ICANN85 | Prep Week – Contractual Compliance Update
Tuesday, February 24, 2026 – 01:00 to 02:00 AM IST

MAE KIM

Hello and welcome to Contractual Compliance Program Update for ICANN85 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, Key Findings from the 2024 To 2025 Registry Audit, Enforcement of Registration Data Policy Disclosure and Registration Data Access Protocol, RDAP Requirements, And Supporting Policy Working Groups and Community Initiatives. Please check the chat box for instructions on how to submit questions and or comments.

All questions will be addressed at the end of the session. 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, Global Government Engagement and Contractual Compliance.

JAMIE HEDLUND

Thanks, Mae, and thank you all for joining our webinar today. The main role of Contractual Compliance is to ensure that ICANN's registries and registrars have implemented the policies developed by the ICANN community. We do this by enforcing our agreements with ICANN's registries and registrars that contains these policies and other obligations.

We address external complaints. We conduct proactive monitoring and enforcement activities, and we conduct audits of registries and registrars to ensure that they are complying with our agreements. We publish monthly reports on our enforcement activities. One of the most important things that we do is to contribute and provide input into community policy development and negotiations to amend our agreements with registries and registrars to ensure that any new contractual obligations are clear and enforceable.

We also actively contribute to outreach activities and training sessions to raise community awareness about our contractual obligations. With that, I will now hand over to Leticia, who will begin to show how active we've been since the last time we did one of these webinars. Thank you.

LETICIA CASTILLO

Thanks, Jamie. Hi, everyone. My name is Leticia Castillo, and I lead the team at ICANN responsible for enforcing the abuse requirements in ICANN's agreements. We began enforcing the DNS Abuse mitigation requirements the day they became effective on April 5, 2024.

Our enforcement work is driven by investigations that are mainly started with external complaints as well as our regular audits. And from April 5, 2024 through December 5, 2025, we launched 463 enforcement investigations specifically related to the DNS Abuse mitigation requirements.

During that same period, we issued four formal notices of breach under those requirements specifically. There was a fifth notice of breach in January that was related to other forms of abuse and specifically failure to investigate reports involving nearly 20,000 domains allegedly tied to investment and cryptocurrency fraud. But that was under a different section of the agreement, as I said.

We also completed a registry audit, and we are in the process of working a registrar audit that targets registrars with the highest concentration of reported DNS Abuse over a period of 13 months. But my colleague, Joe, is going to speak more about the audit right after me. Our work has a real impact. Through our DNS Abuse cases, more than 22,000 malicious domains were directly mitigated during this 20-month period that I am talking about.

However, the most significant impact of our work comes from addressing patterns. When we identify gaps in the registrar's or registry's processes or knowledge or systems, and those gaps cost the noncompliance, we require a remediation plan. And those plans aim to help prevent the same issues from happening again in the future with other domains, with other reports.

So, as a result, our enforcement has actually led to the mitigation of hundreds of thousands of abusive domain names. And it's very hard to quantify, impossible to quantify the full effect of prevention. But in our last webinar, I shared the specific example of a registry that implemented new systems and processes as part of its remediation, following our first notice of breach under these requirements and how those changes enabled them to detect and mitigate over 450,000 malicious domain names in the TLD within a few months. So, our actions go beyond the individual domains reported in any one case.

Next slide, please. This slide helps put our enforcement work into perspective. We enforce all requirements through two phases of our process, the informal and the formal. Both are thorough, but only the formal process, which start with a notice of breach is made public. Most issues, however, are fixed during the informal phase. So, they appear in our monthly aggregated reports and not in public notices of breach with details or names. Only a small number of cases move to the formal phases.

This is because most contracted parties resolve the noncompliance or demonstrate compliance earlier in the process. And to give you a sense of scale, over the 20 months that we're discussing, we launched 3,919 enforcement actions across all policies and agreements. Only 22 public notices of breach were issued. But the request for evidence, the detailed reviews, the back-and-forth remediation work, the monitoring all happens continuously in the informal stage as well.

The notices of breach are just the tip of the iceberg. Most of the enforcement work happens every day within the informal stage with a real impact and full accountability. And I mentioned remediation plans a couple times. So, what they are, they are targeted actions designed to address the root causes of noncompliance to prevent them from happening again in the future.

They can be applied at both the informal and the formal stages of our processes. And the scope and detail of each plan will depend on the specific issue that we are addressing. For example, if the issue is that the abuse contact is not working, the remediation plan requires that to be fixed. But if it is discovered that a registrar or registry did not properly address a report because it doesn't have processes in place or knowledge to receive and address those reports as required by the agreements, then the remediation plan goes deeper.

We have had plans that cover everything from the abuse contact to the processes to address the abuse reports, the processes to address other type of abuse reports, keeping records, et cetera. And the plans that are presented to us include timelines, include progress check-ins. And once they are completed, they are tracked in our compliance system to monitor recurrences.

So, with that in mind, between April 2024 through December 2025, 37 remediation plans were completed. I'm talking about just the work completed, not the ones that are ongoing. And those were related specifically to DNS Abuse mitigation requirements.

Next slide, please. And this slide highlights some ongoing challenges that include the continued increase in both the volume and the complexity of the complaints that we received. Abuse-related complaints have always been our highest volume, not always, but have been our highest volume type for years. And the trend continues upward from January 2025 through January 2026, we saw an increase of those of approximately 52%. And at the same time, most complaints that we receive are not actionable on our end, but they still require a full review and validation, which slows down our ability to handle the complaints that do fall within our scope quicker.

And for example, we saw a group submit hundreds of reports to various registrars and then submit the related complaint to us on the same day, almost at the same time. So, if the registrar hasn't been given any time to investigate, there's no basis to allege that

they failed to promptly investigate and act. Yet, we still had to review all the communications, check timelines, explain the scope to the complainants and follow up a couple of days later to confirm that actually the domain names were in fact mitigated. So, this is just an example of what we're talking about with all these non-actionable complaints, which is not always very straightforward.

And attackers using more and more evasion techniques adds layers to our reviews and complicates the exercise of determining whether contacted parties act reasonably considering all the details and all the information that was reasonably accessible to them. And we're talking Geo-blogging, but we're also many other techniques like rapid or conditional redirects to legitimate page, to blank page, to error pages or pages that only load under specific circumstances. It becomes harder to assess whether the registrar had difficulty verifying or reproducing the evidence, whether the abuse was short-lived or was there or not, or whether the registrar failed to act when it should have because they did have that evidence.

So, in response to these challenges, we're taking several steps. We continue to train and stay informed ourselves. Of course, we are also expanding our outreach efforts so stakeholders better understand what ICANN, can't and cannot do. How to submit actionable complaint to us. We recently published a step-by-step guide about that. We are offering some targeted feedback to frequent reporters and exploring ways to enhance our intake and triage processes so they are more efficient and better suited to the

current volume and complexity of the complaints that we're receiving. And I'm sure there's more things that we can do.

We continue exploring and exploring ways to continue improving, of course. Next slide, please. And this is my last slide. I am not going to go through all the details here. I just wanted to highlight that transparency is a big part of how we operate in compliance. We put out monthly updates on our DNS Abuse work and we recently added open data format downloads to all reports. It's linked there in the announcement. We have published blogs.

We have published guidelines and conducted webinars. We are committed to being open about what we're seeing and working together with the community to improve how DNS Abuse is addressed. And as always, we want your feedback. If you have any suggestions of something you would like us to publish or to present differently, please email us.

The new open data publication we recently launched is actually a direct result from community feedback. So, don't be shy. Your input can really help us improve. And where we can implement it, we will. This is the end of my updates. Happy to take questions at the end. And I'm going to hand it over to Joe Restuccia for an update on the audit.

JOSEPH RESTUCCIA Thanks, Leticia. Hi, everyone. I'm Joe Restuccia. I'm a member of the compliance audit team and I'm going to highlight key findings

from the most recent registry audit that we completed. Before I get into some of the details about the registry audit, I do want to cover just a couple of points about the audit process in general, just because some of you may be newer or unaware of how our process and how we conduct audits typically works.

So, generally, we do conduct two audits per year. They are one for registrars and one for registries. And because we do receive a lot of data, there's a high volume of data and documents that we have to go through. While we do, do a lot of the work in-house, we do utilize the services of KPMG to assist us with that data collection and evaluation.

Also, following the completion of each audit, we do publish a final report. And this final report, it's on our compliance page. There's actually an audit report section where you can view all of the final reports that we have published. They are separated by registrars and registries. And what they typically list is things such as the key findings as well as the list of the auditees.

So, with regards to the audit that we just completed, it did span from October 2024 to October 2025. It was a registry audit and there were 21 gTLDs in this audit. In addition to looking at the usual obligations that we typically look at as part of the registry agreement, a key thing to notice, this was the first audit that we did since the new DNS Abuse amendments went into effect in 2024. Because this was the first time that we were looking at them, questions that we had tested whether the registry operators

understood those requirements and if they had necessary processes in place to comply with them.

As I mentioned earlier, we do utilize the services of KPMG. And as you can tell, that's very helpful for us because in this audit alone, we did look at over 1,800 documents spanned across 14 countries and territories and it was in six different languages. On the next slide, you will be able to see we did publish a link to the final report for this audit. I do encourage anyone, if you haven't taken a look at it yet, to please do so.

While these reports I mentioned before do have key findings as well as the list of auditees, there's a lot more information in there that could be very helpful for you to see, such as the audit criteria, criteria around the audit scope. There's also some more information around the specific tests that we did, as well as even more details around the specific findings that we had and the remediations that took place as a part of that.

For the key findings for this audit, as I mentioned before, there were 21 gTLDs, 12 of those 21 received clean reports. What that means is that those 12 were able to resolve all, or they were able to remediate all findings prior to the close of the audit. Nine of those gTLDs of the 21 had at least one unresolved finding. What that means is that those nine had some issues that they were unable to remediate prior to the close of the audit.

You might be asking yourself, why is it that 12 were able to remediate all their issues, but there were some other auditees who

still had issues that went beyond the audit? A lot of times that can attribute to the nature of the issue that was found. Some of the issues found are sort of easier or can be more quickly fixed, such as if something is missing from a website, that is a lot easier to add to a website, versus sometimes we might find some issues with an underlying process that the auditee is doing.

Sometimes it's a little bit more time and steps involved to remediate that process over time. For the nine who did receive that had unresolved findings, they were required to submit to us a remediation plan.

Now, Leticia did talk about previously what remediation plans do include, but just as a reminder, for this audit, the remediation plans that they submitted to us included the specific steps that the auditee was going to take to ensure that the finding would be remediated, steps that it would to ensure that it wouldn't happen again and recur, and then also the dates on which they expected the remediation process to be completed.

Of those nine, seven have actually since the completion of the audit, they have completed their remediation, and there are two still left to finish the remediation, but we do expect both of those to complete their remediation shortly.

A key note from this audit is that no registry ended the audit with unresolved findings related to DNS Abuse mitigation, and what this means is that some of the DNS Abuse-related issues that we did find, such as those related to abuse contacts, those were all

remediated prior to the close of the audit, and the last item that I would like to highlight is that there was one registry who was undergoing their broader DNS Abuse remediation due to a notice of breach prior to the start of the audit.

When we looked at the processes that that auditee had remediated as part of the enforcement action, we actually did not find any deficiencies in those processes, and so I believe that that underscores and highlights the effectiveness of our enforcement processes and that the tools that we use for remediation and enforcement are all working effectively. That's all I have for the key findings, and with that, I am going to hand things over to Amanda Rose. Thank you.

AMANDA ROSE

Thanks, Joe. I am going to speak to everyone about the enforcement, starting with the enforcement of the registration data policy, specifically regarding disclosure requirements. Just a reminder for those that might not know, the registration data policy went into effect on the 21st of August of last year, so this is a relatively new policy. However, a lot of the obligations track what was previously required under the temporary specification for gTLD registration data.

Section 10 of the policy specifically deals with disclosure requirements or requirements regarding requests for disclosure of non-public registration data, so data which is not publicly available in registration data directory services. There are some key

requirements that I wanted to highlight, mainly the first being that contracted parties, both registrars and registry operators, have to publish a link on their home page that directs to a page or information that describes their mechanism and process for submitting disclosure requests.

That publication has to include the format of the request as well as what content needs to be included in the request, so third parties can understand what they need at the outset to submit to the contracted party in a request for disclosure. They also must include how they will respond or means for providing a response, as well as the anticipated timeline for responding. Next, they have to review each request that is properly formed on its MIPS, so reviewing the content of the request itself.

Additionally, there are specific response requirements under Section 10 now, and that is to provide either the requested registration data. If the requested request is denied, they must include an explanation that describes the specific reasons for the denial. That denial must include a clear explanation of how the contract party arrived at its decision, and that must be sufficient for any requester to subjectively, I'm sorry, objectively, that's an important distinction, understand the reasons for the decision.

In addition, if a balancing test is applied, that is balancing of the fundamental rights and freedoms of the data subject against the legitimate interest claimed by the requester, they must also include an analysis, an explanation of how this test was weighed,

and the outcome. Just a reminder that, not a reminder, but an explanation that this is an if it is applied. A balancing test will not be required in all circumstances.

That is usually specific to local requirements like, for example, most commonly GDPR, but also additional privacy laws that have globally gone into effect, but generally many contracted parties still apply this type of balancing test in their review and analysis of disclosure requests. I also, I don't know if May already added this. Yeah, never mind. There's a link in the chat, just specifically to section 10, which outlines these requirements in detail. So, we can go to the next slide. Okay, this is just an overview of the metrics we have. We started on September 1st here, that is because the policy again went into effect on the 21st of August.

Just cleaner to capture these last complete months as far as the data we have. As you can see here, there is a low volume of total complaints, especially when we look at the volume we received for abuse complaints. For instance, we have 62 total complaints received that relate to these obligations. So, request obligations related to requests for disclosure of non-public registration data. 37 of these were closed at the close of January as out of scope. Examples include when we don't get a response, should we request additional information or evidence?

Example would be, we don't have evidence that a request was submitted to a contracted party. We would follow up and ask for copies of that, for instance. If we don't receive a response, the case

will close. Another large example of that is, if the information or the registration shows as under proxy, that means that the registrant is in fact the proxy service, that under the registration data policy, the full data must be published in the public directory.

So, the registrant information is available. Accordingly, under the current policies, this disclosure request obligations would not apply. And then some of the minor ones are examples of ccTLD, for instance. I noted here also 16% of those closed of the 37 are due to the fact that they are under proxy. So, that is a common complaint we do receive, are complaints related to requests for disclosure of proxy customer data rather than registration data as defined in the registration data policy.

24 of the 62 complaints received did result in a compliance investigation. That's 39%. Five of these, as of the 31st of January, had been closed or resolved. 19 were pending investigations. So, a lot of those included remediation plans, as discussed in several of the previous slides. And as you can see, a large percent of those included remediation plans for, or I should explain, a large percent of those included remediation plans for publication requirements. So, the requirement to publish their process for how to submit requests. 21 of the 24 included questions or investigation of those publication requirements. So, we were unable to find on our own a link to the page that must describe that.

16 also included, or 16 of these included, an investigation regarding response criteria, as it must be. Some of them involved both. Some

of them only involved one or the other, but almost all did involve publication. So, you can see we do perform a review of those cases that we receive. So, even some that might be out of scope, we'll take a look at, or out of scope for the purpose of the request or response criteria. But they might be within scope because they haven't published their requirements, for instance. All right. And lastly, just one was pending review at that time. It's more than likely been processed since then, but that was with the data that we had as of the close of January.

So, next slide. I have just included some screenshots of the new report that we have going back a few months now. We have some specific targeted reports for like DNS Abuse, for instance, and disclosure here that provide a breakdown of things like I included on the last slide. So, complaint volume broken down by reporter type, volume of complaints closed. These also include the closure explanation. So, you can get a breakdown if you are interested on why each case was closed.

Volume of investigations opened, also those closed, including the closure explanation. In the bottom right corner, you can see we have a separate section of the report that includes a breakdown of the Privacy Proxy or redacted cases that we were able to identify while processing the case. So, if throughout our processing, we were able to determine if the case or if the registration was under privacy, whether it was under proxy or whether it was redacted

under the registration data policy, we will document that and include it in this report.

Lastly, I just wanted to touch that the 2025 registrar audit also includes compliance checks regarding these disclosure requirements. So, we test the processes of reviewing and responding to disclosure requests as well as the publication criteria that I previously went over.

With that, I will move on to the next topic that I also lead enforcement efforts on, and that is the RDAP or Registration Data Access Protocol, or RDDS, as a lot of people know it as. I jumped ahead. This is the replacement of the WHOIS that we all knew in the past of how to query registration data for any registered domain name.

As of August 21st, which does match the effective date of the registration data policy, there was a new RDAP profile that went into effect and must be implemented by all contracted parties. This profile is updated to align with new requirements for publishing registration data that aligns with the registration data policy.

Overall, general enforcement informal cases included 98 registrar compliance notifications to date or as of 31 August. I mean, January, sorry. 32 of those are part of ongoing remediation efforts. So, I just want to note that these specific RDAP cases are very technical, very detailed, and can be complex depending on what the issues are.

There's a lot that go into implementation of these requirements, both from a technical perspective as well as getting the right data required under the registration data policy into the RDAP response, and that is the profile or the response profile itself. A lot of times we have to consult with technical services. We will engage in outreach efforts with contracted parties, technical staff.

So, it does sometimes require complex remediations, remediation plans. Apologies. July 2025. So, this is the register audit. We did include RDAP review in the most recent registrar audit. So, each auditee has to go or we review all of the RDAP requirements and follow up if we detect any non-conformance issues with the profile. Of our formal enforcement of RDAP, we have included 18 formal notices of breach that included RDAP-related violations.

Eight of these have escalated to termination. So, that is part of our review of any formal enforcement effort that we do to determine whether they are up to date on their RDDS obligations. That is all I have. I will go ahead and pass it off to JD.

JONATHAN DENISON Thank you. We can go to the next slide there. I mean, this section is basically just to speak on some of the work we do outside of enforcement, which is obviously kind of our core work that we do. But we spend a significant amount of time in other areas like policy, development, working groups, and other initiatives. For those who are unfamiliar, we might be involved in outreach.

A lot of times, different departments within ICANN may host webinars or meetings, conferences where compliance might contribute by providing a compliance perspective. Sometimes these are general topics that we may provide insight on or might be more specific depending on the purpose of the meetings and the audience. And then outreach might also take place during the course of our regular work.

If we see patterns or patterns of behavior or issues that might pop up when we're working or investigating certain cases with contracted parties and we think it might be worth jumping on a call, we will often offer conference calls with contracted parties to kind of work through some of the contractual issues that we're seeing, answer any questions, share information, those kinds of things. As Jamie said at the top, we spend a significant amount of time in the policy development process.

Obviously for us, the main thing is we're going to be inheriting any policy that comes down the line. So, it's obviously good for us to have an idea of what to expect. A lot of times new policy impacts our systems, our processes, our approach. So, it's important that we follow along and we're able to kind of set up our team properly to make sure that enforcement can take place.

Additionally, we may help other groups that are working on or exploring certain policy issues. Sometimes, because we have a lot of direct experience with enforcement or policies, we can also provide a lot of insight and metrics into certain areas. So, any

information or request for information that come along our way we're able to provide to kind of help provide context and inform any questions they may be considering.

But these are just some of the examples of the groups that we are currently involved in. A lot of times, it's on the implementation side, but we do follow along throughout the entire process just so that we're well informed. And I think that's kind of the gist. This is just kind of describing more of what I spoke on. So, I think that's about it.

MAE KIM

All right. Thank you, JD. There was a question in the Q&A pod that has been answered. If anybody would like to speak, you can go ahead and raise your hand right now. Or if you have any questions and you would like to add it to the Q&A pod, this is your time for it to be addressed here in this session. Or if anyone else would like to add anything to our session today.

There is another question in the Q&A pod right now. And I will read it aloud. Going back to the RDP, section 9.2.3 states that where Registrar applies the requirements in section 9.2.1 for the following data elements, Registrar must publish an email address or a link to a web form to facilitate email communication with the relevant contact for the email value, which must not identify the contact email address or the contact itself.

What is the view of ICANN compliance regarding what is required in a web form used to comply with section 9.2.3? For example, is it sufficient to have a three pre canned message that can be sent to the registrant? And for that question, we will go ahead and send it over to Jamie.

JAMIE HEDLUND: Sure. Thanks, Mark. That's a pressing question. It's actually one that goes to an ongoing or goes to a pending complaint that we are currently reviewing and evaluating the very question you raise. Unfortunately, we don't have an answer that we can share right now. But it is something very much that we are looking at.

MAE KIM: All right. Thanks, Jamie. And if anyone else has anything to add to the Q&A pod or would like to speak, you can raise your hand in the session and we can go ahead and go over to you.

JAMIE HEDLUND: All right. Hearing nothing more, I think we can close. Thank you again all for participating and listening. Oh, sorry. Go ahead.

İDIL KULA: I actually showed my question to the chat, but I guess you didn't see, but I'm now voicing it. I wonder that you, do you implement ISO 4201 kind of standards beside the contractual compliance procedures? Like, do you tackle with those ISO IAC

standardizations too in your implementations? Because I thought it might be necessary to implement those kinds of standards, for example, in automatic takedowns of malicious or suspicious DNS cases. Yes, thank you. You can see the question in the chat, by the way, too.

JAMIE HEDLUND: Yes, thank you. Thank you for that. We didn't see it in the Q&A, which is why we missed it. But thank you for the question. The short answer is no; we don't implement that. It doesn't mean that we shouldn't or that we shouldn't look at implementing ISO standards as a means of enforcing the agreement. I'm not familiar with it, I'm not sure.

I don't understand the link between that and automatic takedowns. Just so you understand, we in compliance do not do automatic takedowns. There are obligations under which in the right fact scenario under which a registry or registrar would be required to take action to mitigate or stop a domain from perpetrating DNS Abuse, for example. But those obligations are clearly laid out in the agreements and the advisory and the blogs that we've published. But in enforcing those obligations, we don't rely on the ISO standards. I hope that's helpful.

İDIL KULA: Yeah, thank you so much. Thank you for the information.

JAMIE HEDLUND	Thank you.
İDIL KULA:	Have a good day.
JAMIE HEDLUND	And we have nothing, thank you, Greg, for that. We have nothing to do with AI policies or enforcement, but thank you. So, unless anyone has anything else, I think we'll close. Thank you again, all, for participating. Hope to see many of you in Mumbai in a couple of weeks. Safe travels to everyone who's traveling there. And if you ever have any questions or concerns, please raise them with us. We are always looking to improve how we perform our function and are very much value input from the community. Thank you, all.

[END OF TRANSCRIPTION]