ICANN72 | Prep Week – Contractual Compliance Update
Thursday, October 14, 2021 – 14:30 to 15:30 PDT

MEHDI KURDMISTO: Hello everyone. My name is Mehdi Kurdmisto and I will be monitoring this chat room. In this role, I'll be the voice for the remote participants ensuring that they're heard equally with those who are not the in-room participants.

When a submitting a question that you want me to read out loud on the microphone during the Q&A, please provide your name and affiliation if you're representing one and start the sentence with “<question>” and end it would “<question>.” And I’ll be pasting these instructions in the chat.

When submitting a comment that you want me to read out loud on the microphone, once again, please provide your name, affiliation if you have one, and then start your sentence with “<comment>,” end it with “<comment>.”

Texts outside these quotes will not be considered as part of the chat and won't be read out loud on the mic. Any questions or comments provided outside of the session time will not be read out loud and all chat sessions are being archived and follow the ICANN expected standards of behavior.

With that being said, I'm going to pass off the mic to Jamie Hedlund.

JAMIE HEDLUND: Thank you, Mehdi. My name is Jamie Hedlund. Welcome all to this pre-meeting webinar on Contractual Compliance. I'm the head of the function and I'm really glad to be able to spend this time with the community. I do hope you will ask us questions, which we'll respond to at the end. And any questions that we either can't or don't get to, we will follow up and provide answers to those.

ICANN Contractual Compliance plays an important role in the community's policy development work. We're at the end, we ensure that the policies developed by the community, accepted by the Board and implemented are in fact implemented by the contracted parties.

We also ensure that they abide by the obligations in their respective agreements. And we do these things primarily in three ways: through proactive outreach, through processing complaints, and through audit. We will hear about all these things in the next session. Let me just quickly go over the agenda. We'll spend some time talking about recent enforcement actions on the temporary specification. We'll get an update on the recent registrar DNS security threats audit. We'll get an overview of recent enforcement actions, and then finally, a quick summary of some of the outreach activities.

With that, I will turn it over to Amanda Rose who will give an overview of the temporary specification and Compliance's efforts in that area. Thanks.

AMANDA ROSE: Thank you, Jamie. We can go ahead and advance to the next slide. As Jamie's mentioned, I'm going to be presenting the temporary specification update. Essentially, for the temporary specification for gTLD registration data, that is enforced via the interim registration data policy which went into effect May 20th of 2019 that essentially ensures that contracted parties, registrars and registry operators continue to implement the requirements under the temporary specification.

This isn't much new information, but wanted to give everyone an outline of how we've adjusted our compliance process since essentially GDPR which was May of 2018 when the temporary specification went into effect. Namely, the things that we need to do now are to obtain additional information and background from our reporters in order to verify complaints, this usually confirming they're the registrant if that's the case, getting additional stuff that might have been otherwise displayed in the WHOIS prior to May of 2018.

Additionally, we have to request more information from the contracted parties to verify compliance since that's, again, unavailable. And finally, a large part of what we do still is to continue educating reporters about the changes that have occurred since the temporary specification went into effect. Currently, there's still a lot of confusion about what should be displayed in the RDDS and explaining how registrars and registry operators can modify the existing requirements pursuant to that.

Additionally, we have updated complaint forms to tailor to the new requirements and the changes that have occurred. These can be found on our complaint homepage. There's a link here. I know, can't click on

it on the webinar, but they'll be available on the slides. And we published on that homepage additional instructions as well that can be clicked on as a link to get information about how to submit a complaint concerning access to a nonpublic registration data. So that is available. Next slide, please.

So here is the metrics that we have. We've now been able to obtain a year of metrics since moving to our new ticketing platform called NSp, so from September 2020 to August 2021, we have a slide showing a majority of the metrics that we publish.

A little bit of background. Under the temporary specification, we broke it down into different complaint types. There's kind of four different buckets that we have complaints under, the first being complaints concerning access requests made to contracted parties regarding nonpublic registration data. So reveal requests essentially under Section 4.1 of Appendix A.

The other one is how the registration data is displayed in the RDDS services. So most of these are usually concerning if a registrar for example is not displaying an e-mail or an anonymized e-mail or a webform to enable contact with the registrant, that sort of thing. The other bucket is consent to display the registration data where a registrant actually wants to display the information and they've made a request and it's not being done, that sort of thing. So that falls under Section 7.2 of the temporary specification.

And then the other bucket is just the obligations that are left over that might not be common such as Appendix [inaudible] UDRP obligation to

submit registration data under there, and BRDA changes, that sort of thing.

So here we have the three main ones. We've received 142 complaints indicating an issue concerning access to nonpublic registration data. 104 of those were closed as out of scope. So some examples of out of scope in regards to these types of complaints would be if they are privacy proxy registrations—or mainly proxy registrations where the registration data is actually fully displayed and the requestor is [thinking] the proxy customer information. That does not fall within the scope, so that would be out of scope.

Registration data, that is actually already displayed in the RDDS services. Also would be out of scope. And then the main one for these is when we just don't get a response of information or evidence that we've requested to verify the complaint.

39 new inquiries in this time period were sent to contracted parties or registrars relating to access requests. 32 of those have been closed. This included seven from our legacy ticketing platform. Next, we received 13 complaints concerning display of registration data. These are mainly, again, failure to display like an e-mail form or a webform to contact. And then we sent 18 new inquiries related to this.

The reason that's higher is that's also inquiries that may have been initiated by Compliance based on observations that the RDDS does not meet those requirements. And then 17 have been closed, seven of which were from the legacy platform. And finally, 41 complaints concerning consent to display registration data. 39 of those were

actually closed as out of scope only resulting in two new inquiries concerning section 7.2.

All of this information It is available on our monthly dashboard, there's again a link in the slide once that's available. This shows these metrics on a monthly basis concerning compliance activity related to enforcement of the temporary specification requirements. There's also specific closure detail in the metrics which you can refer to, such as demonstrating compliance or a registrar correcting compliance. So some examples of correcting compliance would be in implementing changes to ensure there's a process to provide reasonable access to nonpublic registration data, also implementing changes to RDDS, display of RDDS. And then examples of correcting or demonstrating compliance would be showing they'd already provided a response and reviewed requests for access. That sort of thing.

So just to clarify, some of the inquiries here are based on complaints that might have been received in a prior period such as in the old system. It also doesn't include cases that might have been received in August, for example, and not processed yet in September, so just to clarify any discrepancies in some of the numbers if you have any questions there.

And with that, I think we can hand it off to Yan for an audit update.

YAN AGRANONIK: Hello, my name is Yan Agranonik and I'm a manager who's responsible for compliance audits at the Compliance department. Next slide, please. Basically, I just want to say a few words about the most recent audit project that we had, which was targeted specifically at the section

3.18 of 2013 RA, which basically lists requirements related to registrars' obligations to handle various aspects of abuse reporting and handling.

By the way, if you saw most recent audit report published, there will be nothing new for you in those slides. The the obligations that were looked at were publishing e-mail address that is functional, that is designed to receive reports of abuse, maintain e-mail and a phone number specifically designed for law enforcement or similar authorities, publish procedures for receipt, handling and tracking of abuse reports and maintain records related to receipt and response to the abuse reports received from reporters.

We also verified that—it's not the in 3.18 but we also verified that phone number and abuse reporting e-mail listed in WHOIS output for domains managed by registrars are also first of all found in WHOIS output and then also their they're functional. Next slide please.

So how did we select resource for audit? The audit population included 126 registrars. They were picked if we found five or more domains listed in security threat reports we received in the previous audit of registries or five or more domains listed by RBLs, which is reputation blocklists which, in case if you don't know, these are publicly [related] sources of information that list domains that were reported by reporters.

In total, all the auditees managed 90% of registered generic second level domain names. So it looks like a good coverage. Now, how did we proceed? We compiled the request for information that we sent to all the registrars, and RFI or request for information contains several

questions and several requests for certain data. Proforma RFI, meaning blank RFI is published on our website.

Prior to audit, we also showed this request for information to Registrar Stakeholder Group making sure there is nothing unreasonable there. And we had a discussion about that. Next slide, please.

So these are audit results. Again, all these results in greater details are published in the audit report that is published on our website. But in brief, out of 126, we found that 111 registrars had some findings that they should have addressed, [and they did.] And we call them initial findings. The way it works is, in case you're not familiar with the audit process here, is after the initial audit, we send initial audit reports with initial findings, asking registrars to take a look at those items and let us know whether they agree that these findings should be corrected or some of the findings maybe we overlooked something and we just need some clarification.

So the breakdown of those 111 registers is below. So 97 had what we should call I guess real findings or real issues and the they've been working actively on correcting those. Out of 97, 78 completed addressing or remediating all the issues before the end of the audit, and 19 had to take a little bit more time because those findings were more time consuming. Next slide, please.

This is a little math here that again shows what I've been talking about. 126 registers in total. No findings whatsoever, meaning they immediately received clean audit report, 15. So 111 initial audit reports had initial findings. 14 out of these 111 showed to us that either we

didn't understand their response, or they gave us additional information that showed to us that these findings were not real deficiencies. So 97 had real deficiencies and 78 out of 97 address them before the end of the audit and 19 gave us the estimated dates when this remediation will be finished. And we will reaudit them later just for those items completed. Next slide please.

It is important to understand that the deficiencies themselves are different in I guess importance or because some of them are higher risk area, some of them are lower risk. For example, if you see there, what we think high priority deficiencies were the address listed on a website to submit complaints didn't work or not even there. We tested all these addresses. Another thing is the WHOIS information, When we pull out the phone number and e-mail out of WHOIS that's supposed to be active and that used by public to report complaints, they may not even be in the WHOIS output or they may not be operational. So that would be another issue that is riskier than other. So that is in response, by the way, to some of the blogs that we saw as a reaction to audit. Next slide please.

So in general, the audit demonstrates, we believe, that registrars take seriously their obligations and if we find something that is considered to be noncompliance, it is corrected. And again, referring to certain blogs, none of the registrars failed the audit. Failure would mean that there is an irreparable finding or deficiency that cannot be corrected timely or it just goes against the registrar's business model, which would result in notice, of which we didn't issue any during this audit round. Next slide please.

A little comment on reputation blocklists because we had quite a few questions of why are we using blocklists at all as a source of information. We do understand that registrars don't have any obligation to react to reports coming out of blocklists, if they receive any. And as you can see, there is a pretty high percentage of registrars not receiving any information about domains listed by blocklists.

But generally speaking, because there's a lot of interest in this area—I mean abuse— we use those reputation blocklists just to see, just to evaluate what's the situation there. Are any registrars even getting any information out of those blocklists or somehow indirectly receive reports from other sources? And as you can see, majority of registrars did not get that information out of the blocklists this way or another. That's it. So the audit portion is covered. All the questions, I'm waiting for at the end of the presentation.

JONATHAN DENISON: Hey, everyone, this is me, JD from Contractual Compliance, and I'll be going over kind of the classic stats that we've seen over the course of the year. Mehdi, can you go to the next one?

So basically, the timeline we're using is September 2020 to August 2021. During that time, Compliance received just over 20,000 new complaints. A little over 18,000 were registrar related and just under 2000 are registry operator related complaint types.

Of those 20,000 or so complaints, almost 17,000 of those were closed without even having to go to the registrar or registry operator. That

basically means that we're doing a whole lot of a lot of education. Generally, these are complaints that are out of scope with the policy requirements and contractual requirements.

So generally, what we have to do is provide some information to the complainant and help them understand the scope that we're limited to, and if possible, offer some other avenues for them to pursue. Other types of issues, we see if the complainant—we require more information from them in order to process. Sometimes we don't get a response to that, and those don't proceed without that evidence. Other things like ccTLDs, general misunderstandings about our role and authority, duplicate complaints, basically, those are just duplicates of existing tickets or cases that are already being handled or even previously closed. And again there's another link there to our metrics and dashboards. And then we'll go to the next slide to kind of see, of those that were sent to the contracted parties, for what types of—the high-volume issues.

So based on those numbers, just over 4000 were sent to the contracted parties over the course of the year. You can see a little breakdown there at the top about which were first notifications, second notifications or third notifications. And just to be clear, notifications we're using kind of generally. It could be either an inquiry or a notice. Inquiries generally more of an information gathering stage. So it's a little less formal than a notice where there's typically already evidence of potential noncompliance.

And this chart here kind of goes over the top three complaint types and volume and on the left side of the chart are the types of issues that were related to registrar obligations. On the right side, it's the registry obligations. And then each category, they're related to first, second or third notifications, describes the general complaint type that we've kind of allocated those into.

So for instance, if you look at the top left of the chart, the highest volume of first notifications for registrars that went out related to transfer issues, inter-registrar transfer issues or inter-registrant transfers. And you can kind of infer some conclusions, I think, from these charts, because if you look at like on the left side, you can see that the inter-registrar transfer issue received a high volume of first notifications, also a high volume of second notifications, and continued into third notifications. Whereas something like the domain renewal redemption doesn't show up as the highest volume under first notifications. Presumably, you could assume that aybe there's not as high of volume initially going out, but the issues aren't getting resolved until later on down the road. So there's that kind of thing there.

And then on the registry side, high volume of service level agreement alerts, zone file access requests, and monthly reports there. And then you could see as it goes down at the notification side, basically, the [monthly] transactions drops off from first notifications, but issues like escrow and payment continue through to the third, third stage. So kind of interesting to look at there. And there at the bottom, you can see 2000 closures for registrars and 616 to registry operators. And then we'll

go next. I'm actually going to pass this on to Amanda to go over the abuse complaints. Thanks.

AMANDA ROSE: Thanks, JD. So this is just an update on some metrics concerning abuse complaints under the registrar accreditation agreement, section 3.18. For those interested, again, this is metrics gathered from the new platform from September 2020 to August 2021. We had received 3328 complaints. And 559 of those have been closed once the domain was suspended or had already been suspended. And 314 were validated, meaning that we obtained sufficient information or evidence from the reporter to proceed with an inquiry or notice to the contracted party.

Once those had been verified, that did result in a first notice or inquiry. Majority of the registrars had demonstrated in response that steps had been taken to respond or investigate to the abuse report and respond appropriately to the complainant or the reporter in that case in accordance with their own abuse or domain name use policies.

Some examples—and this is a limited set, but some examples of what their response may include would be either to suspend the domain name, also providing information to the complainant to report abuse to the entity that's actually hosting the content. Another could be terminating the registrar's agreement with the registrar and allowing the transfer to a different registrar.

Under our abuse complaints we he had not issued a formal notice of breach. We have included a table here on the slides which have detailed metrics by the reporting month about complaints received and closed

as well as the number of inquiries and notices sent. If you could go to the next slide.

You'll see that a large majority of the complaints were closed, 3086 as out of scope without initiating an investigation with the registrar. Again, out of scope examples here include those involving ccTLDs, requests that ICANN take specific actions concerning the domain name, such as suspending it or removing webpage content, which is outside our contractual remit. Of course, a lot of duplicate complaints filed that concern ongoing investigations as well as those in which again, we failed to receive proper authentication or evidence or information to validate.

When closing these complaints, we also provide educational material to the reporters about our authority and our scope, as well as providing alternatives or information on more appropriate entities to contact for assistance. I'll go ahead and hand it right back to JD.

JONATHAN DENISON: Oh, thank you. Yeah, this is just like going into an ask that we have for anyone who submits complaints. Obviously, as you can see from the numbers, we're closing a huge majority of our cases without even going to the contracted parties. So some of these things are just misunderstanding, some of these things are just not necessarily providing everything that's needed to us. So it's just a general ask for anyone who's going to submit a complaint to carefully review the information in the complaint form and ensure the complaint is within the scope of ICANN's agreements with registries and registrars.

Obviously, for a lot of general public, that's not always super clear. So it's understandable that there's ongoing education needed, but it's worth a shot. But otherwise, provide all the information required by the form in order to enable ICANN Compliance to address the complaint. That's generally, if it's like registrant related issues, copies of correspondence that that you've had with the contracted parties, and any kind of relevant documentation that's relevant to the complaint.

And that kind of goes into the third bullet there a little bit as well. So if we talk about things like abuse complaints, we want to see that the abuse complaint had already been submitted to the registrar before we could even start handling that type of issue. So some of those are really important. So just throwing that out there.

Okay. And then, as you can see, I'll go into contractual compliance outreach. We got a request last time I recall to kind of share some of the outreach that we do. We have a page on the ICANN site that's dedicated to just general outreach that we do as well as we post our webinar materials like this as well. But we'll just kind of go over some on the next slide.

And actually, all these ones I want to talk about right now, these outreach sessions were performed by our Istanbul office. So in Ukraine, May 2021, there was a session with Ukrainian registrars in partnership with GSE, Global Stakeholder Engagement. A lot of these are just kind of going over broad contractual obligations, answering any questions. And you can see here the interim registration data policy, everything that that kind of entails all the way into the UDRP requirements. Those

were covered. Of course, abuse report requirements, audit activities, and our compliance approach and process in general.

And then, in the same month, in Turkey, there was a session in collaboration with—it says organized by by—the Istanbul Bilgi University, a lot of the same topics. Obviously, personal data protection authority, and local law regarding data protection was a topic of high interest, so kind of connected local law requirements with the interim registration data policy and how those might kind of work together or intersect, I should say probably. Next slide, please.

In Africa may 2021, it was a busy month for them, I guess, in Istanbul. Istanbul compliance team attended Africa Engagement Forum and kind of gave a general update about the compliance function. So that one was also a bit of a broader type of outreach. And it says here opportunity for ICANN to have a dedicated platform to gather, follow up and coordinate work being done with regional communities.

And then finally, last month, Compliance Istanbul team met with Turkish registrars to kind of go over the audit and DNS abuse obligations. That was also in collaboration with GSE and actually delivered in Turkish language. Yeah, I think I think that's about it. They just kind of kind of went over the results and the obligations in general, I think. And that's it for that.

Well, obviously, we're at the Q&A page. Again, I posted in the chat that we'll be putting this presentation in our outreach page and the prep week pages as well. But I guess now we can move into Q&A. I don't know. Jamie, do you have anything else?

JAMIE HEDLUND: I don't. I think you were in the middle of answering Susan Payne's question.

JONATHAN DENISON: Yeah. I can just address it verbally, I guess. I don't have like a breakdown of which of those 229 third notifications were which registrar. I don't have that in front of me. But in general, typically, just the way our process goes is obviously, if you get to third notice and they're not resolved by third notice, there's potential to go to our enforcement side, which is breach, suspension or termination. I suspect the vast majority of these were related to the very public ongoing issue we had with the registrar over the past year or so. But just because it says there's 229 third notifications doesn't mean that some of those didn't resolve at all.

But regarding repeat failings, we do address those with the registrars in the past if we see issues that seem to be recurring, typically when we're processing compliance issues if there is kind of evidence of noncompliance and we get on the same page, then typically there's a remediation aspect to it. And if there is kind of like a registrar or contracted party in general that appears to have previously remediated but the issue keeps popping up again, we have it within our process to—we could potentially go immediately to like an escalated notice, which is more or less the one notice needed prior to the enforcement side.

So there's different ways that we can address those types of things. Hopefully that helps, but feel free to add on if you need some more.

JAMIE HEDLUND: Jonathan, isn't it also possible that a lot of those were related to a recent termination, ame in before that termination took place?

JONATHAN DENISON: Yeah, that's more or less what I was thinking.

JAMIE HEDLUND: All right, so thank you all for listening and for the questions that we've received so far. Are there any other questions or subjects that people would like to discuss here?

JONATHAN DENISON: There was a question asked earlier in the chat. I'll bump it up now so it can be read and I'll just read it out loud. It was from Laxmi Prasad Yadav, an ICANN 72 fellow, and it was, “What is the total number of registrars and registries? How do you select them for audits or they compulsory go under audit every year?” I think this might be for Yan.

YAN AGRANONIK: Okay. What we're trying to do is we try to—basically, the audit program goes for several years by now. The way we select auditees is we try to obtain the maximum coverage based on number of domains that are managed or registered by those organizations. Typically, before, we did

one registry audit a year and one registrar audit a year. The full population is broken down by several groups based on the highest number of domains registered by them.

However, last year, the audit I've been talking about is not the typical audit that is [directed with all] the obligations, but specifically was looking only at abuse related obligations. Now, we are going back to probably more traditional audits because the results of this DNS abuse related audit now has to be—they have to be discussed and understood, and we have to realize what we're going to do next. So I hope I answered the question. So again, we tried to get the maximum coverage of the registrars and registries based on number of domains managed

MEHDI KURDMISTO: Thanks, Yan. there were no other questions listed in the chat and all the questions asked in the Q&A are answered. So I believe—Reg, that's something I think we're gonna have to look into. I don't know if that can be answered today.

JONATHAN DENISON: Yeah, about adding the domain name into the thing. Yeah, we'd have to look into that. There might be—it's a system thing. So you never know if there's limitations there. But I don't think we would be opposed to that at all if it's possible. But we can check it out.

MEHDI KURDMISTO: I'm just now noticing Jamie had responded to you but it only went to hosts and panelists and I just assumed that you saw that answer as well. Sorry about that. But yeah, so thank you, everyone, for your participation. Yeah, I think if there's nothing else, we can stop the recording. All right, thank you, everybody.

JAMIE HEDLUND: Yeah, we're always open so if anyone has any questions or concerns, please do not hesitate to raise them with us. Either e-mail me or send them to compliance@icann.org and we will address them. Thanks a lot.

[END OF TRANSCRIPTION]