ICANN86 Seville | PF – GAC Discussion on Registration Data Issues and Informational Session on Accuracy of Registration Data
Tuesday, June 09, 2026 – 11:45 to 13:15 CEST

JULIA CHARVOLEN

Welcome to the ICANN86 GAC session on Registration Data on Tuesday 9 June at 11:45 local time. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior, ICANN Community Participant Code of Conduct, and the ICANN Community Anti-Harassment Policy.

Please remember to state your name and the language you will speak in case you will be speaking a language other than English. Speak clearly at a reasonable pace to allow for accurate into interpretation and please make sure to mute all of the devices when speaking. With that, I will leave the floor to GAC Chair, Nico Caballero. Nico, over to you.

NICOLAS CABALLERO

Thank you very much, Julia. Welcome back, everyone. Welcome to the session on registration data issues, our discussion on registration data issues. We have a fantastic lineup of speakers. We have two guest speakers today. We have Eleeza Agopian from ICANN Org to my left. We are having Justine instead of Marc Anderson, correct me if I'm wrong. I'm sorry, Marc is here, I'm sorry. Yeah, thank you.

We have Marc and Justine to my right. And from the GAC we have David Bedard from Canada, Gabe Andrews from the U.S., and Owen Fletcher from the U.S. delegation as well. This session is going to be running, as you know already, for 45 minutes, and then we'll move on to our next session. So, without further ado, let me handle the floor at this point to David for the opening remarks. Please go ahead, David.

DAVID BEDARD

Thanks, Nico. Good to see, everybody. Thanks for engaging in the session here today. So, we just have the agenda here. So, we'll be covering the Standardized System for Access Disclosure of Registration Data, or the SSAD, Supplemental Recommendations. So, that'll be our first agenda item. Followed by a discussion on Urgent Requests for Disclosure of Registration Data. And then Privacy/Proxy Accreditation Discussions Update.

Lastly, we will touch on any GAC Seville Communiqué Considerations as they relate to registration data issues. So, next slide, please. And next slide. Great. So, I won't go in too many details since we have Marc here, he'll be going over some of the history of the SSAD process. But just a reminder for folks, during the ICANN Board meeting in Dublin, the Board made a decision to continue with the RDRS or the Registration Data Request Service for up to two years while the community continued deliberations of the system and its future.

So, this followed the release of a report by the standing committee on RDRS, as some of you might recall. It was, I believe, last August, that proposed a series of modifications to the original recommendations coming out of the SSAD process. So, the Board decided to non-adopt the 18 SSAD recommendations as a package. So, this essentially allowed the GNSO to continue further work on changes to those initial recommendations. And those changes would be informed by what was proposed in the standing committee report on the RDRS.

So, to go through these proposed changes, the GNSO Council established a Supplemental Review Team composed of members of the community. And this will include two GAC representatives, myself, David Bedard, GAC representative from Canada, and my colleague Owen Fletcher from the USA. And the goal of this will to be deliver final recommendations to the Board by February next year. So, our role here is just to really ensure that key GAC priorities are accounted for within the process.

So, especially the authentication work as we know this has been a perennial issue and particularly of importance for the GAC, especially considering the recent work on updates to the registration data policy, which introduces a 24-hour response time to urgent requests by verified law enforcement pending the work being done on the development of the authentication mechanism which we will hear I think a little bit more both from my colleague Gabe here, but also from, I believe, from the Board later today. So,

with that, I will turn it over to Marc to give us a little bit of an overview on the SSAD. Marc, over to you.

MARC ANDERSON

Thank you, David. Good afternoon, everybody. I'm Marc Anderson from Verisign, and I was selected to lead the GNSO SSAD Supplemental Recommendations team. Don't worry about the acronyms. I'll get into all those as we go through this. But I do want to give a little bit of background and history about the SSAD, what we're trying to accomplish, and what our goals are.

The SSAD, or the Standardized System for Access and Disclosure of Non-Public gTLD Registration Data, was developed by a GNSO Council effort after it was identified that a large amount of registration data that had previously been public was no longer public and there was a legitimate need by requesters to have access to that data.

So, the goal of this GNSO Council effort was to establish a standardized system where requesters could go to access the data and would not have to figure out where to go. You would have a single centralized system for accessing or submitting requests to access non-public gTLD registration data. Now this was the work of a GNSO Council effort.

They produced 18 recommendations as David mentioned submitted those recommendations to the Board. The Board produced an assessment what they called an Operational Design

Assessment or an ODA, and that operational design assessment raised significant questions about the feasibility particularly financially of those 18 recommendations. And so, the GNSO Council and the ICANN Board worked together to come up with a path forward.

And the path forward that they identified was that they would initiate a pilot. They would have a two-year pilot period and they produced a pilot system called the RDRS. It's the Registration Data Request System. That pilot was optional and it was to test out the feasibility of a system and to produce lessons learned that could help inform policy development.

I think this is one of the more innovative things that we've done as an ICANN community, is we've produced a pilot to help inform policy development. So, at the end of that two-year pilot period, a standing committee produced a report that captured all the lessons learned from the Registration Data Request System, or the RDRS, and provided that report to the GNSO Council.

The GNSO Council, as David mentioned, then took that report and created a Supplemental Recommendations Team, and that team has been tasked to consider all the lessons learned from the RDRS pilot and update the 18 SSAD recommendations to produce new policy recommendations. The goal of these new policy recommendations, and maybe if we go to the next slide, please, the goal of these new policy recommendations is to produce a new

centralized system for standard access and disclosure that will meet the needs of the different communities involved.

And the different communities specifically that are implicated by this are the requesters, those people with a legitimate need to access non-public registration data, the data subjects themselves, the registrants, and the data controllers. In many cases, that's the registrars, but in some cases that may be registries. So, we're specifically tasked with considering the needs of those three specific stakeholder groups, the requesters, the data subjects, and the data controllers, and make sure we produce recommendations for a system that works for each of those groups.

This slide shows what's within scope. We're committing to producing recommendations that in addition to meeting the needs of the three different groups involved are implementable. One of the things we learned from the initial SSAD recommendations is we have to take into account is it cost-effective. So, we'll be working with ICANN Staff very closely to make sure our recommendations are implementable, are cost-effective, and meet the needs of the broader community.

We'll make sure they're Board ready. And we take into account all the lessons learned from the RDRS pilot and the Standing Committee's report. We have some nice bullets here on what's out of scope. We're not starting from scratch. We have lessons learned and recommendations from the RDRS pilot which give us a really good starting.

We're working on modifying the 18 SSAD recommendations, not scrapping them altogether, not starting over from scratch, really taking advantage of the lessons learned, the pilot that we ran, and producing new or updated recommendations that meet the needs of the community and the three stakeholder groups I've articulated. Let me go to the next slide, please. This is a high-level timeline. David mentioned that we're hoping to finish our work by February 2027.

This is a pretty aggressive timeline, but one that we're committed to meeting. And so, just looking at this timeline, we've already formed the team. We've had our kickoff meeting. Here at ICANN86, we had a day zero event. So, the SSAD supplemental recommendations team met for eight hours on Sunday. We had a facilitator provided by ICANN to help kick off our conversations, help establish consensus and common points of understanding.

And we have three additional sessions. We had one yesterday, and we have two more planned while we're here at 86. And that's been a great kickoff, the ability to have people meet face-to-face is very valuable in developing consensus, and the fact that this ICANN86 meeting in this day zero event happened to coincide with really the starting point of the Supplemental Recommendations Team has been a real advantage to us.

So, being able to get to know the team, interact face-to-face, hopefully will help us build momentum as we work towards this goal of getting recommendations to the GNSO Council by February

2027. So, I think that covers my planned material. I'm, of course, available and happy to answer questions when appropriate. Back to you, Nico.

NICOLAS CABALLERO Thank you so much, Marc. Indeed, we will take questions right at the end. And thank you again, Marc. At this point, let me give the floor to Gabe Andrews from the U.S. Government. Gabriel, over to you.

GABRIEL ANDREWS Thank you. This is Gabriel for the record. And can we advance to the next? I'm going to be talking about Urgent Requests for Disclosure of Registration Data and the law enforcement authentication work that we're working on. Waiting for the slide to settle a little bit here. I'm not sure what it is we're looking at. Okay, so background on urgent requests.

We just talked about the mechanism that people can make requests for registration data through for a specific category of requests that are involved when there's a threat to life or a threat of serious physical injury, or a threat to critical infrastructure, or a threat of child endangerment. These are what we're categorizing as urgent requests in the ICANN context.

And without going into too much background, this was a key part of the discussions for a long period of time. And the recent development was that policy was finally settled that when urgent

requests are made, there would be an expectation for a response requirement within 24 hours, and this is policy now that's published as of last month, and that's the new development since the last time we met.

So, this is the result of a lot of discussion and back and forth, and we're glad to have the issue settled. Let's go ahead and move on to the next slide. One of the key parts of this discussion though is that those urgent requests are predicated upon there being an authentication of who's actually asking. So, they're authenticated to urgent requests. And as Marc just alluded to, one of the key challenges that was originally contemplated with SSAD is the cost of that authentication component because it is really hard and there really aren't perfect solutions available.

And so, what the Public Safety Working Group has tried to do is in recognition of those cost challenges, try to take a step back and say, okay, rather than expecting ICANN to somehow create a system that can authenticate cops around the world everywhere, what existing or aspirational tools might help? What can we bring to the table that can assist with this? And that's the strategy that we've taken. So, go ahead and go to the next slide.

What we've identified to start with, and this is the start, this is not the end. We've identified two efforts that we thought could help here. And one is that in the United States, there's an existing law enforcement enterprise portal that somewhere between 10 and

18,000 US-based law enforcement agencies have access to, that we can use to help authenticate for US agencies.

And then I've engaged colleagues and counterparts at Interpol, like many of you have heard at the last ICANN85, we had them co-presenting on this issue, they're building something called a global digital police identifier system that will also be a portal that their member nations, 192, if memory serves, might have access to initiate requests. In this case, both of these are possible identity provider systems that any law enforcement can make a request to. The request within connect to ICANN systems, it says RDRS here, it might be called S7 in the future, sort of doesn't matter what the name is.

The key piece being that an authentication token is passed in a secure fashion. And then when a disclosure request is made, that disclosure request can be accompanied by that authentication token so that the registrars know that who they're talking to is who they think they're talking to. That's the key piece. It doesn't change any part of what they have to decide. It's just providing that confidence that they're speaking to who they think they're speaking to.

Then the responses that come back from the registrars go directly back to the law enforcement employee. Additionally, and we'll move on to the next slide here too, you may recall from discussions at the last ICANN meeting that we were also contemplating whether or not it would be helpful to share with ICANN and with the

contracted parties lists of known law enforcement agencies and the email domains that they use.

This is not to be confused with real authentication, but it is something that we've heard from folks in the contracted party space might be a useful additional data point, and I think this is still being explored based off of the feedback we got at the last ICANN session that folks do seem interested, but it is not in my mind and in the mind of my colleagues at ICANN, I think this is not the priority work. The priority work really needs to be the true authentication mechanisms.

The last thing I'll mention is that with regards to those portals, even though we're starting with maybe the Department of Justice in the US and with Interpol for its global members, we very much envision that to be the start and that other, what do we call them Marc, the DUG stand for domain user groups? Designated user groups. Other designated user groups can stand up and choose to follow this path and say, hey, maybe it's AfriPol that wants to stand up and act as a designated user group for all of its law enforcement agencies within the continent.

Maybe it's CERTs, the Computer Emergency Response Teams and Security Incident Response Teams of the world, that might not be badge and gun carrying officers, but have a very important role to play in critical infrastructure protection. The key thing is that we're trying to blaze a trail here that others can follow. Let's go ahead and move on to the next slide.

So, with all of this said, the last update that we really have is that there's been some desire by various folks in the ICANN community to have better visibility into how these conversations are proceeding, and I will accept much of the responsibility for that. I think when we were originally engaging my law enforcement counterparts, I was a little bit overly cautious about how much we're talking about how the authentication mechanisms happen, and so I erred on the side of being secure and not as open as ICANN is used to.

But I think we've really walked back from that position and we're embracing now the idea that ICANN can play a leading role in keeping the community abreast of how these authentication tests are proceeding and how we're making progress against this goal. And so, with that in mind, I have my counterpart, Eleeza Agopian, who I'm going to hand the mic over to now to talk about this.

ELEEZA AGOPIAN Thank you, Gabe. This is Eleeza Agopian from ICANN org. And actually, I want to thank Gabe for his leadership in the discussion group with the PSWG. It's really gotten us to a good place with some real models we can look at to help us take this discussion further. So, I'm going to give a little bit more background and then talk about where we are today. I think Marc did a really good job of laying out all of the work that has been done on the policy side.

But I want to take us back a little bit further. So, we had GAC advice from both ICANN79 and ICANN80, which highlighted, of course, the

critical need for the delivery of an urgent request policy. Of course, the flip side of that or the important complementary work to that is an authentication mechanism, so that if an urgent request is indeed coming from a law enforcement official, for that to be enforced, a registrar has to know that they are actually speaking with a valid law enforcement official.

So, that's where the PSWG thankfully stepped in, started some really important discussions with our community. My team within ICANN org participated in that. I think we've had, obviously, conversations with the GNSO. The Board has been very engaged in this conversation. And it got us to a place where first we could publish an updated Registration data policy that was in May, which indicated the 24-hour response timeline.

So, that's a response not an affirmative response, but a response from a registrar for authenticated urgent requests, and those are very narrowly defined, and that's of course defined in the registration data policy. What we are still missing, of course, is that authentication mechanism. Thank you. I will slow down. I have a terrible habit of speaking fast. So, the work that Gabe has been leading as he mentioned has involved a lot of different parties.

We've worked with Interpol, obviously, Gabe's agency, and ICANN to talk through what some of the options are. And what we heard at ICANN85 in particular from the community was a need to make these discussions a bit more transparent and open. It also became clear that we were coming to a bit more of an operational phase.

We think we're at a place where we can do some testing, both with the FBI and with the Interpol, which have two kind of similar approaches, portals that could connect with RDRS or a future system SSAD, whatever it may be called, that would allow us to determine what those technical requirements might be to ensure that we're passing along the right types of token and necessary information for a registrar to ultimately make a decision on whether or not to grant a disclosure request.

So, actually, very recently, just yesterday, you will have seen a letter from Tripti to Nico, and I can paste in the link to our chat that of course, notes the closure of the urgent request policy, that the policy has been set, the timeline has been set, and also that implementation work on an authentication mechanism is underway. This is the discussions we've been having. Because we're getting to a place where by March, as Marc highlighted, the Board anticipates receiving policy recommendation related to authentication, or right now in the SSAD, it's called accreditation, we are looking at this work as a way to get ahead on implementation.

So, you might think about this as pre-implementation work. So, shortly after this meeting, ICANN plans to initiate a call for volunteers for an input group. This is really carrying on the work that the PSWG has started for us to focus in on the operational aspects of a very narrow thing, which is just a proof of concept for how this authentication mechanism could work. And a proof of

concept is just that it's a test that we're planning to initiate with the FBI's LEAP portal and Interpol's GDPI.

Very close to GDPR, but GDPI, Global Digital Police Identity, is their new portal, which they have volunteered to test with us as well. This would be in a pure test environment, so they would not be submitting live requests, but it's a way for us to learn what works, what doesn't, what information do we need from identity providers. So, that would be the FBI or Interpol in this instance. And similarly, on the other side, what do registrars require to receive?

So, we want input from all parties, law enforcement, obviously, governments, registrars, data subjects. We're interested in hearing their perspectives as well. This will be an open call for volunteers. We will also ensure that it reaches all of the GAC membership as well. And again, I would like to frame this really as an effort to get ahead on implementation. We know we're going to have implementation work to do next year once the Board is in receipt of it and approves policy recommendations from the Supplemental Recommendations Team.

But this gets us in a position to be ready to actually implement an authentication mechanism. And the policy side is really important here. The work on an authentication mechanism and this input group, this proof of concept, is truly technical. That can't be finalized without requirements for who can serve in that capacity.

What those identity providers or I guess the term we're using right now is designated user group, but what those agencies need to provide to ICANN to connect to our systems, those are all important requirements that we need to understand from the policy development process and we're really looking to the Supplemental Recommendations Team to deliver that.

The intent with the input group is to begin meeting in July approximately and have something to share with the community, wire frames or process flows in time for ICANN87 is the next one, the annual general meeting in October, and start an actual proof of concept in December with an aim of completing work and any input from that group to be delivered together with the policy recommendations that go to the Board in March as sort of a package for a future IRT which we anticipate would begin year to consider as they implement those policy recommendations.

So, that's a lot of moving pieces, and I hope it was clear, but I'm happy to answer questions.

NICOLAS CABALLERO Thank you so much. Eleeza, we'll have a Q&A, hopefully mini session right at the end. So, at this point, let me hand the floor to Mr. Owen Fletcher from the U.S. Government. Owen.

OWEN FLETCHER Thank you, Nico. I'm Owen Fletcher, the alternate US representative on the GAC, and I'm not totally sure how well you

can hear me. Somebody. Okay, thank you. Trying to get closer here. Could we go to the next slide, please?

So, I will speak, I will give you an overview of where work currently is at in the ICANN community on privacy and proxy services. I wanted to start with a reminder of what these things are because not everyone in the GAC room probably thinks about them every day.

If you use a privacy service to register a domain, then the beneficial user, you the person using the domain, is still listed as the registered name holder in registration data records, but contact information shown is not yours, it's that of the privacy service. I just wanted to also note here beneficial user is a term used in part of the accreditation agreement for registrars. That's where that term is coming from. A proxy service is different in that the proxy service itself is listed as the registered name holder. And then if you are the user or customer of that proxy service, then they're licensing use of that domain to you. So, that's what we're talking about.

Next slide, please. There is a process going on right now to figure out how to implement some long-standing community recommendations regarding the accreditation of privacy and proxy services.

That process within the GNSO is an Implementation Review Team or IRT where both Gabriel from FBI and I are participating. So, the PPSAI, Privacy and Proxy Service Accreditation Issues IRT, is focused on implementing the set of recommendations. There are

many recommendations or multiple recommendations in the list. I pulled one out here that is particularly important. I'm going to read it.

One of the recommendations is registrars are not to knowingly accept registrations from privacy or proxy service providers who are not accredited through the process developed by ICANN. So, the IRT is discussing who should be able to get accreditation to offer a privacy or proxy service, and some related issues would include the one raised by this recommendation about how registration should be treated if somebody who's not accredited by ICANN to provide privacy or proxy services is still trying to do so.

There's a focus in the IRT on accreditation being available for affiliated services. So, what this means is only privacy or proxy services that are affiliated with an ICANN accredited registrar would be eligible for privacy proxy accreditation. So, I think there's general agreement in the IRT that that's the approach that should be taken on who's eligible for accreditation. There are other issues that need to be discussed in coming months within the IRT to resolve various details.

So, for example, what if you do have an entity that's not affiliated with a registrar, not accredited to offer a privacy proxy service, but is indeed processing domain registrations in a way that meets the definition of a privacy or proxy service at ICANN? What do you do then? How do you engage with that? So, an example of how this

might come up is a lot of times registrations occur through various layers of resellers.

The registrar itself, it may not be their website that the customer is using to register a domain. They could have a reseller who helps reach more customers. The reseller could have their own reseller. I'm just pointing this out because the IRT is going to continue with discussions to figure out what policy language will help address all the different situations in which these kinds of things come up.

I'll spare a lot of the other details of IRT conversations for all of you right now. And just one other issue I'll mention is the question of labeling privacy and proxy registrations in data records. So, sometimes if you perform a lookup and get the registration data for a domain, it may not be clear where exactly you should direct an inquiry if you have a question about what's occurring on that domain or any other need to contact or try to contact the person who's behind a domain.

So, one other issue being discussed in the IRT is how can privacy and proxy registrations be labeled as such in the records. That will help with more visibility so it will help you have clarity about where you can direct questions. If anyone has a particular interest in these issues, I'm also happy to talk offline in detail about privacy and proxy services.

I'll lastly just note that separately from this whole IRT process and questions about accrediting privacy and proxy services, in the last couple of years, the GAC has repeatedly commented on privacy and

proxy services just to emphasize that the RDRS or perhaps its successor system should be upgraded so that it incorporates support for disclosure requests when a domain was registered through a privacy or proxy service. I think that's it. Thanks.

NICOLAS CABALLERO Thank you so much, Owen. So, at this point, we have 10 minutes for questions. For the sake of time, I kindly ask you to be very specific and avoid elaborating before actually asking the question. Unless, of course, Justine, Marc, David, or anybody else, Eleeza, Gabe, you have anything to add, let me open the floor at this point for comments or questions. And we have the European Commission. Please go ahead.

GEMMA CAROLILLO Thank you very much. Gemma Carolillo from the European Commission. Thank you to all the colleagues for the interesting update. I have a question for Eleeza from ICANN.org. This relates to how do you see the interaction between the work on the SSAD recommendations and the authentication mechanism that is being developed for urgent requests?

Because in a way, the understanding is that the policy for urgent request is now settled. So, how the SSAD recommendations would impact on the authentication mechanism, which is rather an, I would say, practical tool being developed? Thank you.

ELEEZA AGOPIAN

Thank you. Good question. And tells me I didn't explain well. So, I think I can explain better. The supplemental recommendations team is considering the 18 SSAD recommendations. The first two recommendations were called accreditation and I believe governmental accreditation. Probably had a longer title, but I think that's primarily it. The team actually just yesterday and all of Sunday spent quite a bit of time on those two recommendations.

Those policy requirements are extremely important for how an authentication mechanism is implemented. So, the work that the input group is doing is really purely technical. How would you operationalize a token? How would, for example, Interpol pass its information to ICANN. What we're missing is what is the information that needs to be passed? Who qualifies as an agency, as an authenticator for ICANN?

Those are all important elements that require policy discussions that the Supplemental Recommendation Team is discussing. So, those are the two sides of the coin, if you will. Our intention and hope is to have a liaison between the Supplemental Recommendations Team and the input group similarly between the Board and the input group as well to ensure that we're all aligned on these pieces so that once we do have policy requirements that we are going to implement we're prepared we have the technical know-how and the mechanism that can be implemented so that we can enforce that timeline.

Right now, we don't have any authentication mechanism and we don't have a policy requirement for an SSAD system in place to require use of it to submit those urgent requests. I hope that was clear. Thank you.

NICOLAS CABALLERO: Thank you so much, Eleeza. I have the Government of Indonesia next.

ASHWIN SASONGKO SASTROSUBROTO: Thank you, Nico. I just want to ask to get me further information about the connections between the law enforcement agencies to get data from the ICANN. My question is, is there any data exchange from ICANN database to law enforcement agencies' data? Or it is the law enforcement employee who can open the ICANN database and see the problem and so on?

ELEEZA AGOPIAN: Great question. So, the intention is for the law enforcement employee who is authenticated, they would be passing their information through ICANN, which ICANN would deliver to the registrar or the party from which the data is being requested. There's no data that ICANN is releasing.

It's a flow through to the registrar who then determines, of course, whether or not to disclose the data, which in some fashion right

now in RDRS, flows outside of RDRS back to the requester if they are approved. Please.

GABRIEL ANDREWS

Yes, to everything that Elisa just said. I just wanted to add an additional point here. Sometimes in the discussions with the SSAD SRT, some folks are wanting to kind of merge the issue of like what is all the information an SSAD request has to have and can that be all part of that law enforcement authentication piece and they are two separate issues and I really want to stress this.

The issue of authentication is, are you sure that the person you think you're talking to actually is that person, full stop. That is a very important thing to make happen. And then, in addition to that, the SSAD form or the RDRS form as it stands now can ask all kinds of other questions that might pertain to your requests. Like what's the request about and like how are you going to handle the data?

All of that can be part of the form and that can change over time. But what fundamentally has to occur first is you have to have trust that you're talking to the person you think you're talking to. And I think it's very important, Marc I think is fully aware of this, that we keep these two ideas separate and not mix the two. Over.

NICOLAS CABALLERO: Thank you so much, Gabe. I have China, then India, and then I need to close the queue for the sake of time. We have five minutes. China, please go ahead.

GUO FENG: Here. Guo from China for the record. And actually, I have a comment with regard to the urgent request/authentication mechanism. So, with this issue, I think China believes that this issue is not only a technical and operational matter, but also involves complex topics such as cross-border law enforcement, international judicial assistance, and cyberspace governance.

So, currently, countries generally carry out the practice in cross-border law enforcement cooperation based on bilateral judicial assistance treaties, inter-pol cooperation mechanisms, and their own national laws and so on. So, therefore I think key arrangements such as the authentication mechanism need to be fully discussed within the GAC with law enforcement agencies and the broader community and the implementation path should be carefully designed.

So, if I understand correctly, for the time being, the PSWG is consulting on the design of the mechanism. So, China believes that this should be fully, deeply balanced, explored with carefully top-level design. And so, we hope that relevant policies can fully respect the differences in national legal systems and judicial practice avoid conflicts with existing international judicial assistance mechanisms and avoid affecting countries lawful

exercise of cyber space sovereignty and data governance authority. Thank you. I leave it there.

GABRIEL ANDREWS

I think you raise a very important point. Did not spend any time clarifying something that I really should take a moment to clarify now. The contemplation of how ICANN's RDRS or SSAD functions is another tool. another option for requesting data in a voluntary capacity of the data holders and registrars that exist across the world.

It is not a replacement for, it's not a substitute for other tools that may exist, such as the Mutual Legal Assistance Treaty requests, which are negotiated, as you said, bilaterally or multilaterally between nations, where they will set up arrangements to respond to one another's law enforcement requests.

I will say, having done multiple of those over the course of my career, that is a tool that is very important, but it typically involves 6 to 12 months of work and involves requests that go up through Departments of Justice over to the other nations and then down again. It is terribly important for some specific use cases where you need to get data in an evidentiary capacity to bring the cases to trial.

It's not a very good fit for requesting registration data because of the amount of effort that goes into it. And so, I think that it's important to recognize that a tool like SSAD is going to be very

helpful to investigators across the world to make voluntary requests which a registrar may say yes to or may say no to, and recognizing that that can happen both ways, it's still helpful to us as investigators to have this as one more option in the toolbox.

And none of this is going to ever get in the way of nor replace the ability to send compulsory legal process search ones through MLAT, et cetera. But I think it's a very important point that you highlighted and I appreciate the opportunity to respond to it.

NICOLAS CABALLERO Thank you so much, Gabe. We have two more minutes. India, you get the last question. Please go ahead.

SUSHIL PAL Thank you, Chair. Sushil. Sorry. Thank you, Chair. I'm Sushil from India, for the record. I have just two questions. One is, the request. Thank you for clarifying on the timeline for implementation of the SRT recommendation, which is by February 27, which is again almost six to eight months from now. And I hope that this will be the last committee when we can actually agree on authentication mechanism.

The only point I would like to stress that the implementation of an effective authentication mechanism, it should not be delayed or linked to the development of a comprehensive long-term architecture of the SSAD. That's number one. I think we need to

because I don't think recommendations will maybe get finalized by Jan or by Feb or March next year.

The other one is about making sure that the recommendations of the RDRS or whatever the learnings of the RDRS, they're actually incorporated and taken into account when we actually develop the SSAD framework. I think those are the two requests, especially the one which is the mandatory participation and the second one which is the authentication one. Thank you.

NICOLAS CABALLERO Thank you so much. India, any feedback you would like to give in 30 seconds? Marc.

MARC ANDERSON Thank you. This is Marc Anderson. And great points. I think you're right in noting that while the SSAD Supplemental Recommendations Team has the goal of finishing work on supplemental recommendations by February, there's still an implementation phase. And so, I think just to highlight you're right in pointing that out there's still more work to be done after that February date.

And then, the other thing, our charter, it's actually called an assignment form but it's basically a charter, and our charter is very clear in instructing us to take into account the lessons learned from the RDRS pilot. So, I take my assignment or my job as lead of that

group to make sure they're focused on the lessons learned from the RDRS pilot. So, very well put. Thank you.

NICOLAS CABALLERO

Thank you so much and thank you everyone. We need to wrap up now. Sorry, Justine, no more time for anything actually. We're three minutes over time. Thank you so very much, the Public Safety Working Group, Gabe and Owen, David Bedard from the Canada delegation, Marc and Eleeza. Thank you so much. So, at this point, let's give for the next session, and thank you again.

For the next session, let me call to the head table Gemma Carolillo from the European Commission, Sushil Pal from India, Susan Payne from the GNSO Council, and Jennifer Chung, who's the vice chair, I understand, and from the Registrar Stakeholder Group, Owen Smigelski, and Sarah Wyld. Please come to the head table. Okay, so welcome everyone. Gulten, I understand we're still recording, so no need.

Okay, thank you so much. So, welcome again, Gemma, Sushil, Susan, Jennifer, Owen, and Sarah. The agenda, okay, thank you. So, as you can see there, we have three themes, background on the timeline, the first one understanding the problem space, the second one and some considerations as the third theme.

Without further ado and for the sake of time let me handle the floor at this point. Are you gonna start? You can go ahead, or Gemma

are you first? Please go ahead, European Commission, you have the floor.

GEMMA CAROLILLO

Thank you very much, Chair. Again, let me introduce myself once more. Gemma Carolillo for the European Commission. We are among the topic leads for the registration data topic. I want to give a very brief introduction and also let my colleague from India intervene on why we are here discussing this topic. I think we have some background slides for the purpose but the topic of accuracy of registration data has been on the agenda for a long time.

This has been a matter of importance of the GAC since the early days that the registration data topic was discussed. Sorry, for the GAC support staff, I think we have slides on this matter. Voila. You can hear me? Okay. I see, even if I speak quite loud. Thanks for letting me know. So, I will not go into the details of all the times that the GAC has expressed itself on this issue, but I will just say that we have lots of reference documents because the topic of accuracy of registration data has been on the agenda of the GAC as well as the ICANN community for quite some time.

I wanted to say that we contributed as part of the Policy Development Processes, number one and number two, regarding registration data policies. And number two we had a GAC minority statement where we asked that accuracy be addressed in further

phases. Then we have participated to policy work on the matter, in particular, the Accuracy Scoping Team.

And we have contributed every time the GNSO has, I would say, revive the subject, because if you look at the timeline, we start in 2007, so we are almost reaching the 20 years. But what is happening today is that, considering the importance of the topic for some parts of the communities, the GNSO has held an Accuracy Small Team on registration data.

They have issued recommendations. And the GAC has expressed itself regarding this matter, supporting most of the recommendations that were part of the report. We are trying now, because we have had big time issues with defining accuracy agreeing with different parts of the communities on the way forward. So, we are trying now to narrow the discussion on some practical operational matters that have been identified at the crossroad between registration data and DNS abuse as a topic.

And in particular, we have urged in the Dublin, in the ICANN84 communique, the GNSO to identify an implementation path for the recommendations. Next slide, please. And the focus has been subsequently on the issue of the verification. So, we have seen from reports coming from the ICANN communities, but also in the discussions stemming from the GNSO small team recommendations, that there is a point of attention to the current policy requiring 15 days for the verification of registration data.

This is the maximum timeline. The colleagues from GNSO will explain better to validate and verify the contact information. We have different practices, this is for sure, across regions of the world and there are areas where there is no delegation of domain names before the contact data are validated and verified. And there are other practices, but the ICANN policy gives a 15-day timeline.

Based on the discussions held in between registration date and DNS abuse, we have asked to discuss with the GNSO and with the Board, including with the recent letters, a possible path forward to see whether there is a need to change the current practice with the view of tackling one problem, that is in DNS abuse in the recent time, speed has become the essential element.

So, whether a reduced time frame or whether a waiting time before delegation of a domain name makes sense, is relevant, how to possibly achieve that. And for this we wanted to start a conversation with the relevant parties. This is the reason why the GAC chair has addressed the letter to the board and the GNSO. I will now leave the floor to my colleague from India, Sushil.

SUSHIL PAL Thank you, Gemma. This is Sushil from India for the record. I think in the last conversation on 29th of May between the GAC members and the GNSO Council as well as the registrar's group. There were certain questions which were shared with them on which the GAC largely agreed. Could you get the slide? Largely agreed and these

questions actually fall into three broad headings. One is the background on the timeline for verification requirement.

And other is operational and implementation considerations. And the third is possible paths for implementation path. Although, maybe it might be prudent as to go into the history as to why the 15-day verification timeline was introduced. And I'm sure the GAC would be, sorry, the GNSO would be responding on those two slides on the history and the background of this.

But it's important to stress that, I think the way the technology is evolving, the way the AI is evolving, I think we need to make changes with much more agility than we have made changes in the history, in the past. The next slide, please. And the second is operational and implementation consideration, this is what the GAC member actually asked because, what could be the operational challenges?

Is there any financial constraint or operational constraint on the part of the registrars to put in this mechanism of a simultaneous registration before a domain becomes active. Mind it, I'm clarifying, we are not touching upon the accuracy or a two-factor authentication part here. That is a separate conversation to be handled in the accuracy team. What we are asking only, the request is only to shift the timeline from 15 days given for validation to making it concurrent, the validation concurrent, the moment the domains go active.

So, to our understanding, since it's only a timing issue, there should not be any operation or a financial constraint on the registrars, but maybe GNSO can clarify, I think, what in the last conversation they had indicated, that they need more time on this, but we are just highlighting the issues for this. Next slide, please. The third issue is what could be the possible path for the implementation.

We understand that the two PDP process is already on as a part of the recommendations for DNS abuse mitigation report and the GNSO is actually pretty heavy loaded, that's what we are told, that with the two PDP process at the now, so PDP process may not be the right time given the workload. But there could be other implementation path possible, other implementation mechanism possible, which could be simply the contractual amendments in the existing RIA.

This could be initiated either way. That is the reason for actually the request for trilateral conversation with the GAC as well as the GNSO. And we would also seek the cooperation of the Registrar Stakeholder Group as well to make this crucial step possible. Why it is so important? I think since Gemma asked me to touch upon that part as to why we are stressing upon this, because I think this is the simplest of the recommendation to implement actually.

This does not require any financial constraint, nor any technical, nor new platform to be implemented. I think in the earlier session we saw that there's a complete new system being put in place for request for authentication from the requester and then the

registrar to provide those details for which a technical platform is required to be built. In this case, nothing changes.

Everything remains as such, and only the timing changes, and from the report we have had so far, from the various ICANN research work carried out, by various committees, like an informal report, as well as the DNS abuse, and also pointed out by the Security and Stabilization Advisory Committee in their various reports that the validation and the verification when put in effectively, that leads to sufficient reduction in the domain abuse. So, with that, I think I would close my remarks. Thank you.

NICOLAS CABALLERO Thank you so very much, Gemma and Sushil, Indian and European Commission. At this point, let me give the floor to Susan Payne, who's the chair of the GNSO Council. Over to you.

SUSAN PAYNE Thanks, Nico, and thanks very much to everyone here for organizing this meeting and for the opportunity to engage on these really important topics. So, we do really appreciate being invited to discuss DNS abuse issues and this issue related to the verification. And obviously, we all view the security and stability and the trust in the DNS is being incredibly important, and so, we really do appreciate it.

Now, the first theme, if you like, was about the kind of background of how or where did this 15-day come from and what is this

responsibility that exists. And essentially, as part of the updates to the Registrar Accreditation Agreement or RAA in 2013, there were various changes and enhancements made, but one of those included this verification provisions. They're included in what's called the RDDS accuracy program specification at a very high level.

What they do is they require registrars to ensure that certain information is included and is properly formatted in various data feeds. So, to do with things is an email address, not to check the email address at that point, but is there an email address in there if it's required to be, is a phone number in the right format? That kind of level of checking. And then verification within the 15 days of registering a new domain or transferring a domain or updating the registrant's name or email address.

Verification by one or other means of either via email or via a phone or text message to a phone number. Now, I should just pause and say verification isn't required in that mechanism if it's already been completed. So, if that data has already been verified, then it's not required to be done again if the same data is being used for a new registration because it's already verified. But when the email address is sent or when the…

Sorry, I'm just getting some messages… when the email is sent or the SMS message or the phone is sent, if there's no affirmative response from the registered name holder, then the registrar must either manually confirm and get that verification in a manual manner or they should suspend the domain. And so, as the current

requirements stand, and I think this is what we're here talking about, the verification isn't required prior to the registration and activation of the domain name into the DNS.

So, it is something that can happen afterwards. But as I say, if that verification cannot be achieved and it cannot be manually verified, then the domain would have to be suspended if it isn't possible to get that verification. I will just pause that we have a few questions about procedural matters, but I will also pause and just see if Owen Smigelski wants to add anything. Owen works for one of the registrars and is currently the chair of the Registrar Stakeholder Group.

But in his former life, he actually worked for ICANN Compliance and was kind of involved in the process where the registrar accreditation agreement was updated. So, I just want to pause and make sure I haven't misrepresented anything or if there's any more color and detail he wants to add.

NICOLAS CABALLERO So, before I give the floor to Owen, let me just agree that we don't actually have 45 minutes. That agenda you presented, that was a 45-minute agenda. We only have 25 minutes just in case. Owen, over to you.

OWEN SMIGELSKI Thank you, Nico. Hello, I'm Owen Smigelski, chair of the Registrar Stakeholder Group with the domain name registrar Namecheap.

And as Susan alluded to, I spent seven years with ICANN Contractual Compliance, and as part of my responsibilities there, I led the development and implementation of the 2013 RAA Accreditation Compliance Program within ICANN Compliance.

So, people wonder where did this 15-day verification window come from, and a lot of it is a legacy. So, the 2013 RAA was a successor to the 2009 RAA which was a successor to the 2001 RAA. The 2001 RAA had a requirement in there that if a registrant had to provide accurate details to a registrar for its registration data which would then be in the output at the time the WHOIS, and then If any inaccurate information was provided or discovered by the registrar, they had 15 days to correct that.

And so, that carried forward to the 2009 RAA. And during the negotiations process, that was used as a baseline for any other need to correct or verify information because registrars had already built systems in place to do that. Another reason why that was at window to have that instead of doing a preemptive verification of the email address was because people do come to registrars, register a domain name, and use that new domain name as the email address that they are registering.

And if you require them to verify before they set up a domain name using the new system or a new domain name, then that would really frustrate and make that difficult, if not impossible. So, that's just kind of where that came from and how it continues forward. In

the interest of time, I think we'll move on because I know Sarah and I have some data to present later.

SUSAN PAYNE

Thank you. And I will just go quickly back. I know there were a couple of more practical operational type questions that our colleagues had shared, and I am not the person who can answer them, but I'm very lucky to have some registrar colleagues.

So, I think a couple of them probably are worth us covering off because they are quite useful background information. So, one of them was around if there is a difference in the timing of the registrant responses on new registrations versus transfers of registrations or renewals of domain registrations. And so, I'm going to have Sarah who is going to answer this.

SARAH WYLD

Thank you. This is Sarah Wyld. I'm the Vice Chair for Policy of the Registrar Stakeholder Group and work at Tucows. So, we do verification for new data contact sets that's on a registration, a transfer in, or a contact update, and those are all in the same time frame of 15 days. It's not required upon renewal because that contact set is already verified.

However, if there becomes some reason to believe that the contact set is inaccurate, so for example, the registrar sends a renewal reminder to the domain owner and then is aware that we receive a bounce back, then the same verification is required where the

domain owner must confirm and demonstrate that the data is accurate and operational.

SUSAN PAYNE: Thanks, Sarah. And the other really quick one was I think we were asked about two-factor authentication which is now routine across different sectors and there was a question of why doesn't this happen on domain registration, and again I think it's worth a quick touch on.

SARAH WYLD: Thank you. So, multi-factor authentication is a technical functionality rather than a policy or operational, well, I guess it is operational, it's not a policy, right? If policy gets into requiring a specific technical solution, then we have to update that policy or contract every time the technology improves. So, it used to be very common to do SMS multi-factor authentication. That's no longer the best way because of SIM swapping, right?

So, instead, it's authentication tokens. And so, we don't want to have to update the requirements every time in order to keep up with the tech. But many, if not most, registrars and resellers do offer or require multi-factor authentication. It's just not something that makes sense to go into the policy. Thank you.

NICOLAS CABALLERO: Back to you, Susan.

SUSAN PAYNE

Okay, and I think at this point, it's probably worth moving on to the second theme of our discussion, which is, as we've been trying to frame it within the GNSO, certainly for this, what we really view as the start of a conversation or the beginning, we understand that there's likely to be further discussion. So, for now, what we wanted to touch on was understanding kind of the problem space. And I'm going to hand to Jennifer for this.

JENNIFER CHUNG

Thank you, Susan. This is Jen Chung, Vice Chair of the GNSO Council. We're going to take a look at understanding the problem space. I think it's very important for us before we have a deeper conversation on how to solve it, we should have some common shared understanding of what the problem we're looking at is.

So, the verification obviously here in the 15-day timeline it needs to occur within 15 days, but the domain can be registered and active before or prior to verification being completed. You see there, there's a quote there from our final issue report, both the data from the INFERMAL report and also our final issue report, they reference the research here are important data points. I'm not going to read it out loud. I think that the slides can be shared.

I mean, given the time that we have, I think it's actually valuable for us to take a look at some data that our registrars have also began collecting on this topic. And two of them have actual published

data, Tucows and Namecheap. I think you already heard from Sarah from Tucows and also Owen from Namecheap. They will have some more data to present here.

A caveat here is that Council has not reviewed this published data yet and doesn't have a collective opinion, but obviously, for the purposes of this information session, I think it's very useful for GAC to also take a look at and consider these. These are findings from two registrars.

Not all registrars might show the same trends, but nevertheless, these are definitely data points we can consider. I am now going to pass to Ashley Heineman. She is our Registrar Stakeholder Group councilor on Council to introduce the next parts on the research that separate registrars have been doing. Ashley.

ASHLEY HEINEMAN Yes, I'm going to go very quickly as well because we were under the impression we had 45 minutes. Just to be clear, we were notified about your interest in talking about this about a week and a half ago. So, we are not speaking here collectively as all registrars, but we did want to take advantage of this opportunity to talk to you all.

So, please bear in mind that what we're working with is a snapshot from two registrars. We're very happy to have these conversations, but moving forward, a little more time would be greatly appreciated. So, without further delay, I'm going to go ahead and

turn it over… Who would like to go first? Owen. Turn it over to Owen from Namecheap.

OWEN SMIGELSKI What's the next slide?

ASHLEY HEINEMAN Oh, never mind. Next slide. Oh, my bad. You pointed it out, Owen. It is Sarah. All right. I'll turn it over to Sarah from Tucows. Thanks.

SARAH WYLD Thank you. This is Sarah from Tucows. So, I am here to share some information that we gathered from our operations as a registrar, and I'm going to drop into the Zoom chat the link that's also on the screen so you can review in much more detail at your leisure. First, we looked at when verification is completed, and to make sure that we got the most useful data in this context, we excluded any domains that used an already verified data set as we heard about earlier.

So, we looked only at when is completely new data verified. Almost half of the domains we saw were verified right away. The same day they were registered, they completed that verification. The remaining half broke down mostly into two groups. 25 of all the domains were the verification was completed within that 15-day period. So, the bulk of domains are verified within 15 days. The other 25% were suspended because they did not verify their data.

There was 2% to make up the rest of it, those actually got suspended but then they completed the verification.

So, some portion of people don't make it in time and then come back and complete their verification. So, that was the first set, it's just when is verification completed for new data. Secondly, we looked only at domains that had been used and we shut them down due to DNS abuse. For those domains, most of them used data that was already verified on a prior domain, 82%. 14% completed the verification right away or they were not gTLDs, they didn't require verification.

2% we had flagged for payment fraud, so it's just not part of verification. I didn't think about it. And the remaining 2% were suspended due to incomplete verification. So, to say that again, out of domains that are used for DNS abuse, if we look at how many of them would have been shut down due to not being verified, it's only 2%. Thank you.

OWEN SMIGELSKI

Next slide, please. Hi, Owen Smiigelski. So also, like Sarah, I'm going to drop the link into the Zoom chat. It's on the screen but it's easier to access from that if you want. So, what Namecheap took a look at is we took a one-year sample period which covered 5.3 million domain names, and we took a look to see, hey, what has happened with those?

And through our analysis, our team found that over 98% of the domains that were suspended for DNS abuse had already passed email verification. Of that, 69 days was the median time from registration to suspension for abuse, and 81 days is the average time. Now I just want to flag to say that they weren't doing that for 69 days. They were that old when they were suspended.

Namecheap has done a lot of time, effort, and money to ensure that we have a very quick response to DNS abuse, and our response time to reported or abuse that we are aware of is measured in hours, not days. So, that should not be a takeaway, but what we would like to highlight is that the age of domain names being used for domain name abuse are older domains.

We are seeing ones that are almost in the renewal period being used for DNS abuse. I know INFERMAL cited that. domain names recently registered are the primary vector for DNS abuse. That cites a 2010 study, which might be a little old because that's not what we're seeing today. So, I would caution taking that as a fact because that's not what we're seeing. Of the domains that were older than 15 days, almost 75% of the domains used for abuse were older than 15 days.

So, there's a substantial number that are going through. And then of the domains suspended. for failed email verification, almost 85% of them had no abuse involvement at all. So, innocent people are the ones that are being impacted by this email verification requirement. And then for ones that had suspended for abuse and

also failed suspension was about 1.86%. And overall, we had 1.6 of those registrations were flagged for abuse.

Coming back to that 1.86% about domains that were suspended for abuse, I asked my team, it's not in the blog, but I wanted to see, was there a difference between domains that were verified before registration, verified during the 15-day period, or were suspended after the 15-day period. And the numbers vary from 1.1 to about 1.6%. So, statistically, there's not really that much of a difference when the email was verified, before, during, or after that 15-day period, if a domain is used in DNS abuse.

So, what we're trying to do is put data out there, and again, we can collect more, we can look to more stuff. But if we're going to make a big change, we want to make sure that it's based upon what we're seeing and what could happen out there. Thank you.

ASHLEY HEINEMAN Thank you, Owen and Sarah. And just to note, this is the beginning of our research. What this does reflect is a perspective from a wholesale and a retail registrar. But also, to note here that there is a small percentage of abuse that comes out through this, but I also want to challenge something that had been said earlier by one of the GAC representatives, and that this is not hard to make a time change. There is cost.

There are resources involved in making any change, especially when there's operations involved. This isn't to say that this won't

deal with any abuse because there is a percentage here, but just to keep in mind and prioritization in terms of your resources, our resources, where to put the focus on. So, I will stop there and turn it back to Jen. Thank you.

JENNIFER CHUNG

Thank you very much, Ashley, thank you, Sarah, thank you, Owen, for sharing some initial research on it. Again, I cannot highlight enough that this is the start of a conversation. And also, let's go to the next slide. Kind of just a reminder of where we are in our DNS abuse policy work.

A reminder as well, when the council looked at this as a small team before we were putting together the initial report and the final issue report, we looked at many considerations, and specifically we got a lot of input from the SG's, the C's, the SO's, and AC's. GAC yourselves also sent us your list of priority gaps and topics.

And several factors affected how we were looking at prioritization of this work as a whole, including of course the importance and the impact of a topic across the Board, the stakeholder groups, and the constituencies. The second one is the likelihood of achieving consensus. Third is the visibility and the scope. And then fourth, of course, is the potential impact of reducing DNS abuse at scale.

And of course, based on these factors, and of course, looking at the timeline, the resourcing that we have, we've of course went to the two topics that we currently have, and one is an active PDP, the

Associated Domains Checks. And of course, thank you to GAC sending your experts, sending your topic leads to participate actively in this.

I think there is a very good progress being made there. And also, for Council, we've begun to look at updating the PDP 2 charter, which is the second prioritization gap that we will be looking at. So, we won't go into too much detail here, given the time.

I'd like to now turn over to our agenda item number three on discussions on the next theme. So, if we can move to the next slide. And this is regarding the considerations on how new obligations arise. I'll pass this back to our GNSO Council Chair, Susan.

SUSAN PAYNE Thanks, Jen. We've been we've been asked, if one feels that that changes are needed, what mechanisms are available to do that? And really, there are two. We have the PDP process, which is the Policy Development Process, that's a multi-stakeholder group that gets together. There are some efforts that happen before the PDP kicks off, something like an issues report is put together and so on.

And in relation to DNS abuse, we already have that issues report, and that covered a number of different topics. So, it covered the two that we already have kind of in progress, the PDP 1, which is the Associated Domain Checks, and PDP 2, which will start in an appropriate time which will be on considerations around API access.

But I think as you are aware, a number of other abuse related topics were in the issues report as well including this issue around verification timing. And so, we already have the issues report. And so, we really have the question of what the discussion is around the appropriate timing and the prioritization of the various other issues that are in that issues report that we need to come to.

And generally, typically, around about three or at most four really active projects are probably what gets the GNSO and indeed the wider community up to capacity. But Bear in mind also that what we've tried to do with the DNS abuse is to break it out.

We could have done one enormous great big PDP on DNS abuse covering everything. That would probably take many years because we would be working through so many different issues. But we've tried to break it up so that we can move that through faster, and then when one finishes or gets to a certain point, we can get on to the next topic.

But we do have some pretty meaty things that all of the community are fielding their active participants on including this DNS abuse PDP and the work that just kicked off that you were talking about prior to this around revising those SSAD recommendations for the registration data.

So, it is a factor to bear in mind and it is certainly something that that Council is bearing in mind when we are working on what we prioritize for our next work. I think if we maybe go to the next slide.

And I think Jim was going to talk a little bit more about -- Oh, indeed.

NICOLAS CABALLERO: Thank you. As a matter of fact, let me open the floor now for comments or questions. If we can go back one slide, I see a couple of things I wanted to mention before I give the floor to India. I see an iPad or something there. I have Japan and India. So, I see a couple of issues there. For example, as regarding the -- No, one slide. What happened there? Can you go back one slide? Oh, my God. Anyways, India, you have the floor. Please go ahead.

SUSHIL PAL: Thank you. From the presentation, I see there is a narrative to actually figure it out whether there is a problem or not. I hope that the problem statement or the problem space is already laid out and it's very clear. And when I say it's very clear, it's important that the community discussions that should rely on the broader body of ICANN research and the neutral expert analysis rather than on isolated operational studies of a few registrars. That's important point to note.

The various instituted ICANN commissioned research, be it the INFERMAL study, which is a much broader study whose methods were completely shared with everyone and were examined, and the DNS abuse final issue report, and the various SSAC advisories have clearly spelled out that the timely validation and verification

would lead to significant reduction to the extent of 60% in the domain abuse.

So, that's number one. And second would be, I think we're all talking about as to how the present system takes care of it, right? The Tucows presentation spelled out that there's only 2% of the domain names which are actually abused because they were not verified. I think we should look at absolute number. I mean, if we extend the same, I think I understand two causes, one of the reputed registrars, right?

And if we extend the same 2% to the total domains in the world, we have about 400 million domains in the world. So, roughly about 80% of the domains are being abused. Is that a number we are ready to tolerate and live up in this age? So, I think that's what we have to look at. It's a classic externality problem, when we talk about public goods and the private goods, because none of us are actually getting harmed here. It's the community which is getting harmed.

The money is actually being made by the fraudster, by the malicious actor, and maybe about a few registrars who are actually making money because of the quick registrations at very cheap prices at which they are registering the domains. But who is getting harmed? It is the consumer which is getting harmed. It is the citizen which is getting the harm. It is the brand owners which are getting harmed.

It is actually leading to the lack of trust in the digital economy, and that is what we have to look at. The purpose of registration process is to build the trust in the digital economy, is to build the trust in the digital ID. And let me tell you, the moment you build trust, the scale of domain registration will take care of all the revenue losses which a few registrars may have.

And responding to the question of, Sarah, when I said that it does not involve very significant cost, I say that with full confidence and full authority because we actually look at the operations of a ccTLD very closely. It's just one tweak in the software, nothing more than that. And when I say that, I'm not talking about a two-factor authentication. That's a separate conversation for accuracy team.

It's only making the domain activation concurrent with the validation, that's it. And we also operate at ccTLD, I think, and we are pretty confident as to what changes it needs. It's not that we're not registrars, we're not aware about the operations. And just one more topic I would like to touch upon. I mean, in the various reports, I must comment that these two registrars were sharing the data, but please remember that GAC has been asking the GNSO and the ICANN to have a centralized portal of all DNS abuse.

If the registrars can actually publish all the domains they are registering, in what timeframe they are getting verified, and all of them which are getting abused, in what time they were verified? If the Registrar's Stakeholder Group can take up with the ICANN org to publish all these data by all the registrars, I think that itself will

bring in a lot of transparency in the data we're talking about. Thank you.

NICOLAS CABALLERO

Thank you so much, India. Before I let Susan or Owen or anybody, Jennifer, anybody to answer, I just want to make sure that everybody understands that, number one, we are already over time. Number two, I have a long queue of member states asking for the floor.

Please try to be brief and straight to the point. We're going to go at least 10 more minutes if okay with everybody, but I really think this is an important topic and that we should allocate 10 or maybe 15 minutes extra taking it from our lunchtime. I have Denmark, Japan, United States, and I saw a couple more, but please go ahead, Denmark.

FINN PETERSEN

Thank you; Finn Petersen, Denmark for the record. Thank you for the presentation and the figures you put on the slide. I understand that the 15 days is legacy for a long, long time ago. And we are now in 2026, so many years have gone. We have ourselves implemented and have rules that it must be verified before it's put into the route, and that have followed by EU member states have come together and make recommendation, and one of the recommendations was that the verification should be done before it's put into zone.

We were not aware that there was any practical administrative problem in doing that. I would like to ask, is there any technical problems in doing this verification before it's put into the zone? Thank you.

OWEN SMIGELSKI

So, cognizant of time, I'll answer very quick, because this was raised by India as well. There is a technical cost, because there's always development. We have finite resources for that. And part of our preference is, when we look at the data, we see there's no difference if an email is verified before registration, during the 15-day period, or after, same levels of abuse. And certainly, we have no desire to have DNS abuse out there. It harms our platforms.

We use our platforms as well, too, bad reputation, et cetera. We want to do what we can and focus our resources on things that we know can target and reduce DNS abuse. We're willing to spend the money for that. It's just, as we look at this data, we don't see it as much with the email verifications being something that will significantly reduce DNS abuse no matter where it is. But happy, this is a starting discussion, we definitely want to have more conversations around this.

NICOLAS CABALLERO

Thank you very much. Japan, please.

TOMONORI MITAMOTO

Thank you very much. This is Tomo from Japan. First, let me thank the GNSO colleagues about having this opportunity. And this is a very important first step for our further discussion. And I have two questions. And one is about, well, for the 15 days verification timeline, I think that it's not only for the newly registered domain, but also like inbound transfer changes and the in accuracy discovered. And I think these all four have different characteristics.

So, maybe is it good to think about just one policy for cases, or I think that it might be employed different policies for each case. And my second question is about, it's like Finn's question, but I recognize that there are many registrars having different policy about the verification. Some registrars verify the contactability before the active vision of the domains. What makes this difference, and is there any you know cost problem or technical difficulties, and I'd like to know the details of it. Thank you.

SARAH WYLD

Thank you. This is Sarah. I can speak to that first question about maybe changing the time frames for different types of verification. I find it a lot cleaner and simpler to have one policy where things are the same. So, if it's verification, doing it all on the same timeline will make more sense to customers and will be easier for ICANN Compliance to enforce.

So, if they're trying to enforce a different timeline on different actions, then they have to know which action has happened and it

becomes quite complicated. But that is a topic that we could further discuss as we continue this.

NICOLAS CABALLERO Thank you, Japan. Thank you, Sarah. I have the USA next.

SUSAN CHALMERS Thank you, Chair. Susan Chalmers, United States. We recognize this discussion as the opening of a dialogue with the GNSO on the verification timeline, and we do greatly appreciate Tucows and Namecheap for gathering data to help inform this dialogue, and quite quickly at that. For the United States, our priority remains seeing that the ADC PDP is implemented before the expansion of the DNS as a result of the next round.

But we also agree that the existing 15-day timeline for data validation, which, as my colleague Finn mentioned from Denmark, is a holdover from 2001, is a policy deserving of re-examination. So, we look forward to re-engaging productively, or engaging productively with the GNSO and registrars on this going forward. Thank you.

ASHLEY HEINEMAN Thanks, Susan. Yeah, I think we're interested in continuing the conversation and I think it really does come down to prioritization. This isn't to say that this will have no impact on DNS abuse. We're just trying to give a little bit of insight with respect to what level of impact this would have. And I think something else that we need

to also keep in mind is that how will this impact other areas associated in this contractual language because what we haven't discussed is the impact on renewals.

Would this shortened timeframe also be applied to renewals? Because that's where the real problems would happen. Because those people are already established, they already have established websites, and if you limit that time of 15 days, you're gonna be really impacting business. And so, there are other factors that need to be considered as part of this conversation, because this is looking at one small part of a broader piece of policy. Thanks.

NICOLAS CABALLERO

Thank you so much. Before I give the floor to the European Commission, I just wanted to mention two things, there are more but just for the sake of time. When you refer to progress, PDP 1, ADC making good progress, to start when time is right, who determines when the time is right and what is the time frame in that case? Are we talking about six months, two years, ten years and so on and so forth?

And the same thing applies to the prioritization. When you refer to prioritization, the GNSO Council is working on blah blah blah, mechanisms when capacity is available. So, that capacity might be available in two years, in five years, in six months? And there are

some more concerns and we can talk about that later. At this point let me give the floor to the European Commission.

GEMMA CAROLILLO

Thank you very much, Nico. I just wanted to flag our appreciation for this conversation, which we have encouraged already more than one month ago when Nico sent a letter to the GNSO and the Board. So, I think we had, everyone, ample time to prepare, but we are really willing to take this forward. We do not see any sort of competition between the policy development process and this discussion, first of all, because we are at the discussion stage.

Second, because we are talking about contracts, so this does not necessarily require a policy development process. And third, precisely because we are entering into the new round and new contracts will be signed, it will be important to see whether we are not just carrying on from 20 years on rules that are outdated.

In moment where in the digital economy both users in terms of citizens but especially businesses are very much used to act fast, not necessarily regarding the verification of their email contacts, but even every other sort of business information, and hence, the timeline might be outdated. But in all cases, the principle that stands is that before delegating a domain name into the space, in the DNS space, there should be as a minimum an understanding that the basic contact data are verified. And we take very well note that this may not be enough.

We hear that contact verification of email may not necessarily be sufficient in order to prevent DNS abuse. And of course, we are willing to hear from the registrars that are those who work on the field on what could be better ways, if any. But let's not just bring into the new round of gTLDs and the new contracts, old practices we are not even sure they work at all and are fit for the purpose. Thank you very much.

NICOLAS CABALLERO Thank you. European Commission, Susan, Owen, Jennifer, Ashley, anybody on this?

JENNIFER CHUNG I think I will be responding a little bit on that regarding the two possible ways of how we are going to be able to actually have impact on there. I think if we can go to the next slide. Just a final bit. I know we are over time. Just very, very quickly to the next slide. Yes. Regarding this, Susan already mentioned earlier the policy development process, and I think there was a lot of questions around that prioritization.

But here, I mean, very clear here, when we're looking at the other part, where actually obligations are being made to the registrars of the contracted parties, a real big caveat here is this is not a trivial undertaking. It may not be timely. Here very clearly the requesters, you can see here only the ICAN CEO or the Registrar Stakeholder Group chair can request that. So, currently, we actually have the

Registrar Stakeholder Group chair sitting and the incoming Registrar Stakeholder Group chair sitting on the dais as well.

The limitations here again, the scope cannot modify the consensus policies. The frequency, you cannot proposed modifications more than once every 12 months. Of course, there's bilateral negotiations. There can be proposed revisions. These are subject to public comment. The duration of that is at least 30 days. Again, updated revisions, again based on the public comment received, are also subject to registrar and ICANN Board approval.

So, again, affirmative approval of the applicable registrar's account for 90% of total names under management is required. This is a very high threshold, a very high threshold to get contractual amendments done. So, another kind of context, you'd be like, okay, there was contractual amendments. How was this achieved? Why does this actually work? This is because the registrar's approached ICANN to negotiate more stringent requirements. They wanted to raise the bar for the industry.

So, again, understanding a little bit more about what this path entails is important. And amendments again are effective 60 days after notice. So, given that timeline and understanding that is something that I think is important for us all to have a basic understanding of. I think I'm going to pass now over to Susan.

SUSAN PAYNE

Yeah. Again, we have the slides and hopefully, they'll be shared with you. There may be a little bit more information on the slides than we were able to cover. And certainly, we had intended to talk in more detail about some of the efforts we were doing, like the prioritization work we're doing and so on. So, we haven't really had the time, unfortunately, to cover in maybe as much detail as we might like, but we do really, again, appreciate being invited to come here.

We are viewing this as let's keep discussing this. We would like very much to do so. We absolutely appreciate your engagement on this. We have a set of DNS abuse issues in our issue report, and we will be working out which ones we come to next. And so, as part of that conversation and that decision-making process, hearing from stakeholders on what they are viewing as the priority is very important for us.

So, we all, I think, have a shared goal of keeping the DNS safe and secure and avoiding abuse and safeguarding consumers, and I want to absolutely stress that I think we share a goal. So, even if we may disagree on what the best next path to getting to the goal is, we share the goal.

NICOLAS CABALLERO

Thank you very much. Thank you to the GNSO Council speakers, Susan and Jennifer. Thank you to Owen and Sarah, and of course,

Ashley, and thank you to the European Commission and India for the lead. Apologies for going over time.

By the time you finish speaking, Susan, this was indeed a 45-minute session, but we had the European Commission and then you, and at that point you said, oh, we have 45, no, we don't. But anyways, apologies for that. We're going to have a lunch break now. Please be back in the room at 14:45. Thank you very much. The session is adjourned.

[END OF TRANSCRIPTION]