ICANN82 | Prep Week – Contractual Compliance Update
Monday, February 24, 2025 – 12:30 to 13:30 PST

JONATHAN DENISON

Hello, and welcome to the Contractual Compliance Program update pre-ICANN82 webinar. My name is Jonathan Denison, 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 the 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. Transcripts will be provided for all prep week sessions in Arabic, Chinese, English, French, Portuguese, Russian, and Spanish. If you would like to speak during the 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 enforcement of the DNS Abuse mitigation requirements, enforcement of RDAP requirements, the Contractual Compliance audit, and support of policy and working group efforts. Please check the chat box for instructions on how to submit questions and or comments. I will post those just after this and I hand the floor over to Jamie Hedlund, Senior Vice President

Contractual Compliance and US Government Engagement. Thank you.

JAMIE HEDLUND

Thank you, JD, and hello, everyone, and thank you for joining our Compliance program update. As JD mentioned, my name is Jamie Hedlund, and I lead ICANN org's Contractual Compliance function.

The ICANN community develops consensus policies related to the security, stability, and resilience of the Internet's domain name system. Once adopted by the Board, ICANN org incorporates these policies into our contractual agreements with registries and registrars. The primary role of ICANN Compliance is to ensure that registries and registrars implement these community-developed policies and comply with all their contractual obligations in order to preserve and enhance the security, stability, and resilience of the DNS.

We enforce these obligations by addressing external complaints, conducting regular audits of the contracted parties, and undertaking proactive enforcement efforts. We are committed to transparency and regularly publish metrics and data on complaint-related activities and enforcement actions. We support policy efforts and contract negotiations by providing input on the clarity and enforceability of proposed obligations, as well as complaint processing enforcement and enforcement data to inform discussions around existing obligations.

Finally, we participate in training and outreach sessions around the globe to increase awareness regarding contractual obligations among the community. And now, for a review of our DNS Abuse mitigation activities, I turn it over to my colleague, Romulo Chacin. Romulo?

ROMULO CHACIN

Thanks, Jamie. Can we go? Perfect, thanks. Hello, everyone. My name is Romulo Chacin, and I will be presenting on the Enforcement of DNS Abuse Requirements. So, jumping right in, on April 5th, 2024, new requirements related to DNS Abuse mitigation became effective in both the Registrar Accreditation Agreement and the Base Registry Agreement. On this day, ICANN contractual Compliance started enforcing the requirements and reporting on it.

At a high level, there is now a definition of DNS Abuse. For the purposes of the Registrar Accreditation Agreement and the Base Registry Agreement, this means malware, botnets, phishing, farming, and spam, when spam is used to deliver one or more of the other four types of DNS Abuse. Also, contracted parties are now required to take mitigation actions with a target outcome of stopping or disrupting the use of domain names for DNS Abuse.

There is a clarification that the contracted parties' abuse-dedicated email or web form must be readily accessible on their website, and there is a requirement for contracted parties to provide reports with confirmation that their abuse report has been received.

ICANN org produced an advisory with guidance and information on how we enforce these requirements. This advisory is available at ICANN org's website, and it's also linked at the bottom of this slide for your reference. Now, with these requirements in mind, we can go to that slide. Thank you. And I'm going to turn it over to Leticia Castillo.

LETICA CASTILLO

Thanks, Romulo. Hi, everyone. This is Leticia Castillo. Romulo provided a high-level explanation of the DNS Abuse mitigation requirements that we started enforcing last year. During our last program update, we provided some metrics related to the first six months of enforcement of those requirements. And today, I am sharing some updates on initiatives we are working on and updated numbers to include data from April 5th, 2024 through December 5th, 2024.

And as you can see on this slide, during this period, we launched 249 investigations with registrars and registries regarding DNS Abuse mitigation requirements. Most cases involved phishing, either alone or alongside other types of abuse or DNS Abuse. The domain names were reportedly used to impersonate governmental institutions, online stores, financial entities, and others. Two of the investigations led to formal notices of breach, one to a registry and one to a registrar.

On February 5th, we issued another formal notice of breach to another registrar for a phishing case with a domain name that was

targeting a company that offers financial services around the globe. During this period, we also resolved over 200 DNS Abuse investigations through informal resolution. And this is without the need for a formal notice of breach, and leading to the suspension of over 2,900 abusive domain names and the disabling of over 365 phishing websites.

The informal resolution stage is where most of our investigations are resolved in close across all complaint types. And this is because the contracted party either proves compliance or remediates a non-compliance before escalation to a formal stage takes place. And I want to emphasize that while notices of breach are important, they are not the only indication that enforcement is taking place. Enforcement, remediation, inaction occur even they're not reflected on a public notice of breach as this over 200 resolved cases show.

It is also important to point out that ICANN Compliance has visibility into the domain name and the cases that are subject to our complaints, not over the entire DNS ecosystem and all the actions that registrars and registries take to combat DNS Abuse and to comply with their contractual obligations without ICANN Compliance ever contacting them.

In June 2024, we began publishing reports related to the enforcement of the new DNS Abuse mitigation requirements. These reports are broken out by the type of DNS Abuse. They start with April 2024 data and are updated every month. And we have

been complementing this monthly metrics with blogs and reports that include more context and examples similar to the one we published on November 8th for the six months of enforcement. And we will also release a report after completing the ongoing registry audit, which includes DNS Abuse mitigation requirements.

Next slide, please. Thanks. As I mentioned before, notices of breach are issued when the informal resolution stage of our process is exhausted without resolution. These notices are public. They list the identified violations and what actions need to be taken to cure those violations. Related to DNS Abuse mitigation requirements specifically, we have issued three formal notices of breach so far. Two registrars, one to a registry operator. In accordance with the contracts, registrars were initially given 21 days to cure, while the registry 30 days to become compliant. The three notices of breach are ongoing. They have received extensions to the deadlines while they contract the parties continue to actively work on remediating and becoming compliant.

Next slide, please. And it is not uncommon for us to extend deadlines to notice of breach when certain requirements are met. And this includes the registrar or registry has taken mitigation action on all reported abusive domain names, not just on the initially identified case, but in some cases, on additional domain names discovered throughout the course of this specific investigation. So to be clear, not extension is granted if the abusive

domain names continue to be active and prolonging the exposure of potential victims to the DNS Abuse.

For example, one of the notices of breach was issued for a case involving over 90 domains. And today over 5,000 domains have been mitigated resulting from that notice of breach. We have not yet include the number in our reports because the matter is open and we have been reporting on mitigated domains resulting from resolved cases, but we will be including those updated numbers in our future reports. We have continued to collaborate with the reporting party who has been very responsive and provided additional information. We have continued to investigate and work with the contracting party to ensure mitigation action are taken in a process put in place, but this remained open.

We grant extensions also only if the contracted party has presented us with a detailed remediation plan with a reasonable timeline considering the changes that are needed and demonstrates that the different stages of the plan are being implemented. For example, if stage one of the plan is to be completed by December 4th, on December 5th, we will require confirmation that this was done and test as necessary. And then we will continue considering additional extensions for the remaining stages of the plan as needed and as appropriate.

And also, important to keep in mind, this is a complex matter. ICANN also requires time to review and when applicable test different stages of the plan and communicate feedback, requests

for the information and for action. So, this is also factor in when providing extensions. We will include more details about the status of the notice of breach and any future one in our future reports.

Next slide, please. So, what's next? We're going to continue enforcing the requirements that we have since the day they became effective and reported on it. Not just through our monthly dashboard, we will also intend to release a one year of enforcement report like we did with a six-month report and incorporating some of the feedback that we received regarding that report as well.

We launched a registry audit in October that is currently ongoing. Joe will talk more about it in a little bit. This audit included DNS Abuse requirements, and we will publish the report once it's completed. We're also preparing a registrar audit that will incorporate DNS Abuse mitigation requirements as well.

In the six-month report, we mentioned how we are working on initiatives related to facilitating the submission of actionable complaints to us, including the production of guidelines and other materials for complainants. We're working on this. We do not have a date for publishing it yet, but the documents are drafted, and the entire team of processors have reviewed the data we have gathered throughout the months and shared our own experience, and we do believe that providing this type of additional guidance for complainants will be beneficial, so stay tuned.

And lastly, considering the experience that we have gained and continue to gain throughout the month of enforcing these new

requirements, we're working on designing more proactive enforcement efforts. Again, we don't have a date to launch this yet. It is at the design stage, but something important to keep in mind is that we have never been limited to the information detail and the complaints that we receive. We always conduct a comprehensive review of each case. We note and investigate patterns.

We also have the proactive monitoring in the forms of the audit, and now we're designing a structured initiative to proactively initiate enforcement actions for DNS Abuse that, combined with our daily enforcing via the complaint processing and the audit program, will continue to demonstrate our ongoing commitment to uphold the new requirements. So, a lot to come. Stay tuned. And now I am going to hand it over to Amanda, and I will be happy to answer your questions at the end. Thank you.

AMANDA ROSE Thanks, Leticia. We can move forward. Next topic on the agenda is enforcement of RDAP requirements, which I'll be running through. This first slide just discusses kind of the current state of the requirements and where we're at in terms of registration data directory services. As of February 2024, both registrars and registry operators were required to be in compliance with all RDAP requirements, those that have them incorporated into their agreements, which includes all of the registrars and the majority of the registry operators.

Those requirements include import or implementation of the response profile, as well as the technical implementation guide. These requirements expand on just basically having to have a general RDAP service, which is what we were enforcing prior to the February enforcement date. So that's basically instructing how to implement it exactly from a technical standpoint, but as well as what information must be returned in an RDAP query response.

So right now, there are two versions of the response profile and technical implementation guide, both. There's the February 2019 and the February 2024. The February 2024 is the new version to align with changes in requirements related to the registration data policy. So, by August 21st, 2025, this year, the February 2024 version must be implemented, and again, that aligns with those requirements, so the effective date of the registration data policy is that same date. Until then, they can either implement the 2019 or the 2024 at this point.

Additional requirements include service level requirements. So that's in both the base registry agreement and the RAA. We've begun automated monitoring of these requirements as well, so those are being incorporated into our compliance processes. Registrars only, they have a requirement to provide ICANN with one registered name. That's to be used in our testing and how we look up the RDAP service. So once that's provided, we use that to monitor and to test conformance with both the technical implementation guide as well as the profile. Those that do not or

have not provided it yet, we will use the domain name at random, so it's obviously beneficial to have that test case.

So, in terms of where we're at for RDDS or data directory services, the WHOIS sunset date is now passed. That was on January 28th of this year. At that point, most contracted parties, registrars, and registry operators are no longer required to provide WHOIS services. Many still do, and that's an option under the amendments to continue providing WHOIS. And if they do, they have to continue to meet certain requirements, such as complying with the requirements under the registration data policy or the temporary specification at this point, which is the interim policy. But they can also do a truncated display, in which case they have to include a message referring the querier to the RDAP service so that they know at that point WHOIS might not provide all the information, so we need to go to a new data source.

We can move to the next slide. In terms of enforcement, we enforce both the requirement to have a service, as I stated previously. That was starting in October 2019, and I believe we're at about 12 contracted parties, registrars that have not provided a basic RDAP service, or their URL, which there has to meet a minimum test from IANA services. So that does not include the profile and the technical implementation guide. And as I stated on the prior slide, we did not begin enforcement of those until the amendments were incorporated into the agreements, which attach those requirements.

So, we have ramped up enforcement since the amendments took effect and the ramp up period for the RDAP implementation was over. Since then, we have issued 15 formal notices of breach that have included RDAP requirements to cure their RDAP non-conformance into the notices of breach. One of these notices was based on failure to provide an RDAP service, and that escalated to termination of the registration accreditation agreement.

With respect to most of the other cases that we have in process or have closed, we continue to monitor their RDAP services. And given the technical nature of these types of cases, those that are remediating or becoming compliant give us regular updates similar to what Leticia described with respect to the DNS Abuse amendments requiring they meet certain milestones and explain what process they have in place and what they're doing to ensure that their RDAP is conforming to these requirements.

We can go to the next slide. These are some of the common issues of non-conformance that we see. The first are the technical implementation guide requirements, and these are by best discussed by our technical folks, but this is what we see. There's a content type header that needs to be set specifically to code "application/RDAP+JSON". So, when these aren't set, our conformance flag will come up, and these RDAP services may fail even when they're working at lookup.ican.org, for example. Other web clients may not be able to parse the data such that it would return an error.

There are, I think, if anyone listened to the RDAP presentation earlier today, I believe Andy Newton said there's approximately 30 to 40 various web clients out there that are other than ICANN lookup. So, it's important that those are able to be compatible with that, and that is part of the content type requirements.

The other common issue we see is that the RDAP service is provided only over IPv4. It's required to be provided under both IPv4 and IPv6. Another issue we see often is that it is provided over HTTP, and it has to be HTTPS only, so that will flag as a security issue. The last and common one we see is where the RDAP service does not return a 200 HTTP status. Basically, if the domain is sponsored by the registrar, it has to return a 200 okay status, and if it is not sponsored, then it has to return a 404 not found status.

In terms of the response profile, I'm going to say these in reverse, but one of the main things that I'm seeing more and more now is that registration data that's required under the contracts is missing from the RDAP response. We have the registrant contacts and sometimes the admin and technical contacts, or even the registrar might be missing, or the abuse contacts. Those are missing in their entirety, and that is an issue with the response profile itself. Another issue is that the EPP statuses might not be mapped correctly, because the old WHOIS statuses have been changed under RDAP to the required RDAP statuses instead.

And then the last one, this is an issue. The profile describes exactly how notices must be in RDAP. These were also required under

WHOIS, but things like the referral to status codes and what they mean, if those aren't matched or properly formatted, then it will flag as non-compliant, and that issue should be addressed as well. So, there's many more. If you look at the technical implementation guide and the response profiles, you'll see a lot of requirements. So, we have a lot to work through. Sometimes they're quite easy open-shut cases, and often they are not. So, this is just a quick summary of some common ones that we do see.

And then the last slide is just some resources that we have. ICANN has developed an RDAP Conformance Tool. This is available on the web, and it's also available on GitHub, and that information is available from the RDAP presentation if you go to that as well. So, it can be run locally on a drive or system, and then it can be run over web form or web-based, I guess. So, it's recommended for all contracted parties to test that.

One thing to note, that it is only currently supporting the February 2019 RDAP Profile and Technical Implementation Guide. We are working on updating it to accommodate February 2024 versions. But also I wanted to note and plug that that still does flag issues across both.

So, the Technical Implementation Guide is largely based on the current RFCs, and that doesn't change between the versions. So, all of those flags are going to help or still work if you have implemented or if the contracted party has implemented the February versions already. So, there's a lot of crossover. There are

some minor things that have to be updated, but it should be beneficial to use this tool either way.

There is another link for our RDAP Conformance Tool Wiki. Our technical service colleagues have worked to provide resources helping explain a lot of the information that's in the conformance tools. So, that is quite useful in implementation as well as diagnosing issues that have popped up.

And then the last one is the RDAP Guide. This is Andy Newton's own third-party resource, but it is quite informative on RDAP requirements for anyone that is curious. And he has graciously volunteered to let us share that, which I find helpful from a compliance perspective as well for folks that may not be as technical to help dive in and understand what is required. With that, I think we can turn it over to audit. Joe Restuccia.

JOE RESTUCCIA Thanks, Amanda. Hi, everyone. I'm Joe Restuccia. I'm a member of the Compliance Audit team, and I will be highlighting the current and ongoing registry audit. The audit launched at the end of October of last year, and it is a full-scope audit, meaning that we are testing all of the obligations that we typically test that are part of the registry agreement and ICANN policies.

But one key thing to note is that additionally, we are also testing the new DNS Abuse requirements. The testing that is revolving around those requirements is focusing on verifying that registries

understand their obligations and that they have the necessary processes in place to address DNS Abuse. Where the audit currently stands at this point is that all of the auditees have responded to our request for information, and the audit team is reviewing all of those responses, all of the documentation that we received, and we are asking follow-up questions and seeking additional information or documents as necessary.

Following the audit, we are going to publish a final report. It will be public, so you will all be able to see it, and this is a report that we always publish at the end of every single audit. And it will include many things, but a couple of things that it will include is a high-level summary of the audit, as well as some additional information about the findings that we found. And with that, I will hand things over to Jonathan Dennison.

JONATHAN DENISON Okay, that's me. I am just back with regular reminders about some of the other activities that Compliance is involved in outside of addressing cases, compliance cases. Some of you are aware, of course, that we are regular contributors to ongoing policy development and research work. A lot of times we provide metrics and data to help inform community discussions on specific topics like domain name abuse or renewals of gTLD domain names.

We also take a look at proposed policy language and contract provisions. Of course, from our perspective, we like to see things that are clear and enforceable. It makes our job a lot easier.

Essentially, when we are involved in these things, we have subject matter experts that are assigned to whatever relevant policy development that is going on, and they are dedicated to attending those ongoing sessions and providing feedback. It takes a lot of time, but we are always happy to be a part of it.

We also are involved in training and outreach sessions. A lot of times it could be one-on-one with contracted parties as needed, or sometimes we have broader ICANN outreach sessions that are interdepartmental, and we often attend those as well or as requested. Here on this slide, you can kind of see some of the current projects that we have been a part of. ccPDP4, IDNs, EPDP Phase 2 implementation, and everything else listed there.

We have, of course, the dedicated page for metrics and dashboards, which we leverage a lot when providing this information. And I think that's about it. You can take a look there. Yeah, and then we're at the Q&A. I actually don't see anything in the Q&A pod, so now's your time if you have anything for us. I see Nigel. Are you able to unmute, Nigel?

NIGEL HICKSON Yeah, yes.

JONATHAN DENISON There we go.

NIGEL HICKSON Am I unmuted?

JONATHAN DENISON Gotcha. Yeah, we can hear you.

NIGEL HICKSON All right. Yeah, well, thank you very much indeed. Thank you, Jonathan, and thank you for all the presentations. Really, really informative and clear and good to see what's going on and be very interested to hear the results of the registry audit. My question goes right back to the beginning, really, and it was quite revealing, I think, really, to see that. I did write some figures down, but I can't find them. Of the 204, was it?

JONATHAN DENISON You're talking about abuse, Nigel?

NIGEL HICKSON Yeah, well, you're--

JONATHAN DENISON I can go back to the slide.

NIGEL HICKSON Yeah, no, I'm sorry. Yeah, I don't want to take much time.

JONATHAN DENISON No worries. I think this one, maybe. Yeah.

NIGEL HICKSON Yeah, that's right. So, you resolved 204 mitigation investigations and that resulted only in a few breach notifications and things like that. And you mentioned that if it could be resolved, if these investigations could be resolved by the registrar or the registry taking appropriate action, perhaps taking down the domain names, and you mentioned 2,900 domain names and the disabling over 365 phishing websites.

So the question is, so I'm a registrar and I'm found guilty and I immediately react and solve the problem. But then perhaps I do it again. And of course, sometimes I might get away with it. But then perhaps there'll be another report of my non-compliance or the fact that I'm hosting the dodgy websites. So, I wondered whether anyone can make a mistake once. But if you get the same registrar in more than a couple of reports in a year or three or four reports running or whatever, what do you do then? You don't just let them get away with it, I assume.

LETICIA CASTILLO Thanks, Nigel. Hi, this is Leticia Castillo. Great question. So, we have remediation plans that are locked into our system and flag and monitor. So, these plans are required where if failure is identified that affects multiple domains or system beyond our processes, maybe lack of process to address DNS Abuse. And those

go beyond the specific case. And the root cause must be addressed to prevent its recurrence, which is what you were pointed out.

So, for example, we have a registrar, just an example came to my mind, that admitted that the team was not prepared to address a report. They were still learning how to handle this DNS Abuse reports and the case at hand was not handled properly. This registrar presented a training program to us as part of this remediation plan, detailing the program duration, materials used, who will lead it, how the success would be measured.

The implementation plan was confirmed at the end of October. And we closed the case. We are now monitoring new complaints and signs of recurring failures for this specific registrar. It is too early to determine whether the plan was fully effective, but we do require remediations that are detailed, documented in the system and monitored. And a repeated failure for a previously resolved matter results in expedited Compliance action. So, we will not go through the normal process. We will be expediting the matter and potentially issue multiple breach notices, which have a direct impact on the contracted parties' accreditation with ICANN.

NIGEL HICKSON Thank you very much.

JONATHAN DENISON All righty. Any other curious minds out there? Otherwise, I can hand it to Jamie for a little outro or something.

JAMIE HEDLUND Outro. I like it. Thank you, JD. Thank you all. And thanks to everyone for joining today's webinar. We look forward to seeing many of you in Seattle. And please, if you see us, stop us and ask us any questions you may have or ideas or suggestions for us or send us an email. We are always looking for ideas about how we can do our jobs and provide information that's more relevant and helpful for everyone. I really appreciate everyone's time and safe travels to everyone going to Seattle. Thanks.

JONATHAN DENISON Thanks all. I reckon we can stop the recording.

[END OF TRANSCRIPTION]