ICANN81 | Prep Week – Contractual Compliance Update
Monday, October 28, 2024 – 9:00 to 10:30 PM TRT

MAY KIM: Hello and welcome to the Contractual Compliance Program update pre-ICANN 81 webinar. My name is May 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. I will read them aloud at the end of the presentation. Interpretation for this session will include English, French, Spanish, Chinese, Russian, Arabic, and Portuguese. Click on the interpretation icon in Zoom and select the language you will listen to during the session. 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. All are welcome to use the chat. Please note that private chats are only possible among panelists in the Zoom webinar format. Any message sent by a panelist or a standard attendee to another standard attendee will also be seen by the session's hosts, co-hosts, and other panelists. In this session, we will be discussing enforcement of the DNS abuse and abuse requirements, enforcement of the RDAP requirements, contractual compliance audit, and the support of policy and working group efforts and other community initiatives. Please

check the chat box for instructions on how to submit questions and or comments. With that, I will hand the floor over to Jamie Hedlund, SVP Contractual Compliance and Government Affairs.

JAMIE HEDLUND: Thank you, May, and thank you all for joining our session this morning. I am head of Contractual Compliance and U.S. Government Engagement. Our role in contractual compliance is to ensure that the policies developed by the ICANN community and adopted by the board are fully implemented by gTLD registry operators and accredited registrars. We ensure that the obligations are implemented to ensure to preserve the security, stability, and resiliency of the domain name system. How do we do this? We do this through addressing compliance complaints submitted by third parties, through proactive monitoring, and through conducting contractual compliance audits twice a year. We publish and maintain granular metrics and data on our enforcement efforts, and we hope that that data and those reports are helpful to the community and to inform the work that it does. We support policy and working group efforts by providing data and input regarding enforcement and enforceability of obligations, very active to ensure that any obligations that may be being considered are clear and enforceable. And then finally, we participate in a large amount of training and outreach sessions, both the contracted parties and other parts of the community, to talk about what the contractual obligations are and discuss how we enforce them. Today we'll focus on a few areas that are prominent among the community, and we hope will be

insightful. These are on DNS abuse, RDAP, and the ongoing contractual compliance audit. With that, I will turn it to Leticia.

LETICIA CASTILLO: Thanks, Jamie. Hello, everyone. During our last program update in February, we talked about how ICANN Contractual Compliance was getting ready to enforce the DNS abuse requirements starting on April 5th. This included preparing our web forums to facilitate the submission of complaints and preparing our systems to process those complaints and capture data to report on it. April 5th came, we started enforcing the requirements and reporting on it in detail, as I will explain in a minute. But first, at a high level, these are the requirements. There is now a definition of DNS abuse for the purpose of the Registrar Accreditation Agreement and the Base Registry Agreement. And this is malware, botnets, phishing, pharming, and spam, when spam is used to deliver one or more of the other four types. Contracted parties are now required to take mitigation actions with the target outcome of stopping or disrupting well-evidenced DNS abuse. There is a clarification that the contracted party's abuse-dedicated contact must be readily accessible on the contracted party's website. And there is a requirement for the contracted party to provide each reporting party with a confirmation that an abuse report has been received. ICANN Org produced an advisory with guidance and information on how these requirements are enforced. This advisory is available at ICANN Org's website and is also linked at the bottom of this slide for your reference. Now with those requirements in mind, we can go to the next slide, please.

From April 5th, 2024 through October 5th, 2024, so the first six months of enforcement, we initiated 192 DNS abuse investigations with registrars and registries. These were cases that included at least one type of DNS abuse. Remember, malware, botnet, phishing, farming, and spam is a vector, not the total number of abuse-related compliance investigations initiated, including other types of abuse. The total of investigations into abuse, DNS abuse, and other was 363, 192 of those related to DNS abuse. Two of the investigations resulted in a formal notice of breach to one to a registry operator and one to a registrar based on their failure to comply with DNS abuse mitigation requirements, among other obligations. Formal notices of breach are public. You can see them linked within this slide as well. During this period, we resolved 154 DNS abuse investigations within the informal resolution stage of our process. This is the stage in which more investigations are resolved without escalating to public breach notices. This is because contracted parties demonstrate compliance or take action to remediate a noncompliance before that. Again, this is just DNS abuse. The number of resolved cases across all types of abuse was a little bit over 400. Something important to note is that one single investigation can and often does involve multiple domain names. One investigation into a specific number of domain names may result in the discovery of additional abusive domain names that also act on. This explains how our 154 resolved cases resolved in the suspension of over 2,700 abusive domain names. And the disabling of over 350 webpages for which the registrar or its reseller in a specific case was also acting as a hosting provider. Also important to note that these are the mitigated domain names in the cases resolved during this first six months. We

have many ongoing investigations with hundreds of domain names that are already suspended, but not yet counted towards this mitigation number because the cases are still open or were closed after October 5th, but they will be included in future updates.

And speaking of updates, in June, we begun publishing our new monthly reports related to the enforcement of DNS abuse requirements. These reports are broken out by type of DNS abuse. They begin with April 2024 data and they are updated every month. There are links on the slide, maybe you can post them in the chat as well for everyone's reference. We understood that this format, the format that we use, would provide a comprehensive picture, but also complemented with regular updates like the one we're providing today. But we decide these reports as a starting point. The intention is to continue building on them and improving them over time, so we welcome any feedback the community has about them. We have been participating in multiple outreach events related to the new requirements. For example, in September, we participated in a workshop with contracted parties dedicated to different areas of the contracts, but with an emphasis on DNS abuse in Beijing. The same in Istanbul this month. We do work closely with our colleagues in GDS and GSE that lead this capacity building initiatives and participate in them as much as much as we can. Lastly, we have prepared an audit to validate compliance with the registry agreement that includes but is not limited to DNS abuse obligation, and Yan will explain more about this later on in the webinar. For now, let's go to the next slide, please.

I was mentioning before that we resolved over 400 investigations related to both DNS abuse and other types of abuse during the six-month period we're covering. I've added some visuals here of the reasons for resolving these cases. First, we have the investigations into DNS abuse with registrars specifically. In approximately 52% of the cases, the registrar confirmed DNS abuse and suspended all the involved domain names. In approximately 21% of the cases, the registrar did not find actionable evidence that the domain name was being used for DNS abuse, and we deemed it compliant because we received a reasonable explanation supported by any relevant document of what was done and how the conclusion was reached. For example, a registrar assessed all the information they had, including account information and communications with the holder of the account, and determined that the registrar was in fact affiliated with the entity believed to be impersonated, not impersonating it. In approximately 12% of the cases, the registrar took action to disrupt the course of DNS abuse by, for example, contacting the registrant who then removed specific content within the URL where DNS abuse was placed. In approximately 3% of the resolved cases, the registrar took other action that stopped the use of the domain name for DNS abuse. For example, there was a sinkholing or DNS redirection. The registrar took this action so that any user trying to connect to the malicious domain instead was redirected to a control IP address that the registrar had set. Next slide, please.

This next slide shows the number of DNS abuse cases resolved with registries. The number is three, and all registries suspended all involved domain names. We had a fourth case, but just referred to an issue with

the abuse contact that the registrar also fixed. And the big difference in numbers is consistent with the fact that of the total complaints that we received, 94% referred to registrars. And of the total of investigations initiated, 97% referred to registrars. So it makes sense that during this period, we resolved 151 DNS abuse cases with registrars and three with registries. Next slide, the last one.

As we continue to enforce the abuse-related obligations that were enforced prior to April 5th and continue to be enforced, I added here some data about those cases resolved during the period that we're covering. And we're talking about the registrar's obligation to take reasonable and prompt steps to investigate and respond appropriately to reports of abuse, not DNS abuse as defined in the agreements. In this case, there is no contractual obligation to take mitigation actions with a target outcome, but it does require reasonable and prompt steps to investigate the report and respond appropriately. The action that the registrar takes on the case will depend on their own domain name use and abuse policies and their investigation into the matter. Approximately 57% of our cases resulted in the suspension of the domain names in these cases as well. 39% on other actions. The registrar took other actions by, for example, providing the reporting party with information on how to contact the web hosting provider, report determining the activity was preferred to content displayed on the website. The registrar was not hosting it. The use of the domain name was not violating their terms of service, et cetera. This is just an example. And this is all from me. Happy to answer any question at the end. And now I'm going to hand it over to Amanda Rose.

AMANDA ROSE: Thank you, Leticia. I will be presenting on the RDAP requirements and our enforcement efforts to date. So jumping right in, as of February 3rd of this year, that is the date that registrars and registry operators had to be fully compliant with the obligations within their respective agreements, the registrar accreditation agreement and the registry agreements regarding the RDAP requirements. So within each of those, there is the requirement that the contracted parties implement the most recent or current version of the RDAP response profile, as well as the technical implementation guide. As we're in the stage right now of the interim registration data policy for gTLDs, that actually allows the contracted parties to implement either the February 2019 version, which essentially tracks the registration data requirements under the temporary specification. They can do that, or they can begin implementing the February 2024 versions of both of those, which track the registration data policy and the requirements within there regarding the display and provision of registration data in the public directories. So as of the 21st of August of next year, all contracted parties must have the February 2024 versions in place. We also will, are tracking the service level requirements for providing RDAP services. This is in the links there to both the RAA and the RAs under spec 10.

And then with respect to registrars only, there is a requirement in the registrar information specification to provide a ICANN with one self-sponsored registration that enables ICANN to do technical monitoring of their Fort 43 WHOIS and RDAP services. As of, I guess, three months from today, the WHOIS is set to sunset, at least in terms of the required provision of those two services, both Fort 43 and web-based WHOIS. Registrars and registry operators will no longer be required to provide

WHOIS services. However, they can continue, of course, to do so. If they do, then they must meet certain requirements similar to what we see today in WHOIS. However, they can also offer a truncated version of that, in which case they should or must include a notification that directs the inquiry to the RDAP service, which would include the full registration data set. We can go to the next slide.

Our enforcement efforts are essentially geared toward two different things. One, to ensure that the contract parties have implemented an RDAP service and uploaded their URL into the respective database, and also that the RDAP service that it is providing is in conformance with the technical implementation guide and the response profile. So, efforts regarding the actual service itself began in October 2019 and continue to date. That is the obligation to have a service in place that predated the RDAP amendments going into effect as this requirement existed under the temporary specification. But essentially, the information we have to date indicates that all registry operators have a registered URL in the IANA database. And then, with respect to the registrars, there's only a handful of those that have not uploaded their URL into the naming services portal. And that is essentially the way that the IANA registry obtains the registrar's base URL. And we're continuing to follow up with those registrars that have not yet done so. Starting in June 2023, we began enforcement efforts with respect to the RDAP profile and the technical implementation guides. And we continue to follow up with those that are implementing remediation measures, excuse me, tent-tied. And we request regular updates and require regular updates to track those remediations in progress. We can go to the next slide.

This is a little bit on the technical side, but I have noted several issues that we commonly see with respect to non-conformance with these requirements. And that often leads to a broken RDAP lookup. The first is technical implement, or the first few are from the technical side. The content type headers in the RDAP response are not set correctly, which actually causes a failure for web clients to query the data or pull the data and parse it into a user-friendly lookup. So, you might see if you do a direct URL search under the RDAP domain lookup, you can see a very technical output. However, for most people, that is not user-friendly and it's difficult to parse what the registration data shows or means. So, we rely on things called web clients, which parse the data and display it to the querier in a readable format. Without these content type headers, it breaks those lookups and leads to a failed connection. Let's see. Another one we commonly see is that it is not provided over IPv6. It has to be under both IPv4 and 6. The third one we see is that it is provided over HTTP. However, it must only be provided over HTTPS. So, if those are both there, then it will flag an error or nonconformity. And then lastly, a common one we see is that they're not returning a required HTTP status. So, with that, any sponsored domain name must return 200 OK status and any non-sponsored domain will return a 404 not found status. Again, those are very technical, but it may interest our folks that want to look into these further. But a response profile goes more toward the output and the registration data that we actually see. So, one common thing, EPP statuses are not displayed correctly or mapping to the current RDAP mapping. Another one, this is sometimes minor in nature, but the language and the notices that are required to once come to mind, the EPP status code explanation and the

inaccuracy links to inaccuracy complaints are not exactly matching what's required in the response profile. And that will indicate a nonconformity. And then the main one, which is what we would want to look for, is that the registration data that the contracted parties are required to show may be missing or not provided. So, we can go to the next slide.

I just included three links. These will be available with the slides once they're uploaded. But we have been working on making sure that there are tools in place to help implementation, especially leading up to who is sunset in three months. One is the RDAP Conformance Tool. This allows registrars and registry operators to do a self-diagnosis of their RDAP services. And right now it is available for the February 2019 profile and the implementation guide. However, there is work to be done to update it to also accommodate the February 2024 versions. We also have the RDAP Conformance Tool Wiki. This has a lot of helpful information. Some of the codes that come out of the conformance tool may be difficult for, or not as user friendly. So, there are some pages here which help explain the implementation and how to become compliant. And then lastly, there is an RDAP guide that was created to aid users and developers basically in implementing the RDAP services as well. I believe that draws the RDAP section to an end and I'm handing it over to Yan Agranonik.

YAN AGRANONIK: Hello, my name is Yan Agranonik and I am responsible for audit related activities at Compliance. A few words on the previous audit. Earlier this year, we completed the registrar audit. It's a typical, it was a typical full-

scale audit. 62 registrars were under audit and the report is, the consolidated report is published in August. And you can take a look and see all the deficiencies found on the aggregate level. Next slide, please. Right now, we are about to launch a new registry compliance audit. That would be a full-scale audit, meaning we would look at all the provisions that we typically look at. But in addition to that, some new DNS abuse mitigation requirements will be tested and reviewed. We shared requests for information that will be sent to registry operations with registry stakeholder group. And adjusted it in a cooperative way when we received some feedback. You can take a look at the link that is published right there on the compliance audit programs in general. So the plan is to launch a new registrar compliance audit sometime in spring when we are done with the current audit for the registries that we're about to launch. That is all I have at this point.

JONATHAN DENNISON: All righty, thank you, Yan. My name is Jonathan Dennison and I'm here to advertise our work in policy working groups and other initiatives. Most of you know, if you don't, we are often involved in policy development work and a lot of times on the implementation side. And the reason we bring it up is essentially it does require a significant amount of time for our subject matter experts, which I'm sure many on the call can attest to. But there are multiple benefits for us being involved. A lot of times, because we have various metrics and data points that we can provide through our day-to-day work, oftentimes the data can be requested or provided. And it can be kind of influential in kind of framing how policy work is developed and approached. It also,

from our perspective, because we're the ones who essentially inherit anything that comes through policy, we can provide some insights into the feasibility of how the policy is drafted and feasibility of enforcement, which is obviously very important because we all prefer to be aligned, I think, on what's being developed.

The other thing, of course, is that it allows us to make any preparations we need for our sites ahead of time, so we can be ready when policy comes into effect. And I think we can go to the next slide, these are just some examples of some of the initiatives we're involved in currently, or have been in recently. Transfer policy, PDP, working with the IDN guidelines, you can see the rights protection mechanisms, implementation review, next rounds, RDAP, registration data policy, etc., etc. And then some of the other activities we're involved in is just general outreach. A lot of times we're involved with GSE and GDS teams. We come in and kind of provide some information from the compliance side, typically involving current hot issues. You can see here, in October, compliance was involved in an outreach session with Turkish contracted parties, talking about things like abuse requirements, RDAP, how to generally interact with compliance, our approach on things, and various other topics. And I think that's about it from my side. I think we're at the end here. Yeah, there we go.

MAY KIM: Thank you. We can move on to the Q&A portion. So far we have one question in the Q&A. This is from Chris Lewis-Evans, and the question reads, as Jamie mentioned, proactive monitoring at the start, how many of the 192 DNS abuse investigations were due to the proactive

monitoring versus the other mechanisms to start an investigation? And Leticia, do you want to go ahead and take that?

LETICIA CASTILLO: Sure. Hi, Chris, and thanks for your question. So the 192 investigations during this first six months resulted from external complaints. These were mainly submitted by cybersecurity experts, self-identified cybersecurity experts, and representatives of the entities being impersonated. But we're not limited to what the information that was detailed in the complaint. We always conduct a comprehensive review of each complaint, and we address patterns with regards to the domain names at hand, but also with regards to any observed pattern in the suspected parties' DNS abuse handling processes. We have proactive monitoring in the form of the audits that Yan was explaining, and as we gain more experience with enforcing the new DNS abuse requirements, we will launch more proactive monitoring efforts.

NIGEL HICKSON: Yes, thank you very much. Good evening, and thank you so much for the detailed explanation that you've given. I really just wanted to look at this a bit subjectively, and I mean, this is a very interesting report. Now, I'm talking about the six months, April to September, the time that the new compliance measures have been in place, and the report that you've written, and I suppose the subjective question is that in terms of your interaction with the contracted parties, has this been helpful having these new compliance measures? Has it been easier for you to obtain the information? What's your feeling? Has it been, in terms of

what you have to do, has it been a useful exercise having these new compliance measures? Thank you.

LETICIA CASTILLO: Thanks, Nigel. That's a very interesting question. So we always say it's important to allow sufficient time for the implementation of new amendments to accurately measure their impact, if that's what we're referencing. The vast majority of the cases that we can only speak, we only have visibility over the DNS abuse actions that are taking place with regard to our cases. The vast majority of those cases were resolved without us escalating to informal enforcement actions. So the contracted parties either demonstrated compliance or they understood they were not in compliance, and they provided us with a detailed remediation plan of what they were going to put in place to make sure they became and remain compliant with the agreements. And I can give you an example. We had a registrar that said, yes, we did not have the processes in place, and we have created a specific program from our personnel to train them in the DNS abuse requirement. And this is how the program is going to be implemented. These are the milestones. This is the person who is going to provide the training and how we're going to test that the people addressing these reports have this knowledge and how we're going to assess it. So contracted parties have been responding to us. They have been demonstrating compliance. They have been taking actions to become compliant, if that is the question. But I'm not sure if I replied to your question specifically.

NIGEL HICKSON: No, thank you very much. That was very helpful. Thank you.

MAY KIM: All right. And it looks like we have a question in the webinar chat. How does compliance monitor registry operator compliance with registrant eligibility requirements where safeguards apply? Example for professional licensing. Yan, would you like to answer that?

YAN AGRANONIK: Yes, I can answer that. In previous audits, when those registry operators with the requirements to verify eligibility were included, we had certain questions in RFI and tests to make sure that something is done to verify registrants' eligibility. For example, if there is a professional license is required, then we asked to show and describe the procedure how the registry operator verifies that. So through audits, we do that. I don't know if we had any complaints about it. I'm not aware of that, at least I don't know. But answering your question, the audit is a mechanism to verify that.

MAY KIM: All right. Thank you. There are no other questions in the Q&A or in the chat. It looks like there are no hands up either. So as you can see on this last slide, additional questions can be sent to compliance@ICANN.org. ICANN contractual compliance web forms are available online, as are ICANN contractual compliance metrics and reporting. Information about the audit program is also available at the link provided. This presentation will be posted on the ICANN 81 schedule, and that will be

later on. Let me see. Oh, it looks like there is one more question. And, Yan, it looks like this question is towards you. This is, how are audit candidates chosen?

YAN AGRANONIK: Well, the current round, we choose the candidates using several criteria. We used internal data that ICANN collects on the DNS abuse reports. We also use several other criteria from external parties and internal parties to pick the candidates. For example, number of complaints received. And we will be sharing those criteria with Registry Stakeholder Group. Actually, we already did, but there will be some additional information provided.

MAY KIM: All right, thank you. Any other additional questions? All right, looks like everyone is good for now. Thank you for everyone who presented and everyone who joined us today. Thank you all.

[END OF TRANSCRIPTION]