ICANN86 Seville | PF – ccNSO: Joint Session with GNSO RySG
Wednesday, June 10, 2026 – 11:45 to 13:15 CEST

CLAUDIA RUIZ

Hello, and welcome to the ccNSO Joint Session with GNSO RySG. My name is Claudia Ruiz, and I, along with my colleague, Joke Braeken, are the participation managers for this session. Please note this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior, and the ICANN Community Anti-Harassment Policy.

Please observe the following guidelines to participate in this session. They will be posted in the chat for your reference. During the session, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat. 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, virtual participants will be given permission to unmute. On-site participants will use a physical microphone to speak and should leave their Zoom audio disconnected.

Please state your name for the record and the language you will speak, if speaking a language other than English, and please speak at a reasonable pace to allow for accurate interpretation. Thank

you, and with that, I will now hand the floor over to Alejandra Reynoso, moderator for this session. Thank you.

ALEJANDRA REYNOSO

Thank you, Claudia, and welcome, everyone, to our joint session, ccNSO and the Registry Stakeholder Group. Today, we have with us our new chair, or interim chair of the Registry Stakeholder Group, so let's give a warm welcome to Keith Drazek.

And with that, as you may remember, we had a session a while ago in ICANN83, where we identified topics that we thought would be of common interest to discuss together, so today we are going to explore those, first with internet governance with Annaliese and Jennifer, then we will discuss a little bit on DNS abuse and the PDP that's running now with Nick and Brian, and finally, we will talk about the root server system governance with Peter and Sam. So, with that, let me give the floor and the clicker to Annaliese to start with the internet governance topic. Thank you.

ANNALIESE WILLIAMS

Good morning, everyone. My name is Annaliese Williams from the .au domain administration, and I'm the Chair of the Internet Governance Liaison Committee. The IGLC was established to facilitate discussion amongst ccTLD managers and encourage their participation in internet governance discussions and processes, including those that take place outside of ICANN.

It's a very regionally diverse committee, we have about 30 active members, I think, from across and we have active members from all of ICANN's regions who participate regularly. So, we meet to discuss policy and regulatory and legislative developments in our countries and regions and the impact of those on ccTLDs, just to sort of share information and discuss how problems are being addressed and discussed in our countries and what we can learn from each other. Thank you. If you could get the thing, that would be excellent because I can't see from over there. Thank you.

So, we have prepared documents in the past to inform ccTLD members on internet governance issues that may be of interest and explain for those who aren't following them closely what the impact or potential impact is on a ccTLD manager and we also coordinate closely with other groups across the ccNSO. Yesterday, we had a joint session with TLD Ops and the IANA Disaster Study Recovery Group on resilience, DNS resilience.

So, thank you to the registry stakeholders for meeting with us today. I think this is perhaps a good opportunity for to begin an ongoing discussion. I think many of us are dealing with regulatory initiatives that particularly around cyber security or online harms, DNS abuse. It's an area that we think there may be many common interests between the ccTLDs and gTLDs.

This is some of our recent highlights, the work that we have done and the speakers that we have featured. Throughout last year, we had a bit of a focus on the World Summit on the Information

Society. Many ccTLD managers are closely engaged with their national governments or providing advice to their governments or, in some cases, supporting them by participating on national delegations to these UN processes. But many other CCs are not following it at all.

So, we've had some sessions to explore what it means from the perspectives of ccTLD managers. We sort of have a mix of speakers. We have some external guests. We had last year we had a session with the co-facilitator of the WSIS process and Vint Cerf talking about the IGF and what that means for the importance of the IGF and the importance of technical community engaging in these global dialogues.

And at the last ICANN meeting, we had a session just on updating various regulatory developments that are taking place in different jurisdictions and just sharing the impact and how that impacts on the CC and how CCs are addressing them. So, yeah, I know the whole IGLC would welcome the opportunity for ongoing dialogue with the registry stakeholders. So, thank you for participating and in joining us in this. I might leave that there and pass over to Eugene.

Sorry, I had one more slide. These are the themes that we are focusing on for our forward work plan. And we think that these may be areas that gTLDs are also thinking about. So, the future of internet governance is a recurring theme that sort of was a primary theme last year as well. There is the ITU conference coming up later

this year. Sovereignty has been identified as a priority topic in many countries and regions. Online harms and, of course, resilience that we discussed yesterday.

These themes, we sort of engage with the members and ask them to let us know what the issues are that are being discussed at IGFs or in policy circles or what governments and communities are concerned about and to sort of share that information. And there are some that sort of emerge as a priority topic in pretty much every country and across the regions. So, those are the ones that we sort of pick for future exploration and consideration as a group. Great.

ALEJANDRA REYNOSO: I'll take the transition to remind our speakers to speak at a slower pace because we have interpretation. So, I know these are exciting topics, but just for the sake of our interpreters. Jen?

JENNIFER CHUNG: Thank you very much, Alejandra. And of course, thank you, Annaliese. Well, first of all, my name is Jennifer Chung. I'm part of the Registry Stakeholder Group and I represent .asia. I'm very happy to have this conversation, especially with the ccNSO, because I think for Registry Stakeholder Group, a lot of our focus is directly on the policymaking part of the ICANN community, of the ICANN context, especially in relation to our operations, in relation to how different registry operators look at the ICANN context and how it impacts the work that we do.

We don't have an IGLC. It's really nice that the CCs do have that. But certainly, the work that we do at the Registry Stakeholder Group , we focus on the actual policymaking. So, we focus a lot on kind of doing the doing, the part of the multi-stakeholder, bottom-up policymaking context that we do at ICANN.

So, every year, or it's been every year for the past few years, we've had this Contracted Parties Summit. And this is where the registries and the registrars get together and they discuss a lot of the items that we don't normally discuss at ICANN meetings, because ICANN meetings is really filled with a lot of the policy development part. But at the Contracted Parties Summit, I think for the past three years, we've come up with a summit statement. And it really kind of encapsulates how the contracted parties and, of course, registries being part of it, really view the work in a longer lens.

And I think I've extracted the key points here. We support this multi-stakeholder model, a way of internet governance in improving our efficiency in policymaking, in improving our engagement through intentional collaborative relationship building, which this very session is one of them. And then, of course, monitoring involving technologies and how it impacts security and stability of the DNS. So, I think that kind of maps quite neatly onto Annaliese's last slide, when she identified the areas of common concern and places where we can collaborate further.

I mean, I put a link there, and I hope this slide deck is also circulated to all of our membership, so we can actually click through to see the full summit statement. Of course, our concentration now is on these three points, but there's a lot more elaboration you can take a look at if you're able to click through. But I won't go into too much detail here.

One area that I think that, I guess, the Gs and the Cs already do collaborate, and this is not going to be new to you as I go to the next slide, is the TCCM. It's a technical community coalition for multi-stakeholderism. And actually, Annaliese next to me, and I see other TCCM members in the audience as well, the focus this year on a lot of the work is to look at the ITU plan in part.

And I think this comes quite natural for a lot of the ccTLD managers that work very closely with their country governments. For the Gs, there is one more layer or a few more layers for us to be more involved, because for the ITU plan in part, that's very much member state delegations that go there. However, what is being discussed at the ITU plan in part absolutely does still impact both the Gs and the CCs, and actually the internet governance space.

So I think those who are interested to know more about this, I think this is one area of good collaboration in TCCM. And I'm not just saying it because .asia or myself, we're quite involved with this work. It's actually a good primer to understand, actually, what are these considerations? What are the resolutions that might impact us? And here's a good set of maybe items of concern, or if you're

more interested and want to deep dive into it, then, of course, certainly consider joining. And there is a working group that works on it. I'm looking at Annaliese, and she looks like she's smiling. So do know a little bit more about that.

The two other items there, obviously, is also quite clear. This is TCCM's focus. One is to look at the IGF, the Internet Governance Forum. Last year's World Summit on the Information Society, WSIS, it was a 20-year review. One of the most successful outcomes, at least for this community, I think, is the permanent mandate for the IGF was achieved.

And what that actually means for us here, for the CCs and the Gs, and I think for the ICANN community as a whole, is we don't have that question mark anymore, whether or not we're able to continue discussing Internet governance and digital processes issues in a multi-stakeholder way. And this is actually a very good endorsement for us to continue to be able to support the way we do our policymaking here, the way we do our operations, where we do them.

And then finally, the last bullet, I don't think I need to elaborate anymore. We are all here because we do support the ICANN processes that reinforce the ICANN flavor of the multi-stakeholder model. My last slide here, I've been asked to kind of walk us through a little bit of the preparation upcoming up of the Internet Governance Forum this year. This is just the draft timeline, which I think is probably going to be pretty, I don't want to call it final

because there might be somewhat small adjustments, but do take this as a blueprint of how we're going to get to the very end, which is the successful hosting of the IGF and its new permanent mandate in Nairobi, Kenya.

We are kind of now in the June area. We already have the first open consultations and multi-stakeholder advisory group meeting announced for Nairobi, and I think that will be in two weeks. It will be in Nairobi and hybrid from the 24th to the 26th of June. I urge those of us who are very interested to actually input into this process. The very first day is open consultations and the mode of the IGF MEG is to actually listen to all community concerns, so anybody could input into this on the first day.

I'm not going to go through the entire thing too much because this is just an IGF process, nothing to do with the registries, but I know there's a lot of people who are interested to know what the timeline looks like for this year because we are nearing the latter half of the year already. I'm going to pause here and am I handing this back to Alejandra? Okay, to Alejandra, thank you very much.

ALEJANDRA REYNOSO Thank you very much, Jen and Annaliese. Are there any questions for them? I'm seeing none in the room right now. Oh, there's one. Oh, yeah, Jordan.

JORDAN CARTER

Thanks, Alejandra. Good afternoon, Jordan Carter, .uk. I had a question for Jen that was based just on the bullet points from the CPS statement. Is the GNSO doing any particular work on improving efficiency and policymaking? I'm interested in that. If it's more than a 30-second answer, maybe you can tell me some other time, but it would be good to know.

JENNIFER CHUNG

I'll give you the 30-second answer and then you can talk to me more. The 30-second answer is the GNSO Council is going to pilot a prioritization mechanism and we will talk about it in the GNSO Council meeting today, so if you're interested, do come to that and we would like to get things more efficient. Ten more seconds on this.

I think in general, our focus for any future and the current PDP that's in flight is to make sure it's tightly scoped, that we go through the timeline in a very efficient manner, but the recommendations coming out of it are board-ready and, of course, beyond that, it is up to board approval, it's up to the IRT, but everything in the Council's power to be able to streamline and be efficient and be effective, those are the things that we're going to do. Thank you.

ALEJANDRA REYNOSO

Anyone else? Okay, seeing no hands in the room or in the Zoom right now, let's move forward to our next topic, and that is on DNS abuse mediation. For that, I'm giving it to Nick.

NICK WENBAN-SMITH

Thank you, Alejandra. For the record, my name is Nick Wenban-Smith and I'm with Nominet .uk. Great pleasure to present here with my counterpart from the gTLD registries, Brian Cimbolic, and we will share this presentation between us.

So, everybody loves talking about DNS abuse. It's the subject that everybody is talking about in many different sessions, and the reason why we wanted to present jointly about it is I think we all appreciate that we are ccTLDs and, therefore, a different species from the gTLDs. We are CCs and we have our own distinct policies, and between ourselves, we also have distinct policies, and everybody understands that. However, when it comes to abuse and the criminals who perpetrate abuse, they are, broadly speaking, agnostic as to which TLDs they use.

So, we should, at the very least, have conversations between ourselves as ccTLDs and our friends in the gTLD registries to better understand the problems and where there are issues as between us, that we can explore those and talk about them in a constructive way, and where there are things to learn from how the ICANN contracted parties operate and how ccTLDs, who are obviously not generally contracted with ICANN, how we operate our policies, then there's fertile ground for cross-collaboration.

So, when it comes to abuse, this is a very important topic, and there's a couple of things that we wanted to touch on briefly today, and actually, just as an introduction to the first one of those, which

is the GNSO's DNS abuse policy process, and just to actually speak to Jordan's question around efficiency, I've been involved with a number of GNSO policy processes. The name expedited doesn't necessarily reflect the speed of the process. So, I think that one was a decade. So, it was an expedited policy process taking a decade.

This policy process is, in fact, quite far ahead of our projected work plan, because, to speak to Jen's point around prioritization and narrow scoping, I have a very specific work plan and a good charter, which helps the policy discussions proceed at speed and at pace through the policy discussions. I'll hand over now to Brian to talk through this, because obviously, it's a GNSO policy process.

BRIAN CIMBOLIC Thank you, Nick. Hello, everyone. My name is Brian Cimbolic. I'm with Public Interest Registry. We're the registry operator of .org. I'm also a member of the gTLD Registry Stakeholder Group. Thank you very much, Nick, for that introduction. I always appreciate the time to engage and interact with my friends in the ccNSO, so thank you for the opportunity.

So, as Nick mentioned, there is an active policy development process going on right now, and it's one of two slash three, I'll get to that, contemplated policy tracks on DNS abuse mitigation. This one deals with what is called an associated domain check. So, a little bit of history.

In April of 2024, the gTLD Registrar Accreditation Agreement and the Registry Agreement were modified to include obligations to deal with DNS abuse. So, this means that for the first time in the history of ICANN, gTLD registrars were required to mitigate, whether that's suspension or deletion, domain names that are engaged in things like phishing. The issue that was kind of quickly identified with that specific contract, which was a big success, was that it basically required action one domain name at a time.

And so, what we've seen in the wild is that there are a handful of registrars in particular, as well as a handful of some gTLD registries, that have extreme footprints for DNS abuse relative to their size. There's a reference on this slide to a campaign that was conducted last summer, and that campaign, that DNS abuse campaign, was targeting the elderly in the United Kingdom. The pensioners in the United Kingdom are eligible for a subsidy for winter fuel to heat their homes. And this campaign targeted recipients of those winter fuel subsidies and created a campaign of 2,200 phishing domains. They were sent via smishing, and 90% of those domains were in one registrar. So, the 2,000 domains in one registrar.

The current Registrar Accreditation Agreement would allow for that registrar to act on one domain and do nothing about the other 1,999, even if there was an obvious pattern. So, we, as a community, sort of recognized this as a gap. I want to note the slide here notes that this PDP is based on a NetBeacon white paper and the contractual amendments. While NetBeacon Institute is part of PIR, that white paper was just one of many inputs into the GNSO

process. There was lots of contributions into that process, several of which also called for a PDP on associated domain checks. So, I just wanted to note that.

So, what we are hoping to accomplish here is closing that loophole. So, that exact same registrar, once this policy is implemented, would have to check its accounts, see if there were other domains engaged in similar abuse, and would be obligated to, in this example, suspend the other 2,000 domains at once. So, it really takes the burden off abuse reporters and requires that registrars look into the accounts, look for other abuse, and act on it. So, ultimately, while this PDP won't ultimately reduce the prevalence of DNS abuse, it will ultimately make mitigation significantly faster in the gTLD space.

I want to note that several ccTLDs are already doing these associated domain checks, particularly those of you that have a direct contractual relationship with the registrant. Several gTLD registrars are as well, but we've identified that there are a number of registrars that do not do this. We are seeking to raise the floor. To do one domain at a time is no longer going to be enough in the gTLD space once this policy is implemented. Nick, over to you.

NICK WENBAN-SMITH Thanks, Brian. And I should say, actually, my mother-in-law was a recipient of a text message saying that she needed to go to this lookalike website, which looks exactly like an official UK government website. It's directed through a gTLD, a .qpon, which

I'd never heard of before. So, she said, oh, look, I've got this text message. It's a real scam. This is what you do for work. I said, yes, it is. So, let me take a look at that one. And it's with the registrar that Brian referenced.

That domain name, I did look at it because I was sort of interested in it. It was up and it had been registered for at least six weeks. So, no mitigation action had been taken at any sort of pace. And that's exactly right. That registrar should, as a result of this PDP, change its business practices so that those 2,000 domains are all mitigated immediately on receipt of one abuse report, not have to insist on receiving 2,000 abuse reports before actioning them. They should change that behavior or go out of business is the objective of this policy. We'll see. We'll get there.

So, going to the second slide we have on this PDP. What's nice about the ccTLD world is we are simple folk and we do things straightforwardly without very complicated machinery. And we also have a very, I think, collegiate spirit, largely because we do not compete with each other. Okay. And by contrast, we have the GNSO procedures, which I have to say they would make CAFCA proud.

So, we have a charter. It is pretty complicated. We have 28 community participants plus another 14 alternates plus another 14 members. So, it's already, as you can tell, I think with decision making and discussion, the larger the group of people, exponentially longer and more complicated the whole process is.

And instead of, I think Brian set out the problem statement very simply in his slide, but no, we have to have nine charter questions to help us through this process. So, that's interesting. And well, I mean, this is the straight narrow scope one, right? So, you can imagine what the more complicated ones look like. And I can understand now why it's a bit like some of the long battles of the first world war, sort of perpetual trench warfare for years and years.

But I have to say that my experience has been extremely positive with this particular PDP. It's been extremely collegiate. We have a very clear charter, which is specific to this. When it comes to DNS abuse, there are lots of really interesting areas for discussion. It is a complicated area. Lots of people are very passionate about it. There are many different avenues. It's very dynamic. We know we had the session in, I want to say Prague on AI tools. There's a lot of things going on in the macroeconomic and policy area. So, lots of interesting discussions.

And from the leadership of the PDP, I'm the vice chair of the PDP, Paul McGrady is the chair, these are great topics for discussion in a different room from here. We need to stick to our mandate and get through these questions quickly. And I described it this morning as a Navy SEALs mission. So, we have a limited objective. We have a strong focused team of people. We go in quickly, we achieve the objective, and then we retreat quickly and then go on and do something else. So, that's how we intended to operate. And I have to say, it is going well.

So, we started more or less in the Mumbai meeting, and that's not so long ago. We have basically, I'm probably going to jinx it now, but we've basically done it. We've been through all the charter questions. We've got language for all of the policy proposals. We have not completed the Seville meetings. We have one more meeting tomorrow. And there are four areas where different community participants have outstanding, we cannot live with this in the proposed recommendation wording. And I think we will settle those tomorrow. Again, not wishing to jinx the meeting tomorrow.

And then we are going to instruct the staff to populate the report template with the outcomes of this meeting. That will then be reviewed in two weeks' time. This is like world speed records being achieved here. The timeline for the report to be presented to the GNSO Council is February 2027. That is already four months shorter than the initial timeline. That's less than a year from initiation in Mumbai.

I've already spoken to our board liaison and to the GNSO leadership to potentially expect that report sooner than that timeline. Because we seem to be, there's a lot of convergence and a lot of willingness to solve this problem, as Brian explained. It's a live problem. There are solutions already out there. We want to raise the standards and we want to do it quickly. There is obviously a number of consultation processes prior to adoption. So this is not

going to be a very quick process, but it's going to be a relatively quick process.

I think the final point I'd say is that I've been asked a number of times, this is all very interesting for gTLDs, but what is the relevance of this to ccTLDs? That's a fair question. Why am I spending my time in the GNSO room? Why am I spending my time? So it's a fair question. But I refer you to firstly the contract amendments which require registrars to act on evidence of DNS abuse when it's reported to them.

As you can see from the DASC sessions which I chair for the ccNSO, many ccTLDs are now incorporating that exact same language into their registrar agreements. So we can converge on standards which are sensible and help the industry collectively combat DNS abuse, make it easier for our registrars. Our registrars obviously probably sell both. The large registrars will be ICANN accredited as well as ccTLD accredited. So let's make life easier for them. Let's reduce friction. Let's allow them to use the same processes for their ccTLD abuse mitigation as well as their gTLD abuse mitigation, reduce cost, increase efficiency. Those are all I think desirable objectives.

So it's been interesting. Well, in the UK we do this associated domain check. It's kind of obvious that if you receive one abuse report we look for evidence of other abuse associated with it and mitigate it at the same time. So I wasn't really aware that there are some registrars who absolutely refuse to do this and refuse to

cooperate. So if we can fix that, then that's useful. I'm very happy to give the perspectives from how we manage our registrar channel. We have a big compliance team. We deal with complaints and abuse, same as everybody else.

And I think it's something real because as I described my mother-in-law in the United Kingdom and a lot of United Kingdom people are relatively wealthy, not particularly tech savvy. There are vulnerable communities who are obvious targets for these phishing campaigns. So actually it's good for my community even if it's not directly related to the work of the ccTLD.

So that's my sort of perspectives on that. I don't know whether if anybody's got any questions or interest in the PDP. They're very free. We have got time and we're running a little ahead of schedule I think still.

BRIAN CIMBOLIC

Can I just note briefly and Keith Drezig put this in the chat. I wanted to thank the ccNSO for sending representatives and their participation. Nick, Eberhard, Bruce, we've gotten great contributions from you and Nick has very ably vice-chaired the entire PDP and the work of he and Paul McGrady as chair is I think attributable for a lot of the reason why we're so far ahead of schedule. So thank you very much Nick, Eberhard and Bruce for your participation.

NICK WENBAN-SMITH

Thank you, and I think the final close I was going to say is that I see this as a challenge for the legitimacy of the whole multi-stakeholder process because part of the problem about the GNSO policy development is it's been so slow and I think when the European Commission can legislate on personal data privacy in half the time that the ICANN PDP could not achieve anything and that's not a good look for the ICANN community in the multi-stakeholder model.

So I think we all need to lean in and make that appear to work a bit more efficiently and effectively. So that's partly a part of my motivation for volunteering for that. I haven't followed the Zoom chat. We're good. Any questions in the room? Any concerns? Any thoughts?

ASHISH AGARWAL

Yeah, I have a question. Yeah, I am Ashish Agarwal, for the record. You spoke about the action domain registrar is supposed to take vis-a-vis the domain owner, the rogue domain owner. Are we doing anything new as far as the background check of a domain owner is concerned? Like the due diligence, are we using some AI tools in order to do a background check as a preventive measure?

NICK WENBAN-SMITH

Thank you for the question. So the existing obligations on the gTLD registrars is when they and the requirement to mitigate could come in from a number of different sources. It could come in from a

complaint from an intelligence reporter. It could be because the registries subscribe to intelligence feeds from providers, some of which are free. It could be the registry's own vigilant systems pick this up. If they have actionable evidence, then they are required to mitigate it.

What we're talking about in this PDP is that now they are obliged to look for associations to other domain names which were not specifically complained about because normally in a big phishing campaign, like we heard the description of 2000 with one registrar, sometimes they're an isolated instance of one single abusive registration, in which case you check. There's no other domains associated with it. That's the end of it. But sometimes there's thousands, hundreds of hundreds or thousands of domains obviously in the same pattern.

Now when it comes to association and one of the charter questions, these nine charter questions is what does association mean? We didn't want to be prescriptive as to what that looks like. It could be the same account. It could be the same pattern in terms of the text in the domain name. It could be a specific, say, government department or retail brand, which is the target. You can tell that the domain names are all in the same sort of pattern with a string, some random text, a -.uk, more random text .tld. You can see them. They could all be associated by the time of registration.

So you look at a pattern for the registration time. That's interesting. That registrar normally does a thousand new creates

over the course of a year. Oh, they had a thousand in one day yesterday. Let's have a look and see whether there's anything suspicious about them. There's various indicators that could lead to association. Association doesn't mean they're guilty. It just means that there's a curiosity to look at that account to see whether there are having received one confirmed abusive registration. Let's have a look, see whether there are any other ones in that same pattern or account.

We've not been prescriptive about what association means. It's going to vary from registrar to registrar. There's lots of different registrar models. Obviously, registrars are based around the world. There's different jurisdictions, there's different languages, there's different cultural distinctions as we in this room understand very well.

So AI has come up. Many of us already use some sort of machine learning in terms of the registry intelligence. I know that threat researchers are also starting to use AI increasingly because it's something that can tackle large amounts of data very quickly, can do things which manually take a lot of time, can really accelerate it. Obviously, on the counter side, the threat actors are also using AI to work out which are good domain names to register to carry out phishing campaigns. So it's a sort of an arms race of technology like always. So thanks for the question and I hope that was a useful explanation of how we're doing.

ASHISH AGARWAL Very much. Thank you.

NICK WENBAN-SMITH Thank you. Are there any other questions? Oh, Eberhard. So Eberhard, and then the lady there.

EBERHARD LISSE Eberhard Lisse, I'm one of those poor folks having been nominated or having been volunteered to that group. Just to come back, the registrars under the registrar agreement, the gTLD registrars are not obliged to do any background checks. For business practice, of course, they don't want to have fraudulent credit card payments that get charged back and so on. So there is some form of legitimate or registration data that passes muster.

The point here is that if you now complain about a farming or phishing domain name, the registrar should investigate it and if found to be reasonably actionable, it should take it down. There are a number of registrars who don't do this and ICANN compliance is sort of running behind the ball because there is too many, but when they get somebody, they get somebody and the registrars that are represented are sort of the good boys and they all say that compliance has their ways and means.

The problem is now to find what's a trigger. A trigger is at the moment a validated complaint having taken the domain down. Then we want the registrars to start looking, are there patterns that are efficiently manageable to figure out whether this same entity

has registered similar domain names or domain names for a similar purpose.

As I made this example, I had recently a farming site where I was asked to pay a speeding ticket and what made me suspicious was that the amount was too low. In Namibia, the amount is usually 100 Euro and it was something like 2 Euro and I said that can't be. So then I looked and then I found it was nampul.gafna.top. That's now an abusive domain that should be taken down. It has not been taken down.

I'm talking to compliance because I want to know how compliance works. However, if it's taken down, then the registrar under the new policy would be obliged to look if there is gafbw something.top, gafgouvfl.something.top, gopblsomething.top registered from an entity likely to be the same credit card, IP address, whatnot. And if you find those, they must be taken down.

The big problem I see at the moment and I don't find a way around this is, well, then they go to another registrar. There are many registrars. If one takes them down, they probably not register the same names, but they go with a new batch to different registrars. How we go around that is not there. But again, whether a ccTLD does background check, like in Ireland, you must show that you have a connection to Ireland. In Denmark, you must show, I think, your population ID. In Namibia, we have different pricing models for Namibians and for us.

Point here is, every ccTLD can have their own way of doing it. If in your ccTLD you want to do background checks, do them. By whatever means you want, put it in your agreement. If they don't want to register, they can go to .top or to .coupon.

NICK WENBAN-SMITH Thank you, Eberhard. And I can't be rude about gTLDs with my gTLD friends in the room, obviously. But we all know that ccTLDs are better, obviously. Thank you for that. And one more question. Introduce yourself, please, for the record.

FATMA DEMIREL Okay. There are two sides for mitigation payout, detecting and taking action. I wonder your perspective about the balance between registrar and registry in that roles, because as the ccTLDs, it's a bit different for us to give all responsibility to the registrars because, as you know, and what do you think about the balance of between registrar and registrars to give responsibilities?

NICK WENBAN-SMITH Great. And thank you. Could I have your name and affiliation for the record?

FATMA DEMIREL This is Fatma from Turkey.

NICK WENBAN-SMITH

Thank you very much. Thank you, Fatma. It's a great question. So, one of the things I'm very interested in is the whole ecosystem, like with the point about registrar to registrar hopping to avoid detection. Similarly, between the different registry and registrar, the different contracted parties in the gTLD space or with the CCs, who should be the accountable party or is it both people's responsibility? Is it clear that it should be the registrar? Is it clear that it should be the registry?

As registries, we are the responsible custodians for our safe operation for the ccTLDs. But is it actually better if through the contractual mechanisms we have with our registrars that we push it to the registrar level because they are the people who, for example, have the closest relationship with the end registrants in terms of the payments and the accounts.

And of course, we will see as the ccTLD abuse move from one registrar, they see they're being attacked, then they move to a different registrar. We can pass that intelligence on to our registrar community. But what the registrars see is the different TLDs. So, they say, oh, we have some .uk domains, but now they have .top ones or .coupon ones or .org ones, and they can pass that intelligence to us.

So, one of the things that has made this PDP successful is it's only dealing with a very specific problem of a single registrar having lots of malicious registrations. It is not within the scope that we have spent a lot of time talking about is this issue about abuse across

registrars and abuse across registries. And we have put for not our recommendations for the policy, but one of the things for future discussion is this exact point about the ecosystem, how we can better collaborate between registrars and between registries and registrars and between registries and registries and start to have those sort of conversations.

And that doesn't need actual policy development. It's through things like the DNS Abuse Standing Committee. It's the gTLDs Committee on DNS Abuse. It's the registrars. This afternoon, we're having a session talking with registrars about this exact topic. How can we more effectively work together? That doesn't need a policy development process. That can happen organically because community sees that it's needed, and we can have those discussions in forums like that and try to solve some of those problems.

But to answer your question, I suppose, coming back to the question, it's not for me to tell you in Tokyo how to solve that. That's for your national community, your national framework and legal jurisdiction to decide what's appropriate for you with your registration model. How we do it in the UK is interesting, and I'm happy to talk about it. So, we cross-fertilize good ideas. But ultimately, you guys need to make those sort of decisions for yourselves. It's going to be different in different places.

For example, I know some ccTLDs don't use registrars at all. So, you need to be quite careful about having blanket sort of

recommendations or best practices. It's going to vary from place to place, and it depends. I don't know how many registrars you have, whether they're also ICANN-accredited, or there are lots of different factors which will go into that assessment.

BRIAN CIMBOLIC

Thank you very much. This is Brian Cimbolic with PIR. And so, this is not necessarily a gTLD-wide perspective, but just PIR. We've kind of shifted our thinking a little bit as far as how we would deal with the question on responsibility, registry or registrar, where if a domain was confirmed to be phishing, previously, a few years ago, we would send the referral to the registrar, ask it to take action, and varying levels of success, if the registrar didn't suspend the domain, we would.

The issue with that, though, is that we're basically leaving a phishing domain up for two days. If we give them 48 hours, that's 48 hours that the domain resolves. That's 48 hours that we could be creating new victims. So, in clear cases of things like phishing, we will step in ourselves, directly suspend the name, and then tell the registrar. I think it's more appropriate from where we sit, response to clear phishing, rather than letting the content resolve until the registrar does it itself or doesn't, and then we step in sometime later.

NICK WENBAN-SMITH Thanks, Brian. And that's quite common. We're going to move through the slides now, because apparently, from -- oh, just a quick one from Eberhard.

EBERHARD LISSE There are different types of registries in the G space, and also, of course, in the CC space. On a SYN registry, the registry operator doesn't have all the information, and that's why we're targeting the registrars. If Turkey has a SIG registry, they have the information. If Botswana has a small one without, has a SYN one, then they have to target the registrars. That's why the reason why one of some of the big registrars, like Tucows, they are represented, and they said they don't have certain information. So, that's why we are targeting the registrars.

NICK WENBAN-SMITH Great. Thank you. So, just moving quickly forward to the last couple of speaking points in the session, I'm just going to give a promotional notice for the DASC, the ccNSO's DNS Abuse Standing Committee, and there's a session later where we are having, as I referred to, having successfully had some gTLD registrar, ccTLD interaction. We're now going to go further to the dark side and talk to some gTLD registrars and talk to them about their, what they like about ccTLDs and the pain points in mitigating abuse. That's this afternoon. I'll go more slowly for the interpreters. Too little, too late. I'm sorry.

So, just an advance notice that every two years, the DASC does a global survey of the ccTLDs and their practices around DNS abuse. The first one was in 2022. The second one was in 2024. The more observant of you will notice that it's 2026. So, it's time for the third survey. We've learned from the previous surveys, the draft questions are going to be circulated and they have been circulated if you look on the ccNSO mailing lists for comment and feedback so that people can read the questions well in advance as a preview now.

And I'm giving you advance notice of the survey period, 17th of August to the 20th of September. It's through the SurveyMonkey platform. It'll be well distributed and advertised. It'll be brilliant if we can get as much participation as previous surveys, which have been very well responded to, if that's the right word. And then, obviously, the results will be presented back to the community. It'll be interesting. And we have actually a specific question on AI adoption on that one. So, that's going forward.

These are some additional slides about the PDP, but that's just for the record. I've been told to shut up.

KEITH DRAZEK

Hi, everybody. I'm Keith Drazek. I'm the interim Registry Stakeholder Group Chair, just for the next five months. But I thought I might offer some comments to tie some of the threads together that we've just discussed.

I think Jordan asked earlier in our Internet Governance discussions and the GNSO about how we are achieving efficiency and effectiveness in our policy development work. And one of the response that was given, I'd like to reinforce, is very narrowly targeted and chartered policy development working groups.

So important for us, we've realized and recognized, and we're implementing this, is to make sure that the work of our PDPs is narrowly tailored and focused and chartered accordingly. As such, this PDP on associated domain checks is quite narrow. It does not address nearly all of the topics that could be considered under DNS abuse mitigation. And as such, this is just the first of many PDPs to come.

So, in the GNSO parlance, we had an issues report that listed out three priorities, the ADC, the associated domain check, being the first. The second is going to be focusing on registrars' use of technology and automation APIs, sort of touching on the concept of bulk registrations. So, how do we require registrars to introduce some friction in the registration process to ensure that high volume registrations, creation of accounts, creation of domain names in an automated way aren't contributing to DNS abuse?

A third topic, and I want to call this out very clearly for the ccTLD managers, is a focus more on registry engagement and specifically on domain generating algorithms. And how do we, as registries working with other parties, identify and mitigate the use of DGAs to prevent their use in creating abusive campaigns? You know, I think

Avalanche is an example of that. Configure was another for those who are familiar with the history. So, that is an upcoming bit of work. It may be a policy development process. It may be some other approach, but there is a clear intent to do that.

And then there's a list of about six to eight other potential topics for future policy work that are under consideration and under discussion. So, I just wanted to reinforce that this is just the beginning in the GNSO context. And we very much appreciate the engagement of the ccTLD registries in this work because so much of what we do certainly at the registry level are related. We can learn a lot from one another. And Nick, again, really appreciate your engagement as a vice chair in this group. It's going so well that we may have to have you back for the future work.

ALEJANDRA REYNOSO: Thank you, Keith. Just quick question. Eberhard, you have your hand up on Zoom? Is that an old one? Okay, checking. It's an old one. Kind reminder to speakers, just please speak slowly. Take a deep breath. Now we can proceed with root server system governance. For that, I'm giving the floor to Peter or Sam.

SAMANTHA DEMETRIOU: Hi, everyone. Thank you, Alejandra. I'm Samantha Demetriou. I work with VeriSign, and we are a member of the Registry Stakeholder Group. I also serve on the GNSO Council representing the Registry Stakeholder Group. We're going to be co-presenting

with Peter, but I wanted to tee up this topic for our discussion today.

We're going to give a bit of an overview on the current state of play in the topic of root server system governance and also hopefully open a conversation between the Registry Stakeholder Group members and the ccNSO members about why this is a topic that is pretty impactful to us and start to share some ideas about our potential respective and collaborative engagement with this.

So to set the scene, I'm going to start with some really basic facts that I'm sure are going to be very familiar to most of you in this room, but I think they provide really good grounding for what we're going to discuss in the course of this brief presentation. So the root server system. What is this? It is comprised of 13 root servers, which are the authoritative servers for the root zone. And as we all know, the root zone is the very highest level of the DNS hierarchy, and all TLDs must be delegated into the root zone to be part of the DNS, gTLDs, ccTLDs alike.

We all as registry operators have a strong vested interest in the continued stable and reliable operation of the RSS, root server system, because we rely on that system. And historically, the root server system has been completely self-governing. The root server operators themselves, they work together to ensure the continued availability of the system, but there's no overarching structure that brings them together.

This history kind of actually goes back even beyond what we see on the slide here, really to the time of the IANA transition. When the broader ICANN community was having conversations about the importance of accountability and ICANN being accountable to the multi-stakeholder community, the root server system advisory committee, the RSSAC , began to reflect on the question of who is holding root server operators accountable, and for what are they being held accountable? Should they be held accountable?

That eventually led the RSSAC to propose a governance model for the root server system, which is captured in a document titled RSSAC037, very compelling title, easy to remember, that was shared with the board as an advisory in 2018. This was also accompanied by a sister document, RSSAC038, that provided some formal recommendations that the ICANN Board implement the model proposed by the RSSAC .

As it deliberated over the recommendations, the ICANN Board eventually directed the creation of a governance working group, a GWG. The mandate of that working group was to develop a final model to inform the board's consideration of the RSSAC037 document and determine the next steps in the evolution of RSS governance.

This working group was open not only to members from the root server operators themselves, but also to participants from the Registry Stakeholder Groups, so representatives of gTLD operators, representatives from the ccNSO to represent ccTLD operators, and

other liaisons from other parts of the ICANN community who are similarly situated as stakeholders of the RSS.

In the course of the GWG's work, they developed both success criteria for the future governance system, as well as principles that grounded the development of that governance system, which are all documented in additional RSSAC documents. And then earlier this year, the GWG published its deliverable, which is titled the Functional Model for Root Server System Governance, that captures you know, what kind of system should be implemented.

And with that, I'm going to turn the floor to Peter, because as a representative on the GWG, he's going to go into some of the details about what the system looks like. Peter.

PETER KOCH

Yeah, thank you, Sam. My name is Peter Koch. I work for DENIC, so the DE ccTLD registry. I am also a member of the ccNSO Council. And as Sam just said, I was also one of two ccTLD representatives or appointees, I should say, on the governance working group. But of course, as usual, I will not speak for the council, and I will also not be speaking for the governance working group. The other CC representative is Luis over there. And we had Kurt from the Gs.

So I'm now going to try to present a bit of the results or the gist of the results of the working group, focusing on what that means for the two constituencies in this room. Well, first of all, if we look at the headline, the RSSAC037 was the input generated by the Root

Server System Advisory Committee. And as Sam just said, that's comprised of the root server operators themselves and other parts of the community. There's this other document, RSSAC58, which was the RSSAC generated set of success criteria for the governance working group. And then there is the functional model, which is the output or one of the outputs of the governance working group.

Maybe taking a step back. So this RSSGWG, the Root Server System Governance Working group, had a meta-task. The task was to suggest a governance structure to solve a number of problems that we have at the end in the Mentimeter, actually. But not to solve these questions by itself. And these questions would consist of questions like, okay, so how to deal with a potential retirement of a root server operator, or how to deal with a non-functioning root server operator, or how to add a root server operator to the system.

Again, the GWG had the task to define a structure that would then take up the solution to these questions whenever those arise. The GWG had actually two versions of that. So it was restarted in between. And I must admit, I joined the group in the middle of that. So that was a two-year appointment for a, in the end, four-year ride. And it consisted of the root server operators, the Cs and Gs, and the liaisons, as Sam already said. And it's also reflected here in the council, but there were also representatives from SOs and ACs in there.

Well, the RSSAC was already represented because all the root server operators have been sitting at the table. And that's

important. So all the root ops had a seat at that GWG. And while there are 13 letters, we all know that very sign is running ANJ. So there is 12 root server operators. And that magic number is reappearing again. So keep that in mind.

Now, the output then is the layout of this governance structure. And that governance structure is supposed to reflect and support the identified stakeholders. Now, in the course of the working group, we've been looking at who the stakeholders might be. And one of the key terms was participating stakeholder group. Obviously, the TLD registries, both the Cs and the Gs, have what we called the direct operational dependency on the root name server system, because it's our delegations that are within the root zone. That definition would also cover another entity that is currently not reflected here because resolver operators also do have a direct operational dependency on the root server system.

However, another criterion was that this participating stakeholder group would have to be organized. It would have to be organized not necessarily within the ICANN system, but anywhere. Given that we have a ccNSO and an RySG in the GNSO, the Cs and the Gs obviously seemed organized to meet that criterion. Currently, there is no such organization that we could identify or that would have come forward for the resolver operators. Thus, the resolver operators aren't represented in this initial model. There is still a way for them to get in there.

And here comes the beauty of the number 12. The government's model here foresees that there will be 12 root server operators. Again, they are not represented. They are all at the table, whereas the other constituencies of participating stakeholder groups, the Cs and the Gs, to be represented by six each. Should the composition change, like should there be three groups, then there would still be 12 operators and the three groups could be represented by four people each. And we could even have four groups and then three again. That's the niceness of the 12.

But the key message here is there was no other way to come up with a solution for the governance working group than to have every root server operator at the table. Should the number change, the mathematics could be interesting, but that was not a task to decide for the GWG. That is handed over for the governance structure to deal with in the future whenever the problem arises. So, keep that in mind as well. Can we go back? Maybe? I don't like to press red buttons. Here we are. Yes.

So, these 24 heads will comprise the root server system governance structure council. And that means that collectively the Cs and the Gs have to find 12 people with the qualification, time, energy and whatever criteria we come up with in addition to join this group. And as you see, it is designed by numbers to balance the so-called voting power, which is my term and you don't find it in the documents. So, that's basically it.

And then there are liaisons, obviously, from IANA and the root zone manager, currently Verisign. So, IANA as the responsible party for maintaining the root zone and the root zone maintainer actually doing the technical maintenance, like putting the entries in the root zone and distributing it to the root server operators. And then there will be the one representative from the IETF/IAB as the responsible party on the protocol side in terms of the DNS.

So, what are these 24 people going to do? First of all, they need to bootstrap the organization because there's a number of tasks that the governance working group framed and is now handing over to the structure because that structure will have the better proximity to the questions to solve. They are tasked with solving these questions and we framed that as functions.

So, it says committees/functions on the slide and the reason behind that is that the governance working group identified certain roles or functions that need to be solved but did not want to prescribe what internal structure that governance system should have. So, it could have very different committees. It could be that one or more functions are assumed by the council itself. This is all up to the council to decide.

Let's look at the functions. There will be a secretariat function which is kind of basic. Strategy, architecture and policy function. Forward-looking policy function means the policy making for questions like accountability and technical details. Finance and resource management obviously a clerical function internally and

then one of the politically very sensitive and important but also technically important function designation and removal because there's no such rule for now. There is no procedure in place for removing a root server operator or for adding one or for picking one of many candidates should the need arise to either replace the previous one or should the need arise to add one to the one or more to the system.

And then performance monitoring and evaluation. Actually, there is RSSAC002 for example. That's a document that describes certain parameters that the root server operators have voluntarily agreed to regularly publish and collect and you can go to the appropriate website. The URL escapes me at the moment to find that information so they will share information about the query numbers and UDP versus TCP. That's all interesting information first of all for accountability reporting but also for researchers and for future both capacity planning but also planning that would address technology changes. Think of adding something like DNSSEC to the root zone something at that level so you need certain current and historic data how the overall system works.

And then, of course, also very important and asked for by regulators and governments security incident reporting would be a function that would phrase that and frame that and develop the framework for thresholds and collecting and publishing that information. And again the secretariat to provide the clerical support. Any questions so far?

Okay, the whole report is available. It goes into all the details you want and more probably and you can have a look at that. The status of this report is that the GWG delivered. It's in front of the Board and the Board now has to decide how to proceed and if it follows the recommendation then it will convene the constitution of the governance structure and especially the Council that we've been talking about which would then likely lead to the invitation to both the GNSO and the ccNSO to seat these six plus six people, and that's a discussion that then the both councils or the RySG respectively will have. And I think with that we go back to Sam, right? We covered that, yes.

SAMANTHA DEMETRIOU Thanks, Peter. So Peter teed this up very nicely that the GWG has delivered on its remit which was to provide the model. It does not resolve every governance question related to the root server system because the governance structure should answer those. So this is a kind of brief overview of some of the things related to the broader aspects of RSS governance that have been settled with the publication of this document and what kinds of things still need to be resolved.

And this is one of the ways in which we now enter the picture, our collective groups, right? Because as Peter mentioned, once this gets stood up, we are to appoint six representatives a piece, so a total of 12, to do the work of starting to operationalize the governance and go take it from its establishment into

implementation and then finally into a self-sustaining governance structure.

I think the more exciting ones to focus on are certain things very concretely like what should a connection be between the future governance structure and ICANN? Should there be one? Should it be a new stakeholder group? Sorry, not stakeholder group. Should it be a supporting organization? Should it be an advisory committee? Obviously details around the formation of committees have to be worked out.

There's still open questions about financing both for the governance system itself but also potentially for root server operators to be resolved and then also the big one, right? The biggest one as it pertains to the broader topic of accountability is criteria for RSOs in operating root servers, and then also for how root server operators could be potentially added to the system or removed from the system for whatever reasons that may arise.

So does anyone have any questions before we…? Yeah, go ahead, Olga.

OLGA CAVALLI

Thank you very much, Samantha and Peter. Very interesting presentation. This is Olga Cavalli from the ccNSO, a NomCom appointee. This decision about the connection between governance structure and ICANN, where are these decisions to be made? You're presenting a document to the Board, but for what

you have explained, it doesn't seem to be just an ICANN issue? Should be inside ICANN or how this decision should be made or where are they going to be made? And thank you.

SAMANTHA DEMETRIOU I think I can take a first crack and Peter please jump in if I get anything wrong here. I think the big question is because historically the root server operators have always been independent in the sense that that they were doing the operations and they kind of just loosely come together, right? So it will be the task of the future governance system, I think, to weigh in on this decision. But I also think there's potentially a role for ICANN and the ICANN community to play in weighing in on what we see as the preferable outcome of that question.

PETER KOCH Yeah, this is Peter. Maybe I can add. Obviously the question was discussed in the governance working group but the governance working group could not come to a single conclusion which might be informative of what the elephant in the room is. Now when the Board makes a decision then obviously there would be a community consultation, whatever the Board rules are, but at some point the governance structure needs to be seated and seated and that means some maybe preliminary decision would have to be taken by then because otherwise you can't have a committee.

	One suggestion was to follow the PDI model and as Sam said, the other could be some structure within ICANN or something completely outside and then the pros and the cons would have to be discussed. And as a CCs we have this independence in us, right, collectively even. That's one of the tough questions for the Board to chew on and nothing is cast in stone here but it's very important for the bootstrapping to work that there is at least a preliminary decision made otherwise it will all be in the void of course. But thanks for asking that question, very important.
ALEJANDRA REYNOSO	Jordan.
JORDAN CARTER	Jordan Carter .uk; you may be about to cover this, but are you going to tell us exactly where this process is at now and if we need to do anything now?
SAMANTHA DEMETRIOU	Yes, so where this is at now is it's sitting with the Board to make a determination of what to do next on this. Until the Board makes a decision there isn't a formal requirement of us at this point, although I think including on the topic of the question Olga just raised, like what should the connection be, I think to the extent that we as registry operators collectively have a view on that it might be interesting to consider providing some input to the Board on that. I'm throwing this out there just as purely hypothetical. It's

something we could explore but there right now isn't an urgent role for us to play.

PETER KOCH

Thanks. Peter here, and let me maybe add that everything that Sam said was absolutely correct. There is no urgency but there are some foreseeable questions, one of which is in addition to the like the legal structure or not of whatever the committees are, sorry, whatever the governance structure and the Council is, without wasting too much energy on making calls for appointees but thinking about how to find and support the 12 appointees that will potentially be invited and do that, and also develop a maybe shared opinion on the questions on the table and do that informally. Maybe also going back to our respective submissions in the comment period. Does that answer the question, Jordan? Okay, thank you.

SAMANTHA DEMETRIOU

Any other questions? Checking the Zoom room. Okay, so we do have a poll to help kind of juice some discussion, get us going, and that question is what is the most important governance issue that the future RSS governance structure should resolve? Is that evaluating root server operator performance, the criteria for adding or removing a root server, financing of root server operations, security incident reporting, other, something we haven't thought about yet, or you don't care. I've put you to sleep

and you just want to go to lunch. We'll give it a minute for Mentimeter to catch up.

And while folks are weighing in and filling in their response here to kind of go back to Jordan's question about what's in front of us at this moment, I think one of the things I would like to encourage our two groups to think about in the short term, not necessarily the immediate term, but the short term, maybe for the next year or so, is starting some regular collaboration between our groups on this topic.

Perhaps if there are dedicated, like a dedicated group, almost like sub-interest groups who want to keep talking about this and keep track of how the governance system is working its way through the board consideration and all that, and really just getting ourselves prepared not only for the future participation potentially in the council, but if there are topics that we have strong opinions on, coming together with one voice to be able to provide input.

All right. Looks like we're kind of leveling off in the responses. I will say I am not surprised that the leading response is the criteria for adding or removing a root server operator. I think that is maybe the pinnacle of accountability as we understand it, right? But if folks replied with something different or have a different view, I'd love to hear from you if you're interested in weighing in. Olga?

OLGA CAVALLI Thank you, Samantha. I think that I'm confident of people running the root server, so I think that they should be technically skilled to care for the security and for know-how to adding or removing a root server. So I think the financial root server operator should be the most important, because I have been following this issue for a time, and I think that's a critical situation. Thank you.

SAMANTHA DEMETRIOU Thanks, Olga. Anyone else want to opine? Right behind Olga?

IRINA DANELIA This is Irina. I'm on the first one, because I would say that evaluating root server performance and the entire system performance gives actually a big indicator whether there is a need to add a root server or whether there is a need to remove one. So it's like basic measurements to decide on next step.

SAMANTHA DEMETRIOU Yeah, very good point. Those are very closely tied. Yeah, I was going to say, I think we only have about four minutes left, so I'll do one last call if anyone else wants to jump in or ask a question. All right, I'm not seeing anyone. So the last thing I want to do before I hand it back to Alejandra is just thank Kurt Pritz. He was, as Peter mentioned, one of the two Registry Stakeholder Group representatives to the GWG, and he couldn't be here in person, but he was very helpful in putting this presentation together and

making sure we were hitting on all the right points. So thank you to Kurt. Ale, back to you.

ALEJANDRA REYNOSO

Thank you, Sam and Peter. Now we have some future work to think about. It's already in our work plan, if you remember, on our upcoming activities. Thank you to all our panelists on the topics that we discussed today. We went through the internet governance, DNS abuse, and now the root server governance. We believe that this interaction between all registries, the Gs and the Cs, it's a good thing to move forward, but please do fill this survey now for us to know if this is a good idea. We should continue doing this. We are planning on having maybe a one-off session each ICANN meeting so we can get together and discuss topics of importance.

So with that, please give a hand to our presenters. They were very kind to share with us their thoughts. Thank you. And with that, we will reconvene after lunch here for a second ccTLD news session, and this session is adjourned. Thank you. Oh, Keith, please.

KEITH DRAZEK

Thank you. Sorry, just wanted to say we, the gTLD registries, very much value these sessions. So thank you for inviting us in, and we look forward to doing it again on a regular basis. They're really good, and we very much appreciate your engagement. Thanks.

[END OF TRANSCRIPTION]