ICANN84 | Prep Week – Contractual Compliance Update
Tuesday, October 14, 2025 – 19:00 to 20:00 IST

MAY KIM

Hello and welcome to Contractual Compliance Program Update for ICANN 84 Prep Week. My name is Mae Kim and I am a Participation Manager for this session.

Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and ICANN Community Anti-Harassment Policy.

During this session, questions or comments will only be read aloud if submitted within the Q&A pod. Interpretation for this session will include English, Spanish, and French.

If you would like to speak during this session, please raise your hand in Zoom. When called upon, unmute your microphone to speak. Please state your name for the record, the language you will speak if speaking a language other than English, and speak at a reasonable pace.

In this session, we will be discussing key outcomes from enforcement of the DNS abuse mitigation requirements, results of enforcing RDAP requirements, and supporting policy working groups and other community initiatives.

Please check the chat box for instructions on how to submit questions and/or comments. I will be inserting any links from the presentation in the chat. With that, I will hand the floor over to Jamie Hedlund, Senior Vice President Contractual Compliance and U.S. Government Engagement.

JAMIE HEDLUND

Hi, and thank you for joining our webinar today. My name is Jamie Hedlund, and I am pleased to be speaking with you as head of ICANN Contractual Compliance.

So what does compliance do? At a basic level, we enforce our agreements with gTLD registry operators and registrars. In the larger context of ICANN's multi-stakeholder model, though, we find ourselves at the end of the community-led policy development process. We ensure that the policies developed by the community, adopted by the Board, and implemented by ORG are carried out by the contracted parties.

These community-developed policies, along with other obligations, are incorporated into ICANN ORG's agreements with registries and registrars. We are the last step in the bottom-up policy development model. The credibility of that model depends in no small part on our efforts to enforce the obligations contained in these agreements.

To hear more about our enforcement role, I will now hand it over to Leticia Castillo, who will talk about our efforts to enforce DNS abuse mitigation requirements. Leticia?

LETICIA CASTILLO

Thanks, Jamie. Hi, everyone. My name is Leticia. I lead the team that enforces the DNS abuse mitigation requirements that became effective on April 5th, 2024, and we started enforcing these requirements the day they became effective without delay. Our enforcement is driven by investigations based on external complaints and other information available to us, along with regular audits.

From April 5th, 2024 through August 5th, 2025, that's a 16-month period, ICANN Compliance launched 400 enforcement actions, 400 specifically related to DNS abuse mitigation requirements. At that time, we issued four formal notices of breach of the agreements under those requirements, and we launched one registrar and one registry audit that tested DNS abuse mitigation requirements, among others. The registry audit is wrapping up. We are producing a final report that will be published. It has lasted longer than prior audits, and this reflects our commitment to fairness and ensuring the new requirements were tested and fully met. And the registrar audit was launched a couple months ago and targets registrars with the highest concentration of reported DNS abuse over a period of 13 months.

As a direct result of our investigations, nearly 20,000 malicious domain names were mitigated during this 16 months that we're talking about. And most importantly, hundreds of thousands more were addressed through the processes and improvements that registrars and registries implemented following our enforcement actions. So this means that our actions go beyond the reported domain names in individual cases. We seek to remediate the underlying patterns that cause the noncompliance and ensure continued compliance, and I will talk more about that in a few minutes. Next slide, please.

Enforcement happens in two ways, through the formal and through formal processes. Both are equally thorough, but they differ in visibility and escalation. And let's break this down. Informal enforcement notices, those 400 that you see in the chart, are not public. We contact the contracted party, we require clear evidence of compliance or remediation. There is a structured process with timelines for resolution, and while you will not see the informal notices on our website, they are being sent out every day. And also the 400 you see in the chart is specifically related to DNS abuse requirements.

And formal enforcement notices come into play if the issue is not resolved informally. And this stage is public, a notice of breach is published on the website, and it can ultimately escalate to suspension or termination of the agreements. And here, too, we require evidence and remediation following a clear timeline. And

this is what this chart shows when it comes to DNS abuse mitigation requirements. Over the 16-month period that we were talking about, we initiated 400 enforcement actions at the informal stage, and aggregated numbers for those are on our monthly reports, but you don't see the notices themselves on the website. And during the same period, there were four formal notices of breach public and posted on our website. So it is important to highlight that resolving noncompliance before it goes to a public notice of breach is actually quite common. Please go to the next slide.

For context, across all ICANN policies and agreements and the same timeframe that we're talking about, so all requirements, abuse, transfer, renewals, RDAP, there were 2,970 enforcement actions launched in the informal process, and 19 formal public notices of breach. So the key takeaway here is that whether enforcement is informal or formal, we are taking rigorous action every day. We hold contracted parties accountable and work with them to resolve issues. Public notices of breach are just the tip of the iceberg. Most enforcement happens at the informal stage, and it is full enforcement and impactful and reported in our monthly reports via aggregated data. Next slide, please.

Now let's talk about remediation plans are targeted actions that are designed to address the root causes of noncompliance to prevent them from happening again in the future. Remediation plans can be applied at both the informal and the formal stages of our process, and the scope and detail of each plan will depend on the specific issue to be addressed. For example, if the issue is that

the abuse contact is not working, the remediation requires the registrar or registry to fix that. If it is discovered that the registrar did not properly address the report that we are reviewing because it doesn't have processes in place to receive and address DNS abuse reports as required by the agreement, then the remediation plan goes deeper to address all related issues.

And we have had remediation plans that covered everything from abuse contact to information that must be posted online to processes to address DNS abuse reports, etc. And the plans that are presented to us include timelines, progress check-ins, and once they are completed, they are tracked in our system so that if the issue happens again, we can take expedited compliance action. So with that in mind, between April 2024 through August 2025, 31 remediation plans were implemented, specifically related to DNS abuse. And I will give a concrete example, next slide.

Here, so let's take a look at a case that went to public notice of breach. It was the first notice of breach issue for the then new requirements. In this case, it was determined that the registry did not have systems and processes needed to comply with the DNS abuse mitigation requirements. And because remediation was not provided during the informal stage, this case escalated to a public notice of breach. To cure the breach, the registry took several actions. You see at a high level, a few of them there, establishing a dedicated system and staff to promptly handle abuse reports with regular internal audits to improve their processes. And by July

2025, they reported acting on nearly 150,000 abusive domain names that were reported by third parties through these channels.

They also introduced proactive monitoring system to detect DNS abuse, which allowed them to mitigate over 300,000 malicious domain names also by July 2025. So they took more action. We published a blog in June with more details about this remediation. It is linked here in the slide if you want to take a look later. And I want to stress that compliance continues to monitor these actions to ensure ongoing compliance with regard to this remediation plan and all the others that we have logged in their system following our cases. And we are not claiming that all abuse was removed from this TLD or that any TLD is perfect. What we're saying is that specific actions were taken with specific results through compliance enforcement. And those actions went well beyond addressing the 92 domains that initially triggered that case.

So next slide is here. Transparency is critical for us. This is why we regularly report on our enforcement actions. We publish monthly reports with updates on DNS abuse mitigation requirements enforcement. Our first six month report was released last year in April. This year we held a webinar sharing key highlights from the first year enforcement of the new requirements. And then we continue to provide updates at ICANN meetings and different events like today's webinar.

We welcome your feedback. I would like to end my section with a call to action. If you have any suggestions or input, something you

would like us to publish or display differently, please email us to compliance at ICANN.org. Use the subject line on the slide. We want to serve the community, not just by enforcing the requirements, but by being transparent and reporting on our actions. So your feedback can help us and if we can implement it, we will. Thank you. And I'm willing to hand it over to actually Jonathan Dennison. Amanda had some last minute issues, so she's not going to be able to join us. Jonathan.

JONATHAN DENISON thank you. so I'll be stepping in to speak on the registration data access protocol.

Just a couple things. This means I'm not technically the subject matter expert in this area, but what that means generally is like if you have any specific questions or detailed questions related to this. submit them, then potentially we're just going to have to take them back and come back to you with an answer, but don't be shy. Either way, feel free to submit. We don't want to leave you hanging.

RDAP. This is a directory service that's to be provided by all registrars and registry operators. Its intention was to replace the WHOIS protocol and all these protocols sit under the RDDS is the registration data directory services. Essentially, it's related to the domain name registration data, or you can call it contact information if you want. But essentially, this slide goes over the current state of requirements related to RDAP.

So here you can see the February 2024 RDAP profile is the current version that's to be implemented. It also includes service level requirements related to the RDAP service, meaning stuff like how much downtime is either permitted or not permitted related to these services. There is no requirement to provide an RDAP web client because we have services like lookup.ican.org, which anybody can use to query the registration data for particular domain names. There, as I said, the current profile is February 2024. Essentially, it's reflects changes that align with the registration data policy, and that's the policy that sits on top of the agreements that we have with contracted parties that talks about that registration data that needs to be collected or may be collected. And if you do collect certain information, what you have to do with that information, display requirements and so forth, and then other things like requirements around disclosure requests where anybody can submit a request for the underlying data that's being redacted in the output. Let's see. Yep, I think we can go to the next one.

And this slide here essentially goes through some of the overall activity that compliance has been involved in when enforcing the requirements related to RDAP. Back in October 2019, obviously this goes back a ways. It's been a long journey when it comes to RDAP because there have been multiple policy changes throughout the years that have amended the requirements. So it's been a lot of changes that everyone's had to keep up on. And hopefully at this point, though, things will start to settle and get to more uniform

place. But back in October 2019, we just started off with enforcing the actual implementation of the protocol and essentially producing the URLs related to the service. RDAP registration data access protocol. Sorry, I was just responding to the chat there. so back then, 387 compliance notifications were sent to registrars without an RDAP URL. As of today, only four registrars are lacking a URL. I think it might actually be three now. But at that time, the cases were limited in scope since the profile requirements were not around at the time.

So then we get to August 2023. That's when the RDAP amendments became effective. And this established the data that must be provided in the response when you query registration data. And it also provided for the formatting of the responses. Basically when you query how to, it's not only how the service is implemented, but also how the information is mapped out when you conduct those queries. So there's some uniformity to what you're seeing in response to the queries. Let's see. Then, of course, updates to technical and the RFC requirements. Some of those examples there are the higher level requirements where the service has to be available over IPv6, use of HTTPS, and so forth. The next one.

So, during the journey here in August 2023, compliance started enforcing the RDAP profile. There's two components to that, the response profile and the technical implementation guide, and I already explained, but the technical implementation guide is more about how to implement the service and then the response is like

that mapping of the information. At this time, compliance initiated around 75 registrar compliance notifications. And the trick here is that the resolution of each case can take over six months, depending on the complexity. And as of September of this year, 31 are ongoing remediation efforts. It's a very complicated, very technical area, and it requires a lot of expertise and going to different tools that are available to assess compliance. And it's just, it's the nature of how it works, but it does take a long time, but our goal, of course, is to work with the contracted parties to come into compliance because we just want a service that works.

And of course having said that, of course, if failure to engage in the remediation efforts, of course, through the informal compliance process that Leticia described earlier, then those could result in notice of breach on the formal enforcement side. In July 2025, incorporated requests for information and RDAP testing into the current Registrar Audit Program. Basically, through the Registrar Audit, including questions related to RDAP implementation were built in, so that's ongoing as of now. As a result of the enforcement that has taken place over the past few years, compliance has issued 17 formal notices of breach that included RDAP-related violations. Two of those notices of breach escalated termination. I think it might actually be higher. RDAP might not have been a primary reason in the notice of breach, but I do believe a handful of them at least referenced RDAP in them. So let me go to the next one.

This slide essentially talks about the RDAP conformance tool. This

is a tool that you can access online to check your own conformity to the RDAP requirements as a provider. And this is an example of what an output might look. And it's a tool that compliance uses when assessing compliance, of course. And just to illustrate there, some of the cases we see can have 300 plus errors in a single test of URL. So it goes back to what I was saying earlier where it's a long process. If you're having 300-something errors, then it takes a long time to work through all of those, but that's okay. And we'll go to the next slide.

So this expands on how we approach RDAP enforcement. Beyond the tool, there's a complete review of the RDAP requirements, which typically includes manual checks for all required registration data in accordance with the registration data policy. These two things are intertwined at this point, so we try to take a holistic view on things and not just address piece by piece. There's RDAP test command. It's a command line interface testing utility, and it's available at that GitHub link there. And then there's a comparison of RDAP conformance tool results with the applicable requirements, again, taking a holistic view at the conformance to the requirements. Functionality testing for use with RDAP web clients. Service level requirements testing, again, going back to the operability of the service. And then consistency testing. So as you can see, there are a lot of parts there that compliance needs to consult with in order to get a general understanding of whether the protocol is compliant or not. So it's a very timely process. Time consuming process, I should say. And then there's the little heads

up there, the RDAP conformance tool. Users manual is a resource to complement the RDAP conformance tool and aid in RDAP implementation, and all these are available online for people to consult with. Next.

So this is the negative, is you have to hear me twice, so I'm going to just roll into some of the other activities that compliance is involved in beyond strictly enforcement requirements. As you, so many of you probably know, we are regulars in ongoing policy development and research work. This is an update since our last presentation prior to ICANN 82, so these are some of the groups that we've been involved in since then. And for policy review PDP, the Rights Protection Mechanisms Implementation Review Team. That is a mouthful. New gTLD program, next round, specifically involved in development of the next round registration, registry agreement. Been involved in registration data policy implementation, proxy services, accreditation, and so forth. I think you can see there. We'll go next.

What do we do when we're involved in these groups could be various things. Sometimes we get requests for metrics and data to help inform discussions around certain policy development. A lot of these things can be pulled from our metrics and dashboards page that's on our compliance page on the ICANN.org. But of course, we can also do ad hoc requests as well, if needed, or at least we can look into our ability to do so. Generally, the main thing is providing input on whether proposed policy language and contract provisions are clear and enforceable. As Jamie alluded to in the

beginning, we inherit the end result of all of these working groups and policy development. So our main thing is we need to be able to understand and clearly enforce whatever comes our way. So we obviously want to provide our input and our insight into feasibility and clarity regarding any language that's developed.

Let's see. Other examples are feedback on like I said, feedback on draft provisions related to the next round registry agreement. Other examples can include developing ideas on how to implement recommendations related to the rights protection mechanisms. In a practical and meaningful manner the ability to report noncompliance during URS proceedings. Also, things like developing ideas on implementation of provisions related to disclosure requests or EPDP phase one. So stuff like that. I think I'm going next.

So this is some of the outreach that we've done. Occasionally we get requests for joining other departments in ICANN that are they're hosting outreach sessions and. Sometimes we present information related to our compliance efforts, or maybe it's how we approach certain enforcement of provisions. And here are some examples that we've been involved with since ICANN 82. The first anniversary of the DNS abuse mitigation requirements. In April of this year, compliance conducted a webinar providing key highlights analysis of enforcement metrics for that first year. Next steps and more. We were at the contracted party summit in Vietnam earlier this year. We engaged in multiple one-on-one sessions. We do that a lot at the ICANN meetings. And we're always happy to meet with any contract

parties or whoever. We attended the APAC DNS forum from May of this year as well. We participated in the policy forum ICANN 83 in Czech Republic. And again, we were there and conducted various one-on-one sessions. As you can see, some examples of topics related to DNS abuse in RDAP. And yeah, I think that's it May?

MAY KIM: Yep, that's it. Thank you, Jamie, Letitia and Jonathan. If anybody has any questions at this point, please feel free to put them in the Q&A pod. There are no questions currently to address.

And no hands raised. So looks like everyone has been thoroughly informed. Thank you very much for joining us today. And if anybody, Jamie, Letitia and Jonathan, if you'd like to add anything.

JAMIE HEDLUND: No, thank you all for joining. And please do follow up if you have any questions. A number of us will be in Dublin, but we are available 24-7. Thanks.

MAY KIM: Thank you all. And as you can see on this last page, it's the ICANN webpage and social media link for connecting and keeping informed on all things ICANN. Thank you!

JAMIE HEDLUND: Thank you all. Have a great day.

LETICIA CASTILLO	Thanks everyone.
TINUADE OGUNTUYI	Thank you so much.
LETICIA CASTILLO	Bye.

[END OF TRANSCRIPTION]