registry operators are doing related to the spec 11(3)(b), meaning what security threat monitoring [inaudible] reports are performing.

We know that in spec 11(3)(b), this requirement is specifically written out for new gTLDs, but we also send a similar request for information and questionnaire to legacy TLDs, which do not have this obligation or at least at that time.

Briefly, what we try to do is we try to compare the reports that have been provided to us from registries to publicly available information. What I mean by publicly available information is reports from reputation block lists (or known as RBLs). Yes, we had a discussion about how reliable these are and this discussion and the difference between what we've seen in registry reports versus to what we see in reputation block lists is reflected in the published report. So you can read for yourself.

Briefly, results of this audit was where most of the registry operators do perform some type of monitoring and they do keep reports that show what exactly has been done. Only 5% of the registry operators did not do anything in this area, and basically at that time, their belief

---

was the income was so low that it's not really necessary to perform any monitoring.

Brand TLDs don't have any abuse whatsoever because they have procedures in place that allow only registrations for trusted parties.

Also, we have seen that different registry operators use different methods to monitor. Some do have in-house tools and software to do that and some engage third parties to do that.

For legacy TLDs, again, we did not receive sufficient information to understand what exactly do they do. We have some information but not as good or solid as gTLDs. Next slide, please.

Most recent registrar abuse obligation audit. The scope here was to look at the obligations listed in section 318 of RAA. What we've done is we looked at all obligations in 318 and verified that registrars are compliant with them. Most typical ... Typically, registrars have some type of response to 318, but as you can see, quite a few have deficiencies. By deficiencies, I mean verified absence of compliance with certain obligations. Some of them are more serious and some of them are less serious.

Examples: email or some type of contact information is missing from the website or WHOIS for the domain related to abuse contact. Phone number is missing or not responsive. Email is listed but it's not responsive. We sent test emails to see if there is any kind of response. LE, law enforcement, agency contact information that should be responsive 24/7 either do not exist or is not responsive, but there is a

---

reason behind that. I'm not going to explain what's the reason behind it but it's in the report that you can read.

Also, some of the registrars are performing some actions against reported abusive domains but there is no report retained.

So, in the scope, we have 97 registrars and 78 out of them not in scope. 97 registrars have deficiencies and [70] completed remediation before the end of the audit and we actually verified that. And 19 gave us a timeline explaining when deficiencies will be remediated, and by now we have confirmed that it has been done.

It was an interesting audit, let's put it this way. But everyone cooperated and I hope that we both learned a lot from this activity and I encourage everyone to read full reports that are published on our website. And we'll continue questions at the end of this session.

JONATHAN DENISON:

Thanks, Yan. JD here again. Just real brief just describing outreach activities since our last reporting. September 2021, upon request from [inaudible] registrars, the clients team in Istanbul provided an update on the results of the audit and of registrars compliance with DNS abuse obligations. It was in collaboration with the Global Stakeholder Engagement team and was in the Turkish language.

Basically, during these sessions, provide clarifications on abuse obligations for registrars through the RAA and just general questions about the audit program related to the abuse obligations.

---

Beyond that, we still do our standard outreach/conferences that we have with contracted parties that are a little bit more informal but basically done during the course of regular work and those are just individualized as needed, just to clarify obligations, answer questions, whether it's about the obligations themselves or process, stuff like that. Those obviously are not published because those are on an individual basis. But we continue to do those regularly.

JAMIE HEDLUND:

We've gotten four questions in the queue and we will take them in order. We got these in the Q&A pod. I don't think we got any in the chat, but if you have questions, please either add them in the chat or in the Q&A pod. JD, do you want to take the first one?

JONATHAN DENISON:

Sure. Chokri writes, "It's possible to integrate complaint and abuse reports in the ICANN open data platform." It's an interesting thought. Probably a couple of issues there. Firstly, how to go about even doing such a thing, and secondly timing would be an issue there. But we can take this back. Thank you.

JAMIE HEDLUND:

Yeah. Just to add, that data absolutely should be in the open data platform, the data that we publish. There's just no timeline that I'm aware of to do it but it is something we'll look into and we appreciate the importance of access to raw data for the community to manipulate.

---

I'll take the next question from Mark. "How does a team interpret the difference between the small number of abuse complaints in face of the significantly larger amount of abuse that we empirically observe on the Internet? What is missing for the system to be a better avenue for abuse complaints?"

Mark, that's an excellent question and one that I think is often actively discussed in the community. In response, I would say a couple of things. One is ICANN Compliance and ICANN Org does not have jurisdiction over all abuse on the Internet. For example, abuse that happens on social media platforms is apparently a very large percentage of abuse, at least according to governmental consumer protection agencies and we have obviously unique identifiers have nothing to do with social media platforms and they're not registries or registrars, or when they are, they act as that and not as social media platforms. So there is that.

The other is it's interesting when you start looking at types of abuse [inaudible] COVID and has been [inaudible] elsewhere. There were—

JONATHAN DENISON: I think you're breaking up, Jamie.

JAMIE HEDLUND: Percentage was quite small. Finally, we do get complaints. We do get a lot of complaints. Unfortunately, many of them are not fully formed. That means that we don't take them any further because, often, the complainant hasn't tried to resolve the issue with the registrar. The

---

registrar’s obligation is to investigate and respond reports of abuse. If they haven’t been given the opportunity to investigate and respond, there's no violation and we obviously encourage anyone coming across abuse to report that to the registrar.

Once it is reported, we do investigate to see if the registrar has fulfilled its obligations under 3.18 of the Registrar Accreditation Agreement. We recently publicly breached a registrar for failing to fulfill its obligations to investigate and respond and will do so again in the future.

While we do proactively monitor for abuse and look into reports of abuse that may not come from complainants, as well as those that do come from complainants, we only see what we see. So we encourage those who do come across abuse to submit complaints. First, try to get the registrar to address it directly, and if they don’t, then submit it to us and we will respond. We’ll investigate.

So, I hope that’s helpful. JD, you want to take the next one from Alan or Leticia?

LETICIA CASTILLO:

Sure. “What complaints result in having the registrar deposit escrow data? How does a complainant know that escrow data was not deposited?” Thanks for your question. Medhi, is it possible to go to slide nine? Let me clarify there. If it’s possible, thank you so much.

So, in [inaudible] I was talking about the complaints that we have been receiving from self-identified registrants, whereas in this slide I

---

was talking about cases initiated with contracted parties to address contractual obligations that most directly address the protection of registrants. So, we have complaints that were submitted by registrants but we also have, like the case of data escrow, that resulted from ICANN’s own monitoring. We do not have external complainants reporting data escrow issues to us. We have the data escrow providers sending us exception reports that we review. We have staff that is trained and dedicated to these types of obligations and they review this report and they create the cases and address them with the registrars until they are resolved. So, I hope that clarifies the point.

YAN AGRANONIK: Can you guys hear me?

MEDHI KURDMISTO: Yeah, we hear you, Yan.

YAN AGRANONIK: I can respond to the next question. “You report that 97 out of 126 registrars has remediated problems with operational issues regarding abuse contact and such. How do you verify operational status and ensure that it continues to be operational?” Excellent question.

It’s not just about registrars. It is also applicable to registries as well. Basically, you’re asking, all right, they fixed the issue that you found during an audit. How do you know that the issue did not come back?



---

The answer is we only verify that they've corrected an issue either during an audit or shortly after. It is possible that some contracted parties did it just to satisfy an audit and we have seen it in the past, meaning there is an issue, it is addressed. A couple of months later, we somehow found out that the issue is still there. Simple example.

There is a phone number published to contact contracted party about abuse. It was not operational during audit. Then it became operational. Everything works fine. Then a couple of months later, the phone number is not responsive again or just disappeared from the website or WHOIS.

If we find out that it happens and we do find out that it happens either via complaint submitted by someone or via next audit, then the issue is escalated really hard. Contracted party usually gets on the audit list every time we do the audit as a result of that and we also begin checking this particular issue from time to time. I hope this answers your question.

Next question is: "When do you envision next, when next registry operator and registrar audit and at what scale?"

We are planning next registry operator audit now, which we plan to initiate sometime after ICANN meeting. The scope would be the full scope, not just abuse or any selected articles. So it's a full scope registry audit that we plan to initiate sometime after ICANN meeting. That's it.

---

MEDHI KURDMISTO: Two more questions in the Q&A pod. One from JP saying, “Following on from Mark, 3.18 of RAA focuses on the registrar’s effective processing of abuse claims versus the underlying abuse allocation itself. Are there any situations beyond security, stability, resilience of the DNS where Contractual Compliance addresses abuse specifically?”

LETICIA CASTILLO: I can take it. Thanks for your question. So, we do not address abuse specifically. We ensure that the obligation to take steps to investigate and respond to any abuse report is complied with, along with all the other obligations I was mentioning before, having abuse contact posted, keeping records, etc. But we do not address specific abuse.

MEDHI KURDMISTO: Thanks, Leticia. One more question in the Q&A from Dmitri. “When approximately will registration be available in .MM ccTLD?”

JAMIE HEDLUND: Hi, Dmitri. Unfortunately, we can’t answer that. We enforce agreements in the gTLD space, not ccTLD. So you’ll have to ask that of the ccTLD itself. We’re happy to get you contact information if that’s helpful.

MEDHI KURDMISTO: Thanks, Jamie. Then there is one comment in the chat that I’m going to read out loud. This is from Jothan Frakes. “The registries and registrars have worked together as part of their efforts to combat DNS

---

abuse and have drafted a document to aide in reporting of abuse and understanding the process in order to educate and [improvise] the productive nature of reporting abuse.” Then he’s provided a link to a guide. “This hopefully will reduce, misdirect reports of abuse and ensure there is actionable information within reports.” Thank you very much, Mr. Frakes.

JAMIE HEDLUND: All right. I think that wraps up questions from the Q&A pod as well as the chat. Thank you all for joining. I hope this was helpful and please do look for the publication of the new reports which will be out any day now. Thank you, again, and have a great ICANN73.

MEDHI KURDMISTO: Thank you, all.

LETICIA CASTILLO: Thank you.

JONATHAN DENISON: Thank you.

**[END OF TRANSCRIPTION]**