ICANN85 Mumbai | CF – GAC: Discussion on WHOIS and Registration Data Issues
Tuesday, March 10, 2026 – 10:30 to 12:00 IST

JULIA CHARVOLEN

Welcome to the GAC discussion on WHOIS and Registration Data on Tuesday, 10 March at 10:30 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.

During the session, questions or comments will only be read aloud if submitted in the proper form in the Zoom chat pod. Interpretation for this session will include all 6 UN languages and Portuguese. If you would like to speak during this session, please raise your hand in the Zoom room. Please remember to state your name for the record and the language you will be speaking in case you will be speaking a language other than English. Please speak at a reasonable pace to allow for accurate interpretation. I will now hand the floor over to GAC Chair, Nicolas Caballero. Thank you.

NICOLAS CABALLERO

Thank you very much, Julia. Welcome back, everyone. I hope you enjoyed your coffee. We have a fantastic lineup this morning for this session. This is going to be a 90-minute session, an hour and a half, basically till lunchtime. And for that, we have Eleeza Agopian. I hope I pronounced your last name well. My apologies, just in case.

We also have Gabe Andrews from the FBI. We have David Bedard from the Canadian government, and of course, Mr. Fletcher. I'm sorry, Owen Fletcher. I just forgot the first name. Mr. Fletcher from the U.S. government, of course. So, we have a lot to talk about. I just want to make sure we have enough time for a good Q&A session afterwards. So, without further ado, let me give the floor at this point to, is it you, David? Are you going to start?

DAVID BEDARD We'll do PPSAI. Yeah, we're going to do PPSAI first.

NICOLAS CABALLERO Ah, PPSAI first. So, yeah, that's Owen then. Owen, over to you.

OWEN FLETCHER Thank you, Nico. I'm Owen Fletcher, and looking at the slides, we're, okay, so Fabien, can you advance, please, to the PPSAI slides? Next slide, thank you.

So I'll just give a very short, maybe one-to-two-minute bit of background on where this issue is right now. Then we have a presentation from Jason Ken of ICANN Org about this topic. So, for those of you who are new or have not been in the GAC for very long, you may not recall a whole lot of discussion about Privacy and Proxy Services in the GAC.

In recent ICANN meetings, the GAC's discussion and comments have focused on supporting disclosure requests for customer data

regarding registrations through Privacy and Proxy Services through the RDRS. But Privacy and Proxy Services more generally are an issue of longstanding interest to the GAC.

Domain registrations through Privacy Services have become very common in recent years. Jason will all be explaining more about what Privacy and Proxy Services are to help understand what that means, to help us understand what that means. The GAC, through myself and Gabriel Andrews of FBI, is participating in a current implementation review team, or IRT, that is working to implement some recommendations that were accepted by the ICANN Board years ago regarding accreditation of Privacy and Proxy Services. So, the PPSAI is the Privacy and Proxy Services accreditation implementation recommendations.

So, as Gabriel and I follow the discussions of the IRT in coming months, the GAC will likely have more updates on this issue and maybe some opportunities where it would be appropriate to comment on what's happening there. So, we thought this would be a good opportunity as the topic leads to have the full GAC get some background on this topic and have it more recently in our memories for when there are appropriate times in coming months to comment on developments in the PPSAI implementation.

Can you do the next slide, please? I'm going to hand it over to Jason Kean from ICANN Org who is helping to run the work of the IRT. And thanks to Jason for doing this virtually from I think the US West Coast where it's late at night. Thanks.

JASON KEAN

Great, thank you, Owen. Appreciate the opportunity to speak with everyone about Privacy and Proxy Services and the accreditation issues and current implementation. So, I'm going to give everyone a high-level overview of some of the substance and also some of the work. So, as you noted, when this comes up for Public Comment, your GAC colleagues are ready to discuss it and provide Public Comment on the draft consensus policy.

So, just a little bit of level setting, some definitions. Privacy service allows a customer to register the domain name and their own name as a registered name holder, but the contact information of the Privacy service is displayed in the publicly accessible registration data directory service. So, their own name, but it is reacted, it's through a Privacy service.

Proxy service allows essentially the Proxy Service to register the domain name as a registered name holder and then licenses the use of the domain to the Proxy customer. So, that's the distinction. The full registration data of the Proxy Service registered name holder must be published in the RDBS. So, trying to delineate and level set for everyone on that.

There's quite a bit of history as Owen had suggested here. This was an outstanding issue from negotiations of the 2013 RAA. And in October, 2013, the council initiated a PDP to make recommendations for consistency across Privacy and Proxy Services. So, quite a while ago. The Working Group, as Owen

mentioned, produced recommendations, they were adopted by the Board 2016 and implementation began. However, ecosystem is evolving.

This implementation was put on hold in 2019 due to overlapping issues with ongoing work related to the GNSO's expedited policy development process on the temporary specification in light of the European Union's general data protection regulation. So, started a long time paused while additional things were being done in the ecosystem.

So, upon publication of the registry data policy, which implements the PDP phase 1 recommendations, ICANN Org called for volunteers to reconvene an IRT to support the continued implementation of these recommendations. This IRT was convened in June of 2024. And in light of changes to law policy and industry practices, again, we're talking 11 years after the original recommendations.

The first task of the IRT was to respond to a set of threshold questions to inform continuing implementation given the changes in the ecosystem. Those responses to the threshold questions were submitted to the council in August of 2025. And along with the request for additional guidance, and the council responded with its guidance on the 13th of November, 2025.

Some areas at high-level definitions were discussed. They seem to be pretty stable with the original recommendations. What was envisioned in terms of accreditation for Privacy and Proxy

providers was also discussed. And I'll touch on that in a little while, as well as alignment with current policy, namely the reg data policy, and Urgent Request timelines as well, and considerations for SSAD, RDRS, or a successor system. So, a lot of considerations with the guidance.

Next slide, please. So, the objective of implementation, as I noted, pulling it together, to develop service requirements in line with the original recommendations, but also in line with the implementation guidance provided by council.

The impact of these recommendations, once implemented, will be a new consensus policy which will supersede placeholder language that was included in the 2013 RAA, along with a temporary requirement specification for Privacy and Proxy Services in the agreement, which is still standing. It'll just be superseded once this consensus policy is adopted.

So, the IRT settled on an implementation plan with ICANN Org. This is available on the community wiki page. It details deliverables, dates for the work, milestones, and also has a work breakdown, which does sequentially how the IRT will be conducting and achieving this work over time, week by week. This will, you can see the implementation progress at any time on the Privacy Proxy wiki page.

So, the current work just came from an IRT meeting earlier is working through the foundational assumptions for how the consensus policy requirements would flow to the various parties

associated with Privacy and Proxy Services, and also how those requirements would be enforced through compliance. IRT alignment on this flow of requirements will determine how the consensus policy is structured and drafted. And I'll get into more of that in a moment.

Next slide, please. Thank you for the link, Fabien. So, previously discussed accreditation models, which were presented to council included what was originally envisioned, which is a heavyweight accreditation agreement for all. A lot of work would have to go into this dedicated standalone program.

Then there were lighter weight options, a fast-track opt-in for registrars, a model where everyone was already in and had to opt out. And then there was an additional model which was floated, which was essentially no accreditation and would be a pass through to the registrars. A lot of considerations were taken on these in discussion with council and the IRT. And this serves as a foundation for the direction to go with the consensus of all parties.

Next slide, please. So, this fed into what you see here, which was just discussed earlier, which is looking at the foundational assumptions for what a consensus policy would look like. I'm not going to get into too much detail here, but essentially what does that flow of requirements look like?

Current thinking is that there would be a list of ICANN accredited Privacy Proxy Service providers. Registrars could opt in and opt out using registrar information specification data. So, that's how it

would be managed. And then through that, it would flow to affiliates, which in the context of this policy means a service that's affiliated with a registrar essentially to keep it simple.

And resellers in this context, a person that participates or organization in the registrar's distribution channel for domain name registrations. We're trying to include definitions specific to Privacy Proxy, but these also appear in the RAA. So, we're trying to ensure consistency across that. So, this is what is currently under discussion.

The team did reach alignment on how this should function at a high level and also what are additional considerations for how the language will read. So, this was a major milestone today. And in the coming weeks, which I'll get to in a second, the ICANN Org will develop a draft consensus policy and work through that with the IRT.

Next slide, please. So, upcoming work, this will be done through modules, as I mentioned earlier with the work breakdown, first through definitions, then through the meat of the consensus policy itself, then disclosure frameworks, and there will be a human rights impact assessment. And I'll get to the timing of this in a moment. But the consensus policy is targeted for Public Comment in December of 2026. So, trying to move quickly.

Next slide, please. What you see here is the current implementation plan. So, although it was active, I didn't try to get too far ahead of ourselves here. This was just achieved. So, the

flow alignment and the foundational assumptions were aligned upon. So, we are on target there. And we will be transitioning into drafting the consensus policy through the modules that I did just identify. And I do have highlighted here the Public Comment proceeding again, which is projected for December 2026.

When you do go to the wiki, you will see a link to something that's similar to this to keep track of where we are and if we're on pace to achieve our objectives. But we're moving forward quite well. The IRT is very involved, as I know Gabe and Owen can attest. And moving forward towards that timeline with pretty good alignment.

I do believe that that is the end of my slide. One more slide. I think I have a list of links. Great. So, these are just a list of all the links and the resources that I did go over. So, we'll stop here to see if there's any questions that I can help address. Thank you.

NICOLAS CABALLERO: Thank you so much, Jason. Hard work indeed. Let's pause for, let's say, we have five minutes for a short Q&A session at this point. Let's see if we have questions or comments in the room or online. I don't see any hand online yet. Let's see if we have questions. And I have Reg, is that you? Reg Levy, go ahead, please.

REG LEVY: Thank you. Reg Levy from Tucows and not a GAC member. I'm happy to cede the floor. I have a question for Owen from his introduction because he indicated that the use of Privacy Services

and of Proxy registrants has increased recently. And I don't see that as a provider of Privacy Services. So, I was wondering where that came from and what that, yeah. Citation requested. Thank you.

OWEN FLETCHER: Thanks, Reg. This is Owen Fletcher. This is, I'm not sure I used the word increased. I think I said have become very common. This is just something that I feel like if you talk to people in the community, you will hear said. And I'm not sure what kind of authoritative data might be out there about it. Presumably coming from registrars. But it would be interesting to know if anyone has data like that so it could be more solidly quantified. Thanks.

NICOLAS CABALLERO: Very quickly, Reg, go ahead.

REG LEVY: Yeah, Reg Levy again from Tucows. We've seen a decrease since GDPR in the use of our Privacy Services.

NICOLAS CABALLERO: Thank you, Reg. Well, noted. I have India next. Please go ahead, Sushil.

SUSHIL PAL: Thank you first of all, pardon my ignorance, but I was just wondering since we have GDPR and most of the Privacy protection

laws already in place in many countries, which is actually a fundamental right for the citizen. So, I'm actually wondering as to why this service should be there, I think. So, that's one thing.

I think just if someone can help me understand that better. I think, secondly, to Jason, actually, I mean, looks like a very hard work. If you could simply demystify for us as to what change this will bring, you know, I mean, without getting into the process and the mechanism of the ICANN, I think.

JASON KEAN

Thank you, India. I can't speak to as why this is needed at this moment, but in terms of what change this will bring, this has been something that's been accounted for in the RAA for quite a while. So, the placeholder language has been there, waiting for this accreditation to come through to have a little bit more consistency across the Privacy and Proxy Services.

So, that's one thing. And then also there's additional alignment with existing policies, namely reg data with disclosure and forward looking towards the SSAD and RDRS in terms of how Privacy and Proxy disclosure will fit in via policy. So, this is one piece of that puzzle.

NICOLAS CABALLERO

Thank you very much, Jason, India, is that okay? Microphone, please.

SUSHIL PAL

Maybe I'll connect with the colleagues later, although the first part has still not been answered. If someone can answer that as to if it is a fundamental right, right, I mean, why do we need these? Maybe Reg can clarify if it's okay for her, I guess, since she's delivering these services, I guess.

NICOLAS CABALLERO

Reg?

REG LEVY

Hi, everyone. Reg Levy from Tucows. We see a number of reasons that people may want to obscure their information online. I know that when I first registered my domain names, I had been a woman on the Internet for most of my life, and I knew that that was a dangerous thing for people to be aware that I am.

Now I do DNS Abuse mitigation, which includes pissing off some real nasty people for fun and profit, and so I continue to make sure that my home address is not available publicly on the Internet. A lot of human rights workers are using these services to make sure that they can utilize their free speech rights in a way that protects their privacy and their safety. Some people just don't want their information out there. Lots of data miners have lots of information about lots of people, and some people are becoming uncomfortable with that.

NICOLAS CABALLERO

Thank you, Reg. Is that an all-hand India? So, thank you so much. So, for the sake of time, we need to move on, and for that, I will hand the floor at this point to Gabe. I'm sorry. I'm sorry. David Bedard, who's going to walk us through, you know, some updates on LEA authentication with ICANN Org. Over to you, Dave.

DAVID BEDARD

Great. Thanks, Nico. And good morning, everybody. I'm David Bedard from the Government of Canada, GAC rep. So I'm here to give a bit of an update on the policy work that's being done on Urgent Requests for disclosure of registration data, and apologies if I speak too fast. I'll do my best to speak at a reasonable pace.

Great. So, just a bit of background on this, and I won't go into every detail, as it is a bit lengthy, but please feel free, I think you'll have access to these slides, please feel free to check out the hyperlinks if you want a bit more detail on the background. So, the issue of Urgent Requests for access to user data stems from an EPDP Phase 1 Recommendation 18, which called for a mechanism to handle Urgent Requests involving imminent threat to life, serious harm, critical infrastructure, or child exploitation, so very narrow circumstances of these requests.

During a 2019-2023 implementation stalled because the community really couldn't sort of agree on a response timeline, so after the GAC's August 23 letter, the ICANN Board decided

Recommendation 18 that outlined this needed to be revisited, and I think I'd really sort of want to put a point here that coming out of that, the parties agreed in October 2024 to move the work forward on two parallel tracks, so I think if you're walking away from this slide, that's sort of the crunchy bit that you'd want to know.

So, there was an authentication track, which was tasked to explore mechanisms to authenticate law enforcement requesters, sort of making sure those requests for urgent data that were claiming to be by law enforcement were actually coming from a law enforcement agency. And that work was being led out of our colleague in the PSWG.

And then there was a Policy Track, and this was to develop an appropriate response timeline for authenticated Urgent Requests, and that was established through an implementation review team.

So, after the registration data IRT restarted its work following ICANN83, the GAC weighed in during the Public Comment period last December, so we supported finalizing the process and confirmed that a 24-hour response timeline for Urgent Requests makes sense, except in genuine cases of force majeure situations. As we noted that this timeline should become enforceable as soon as a law enforcement authentication mechanism exists, again, that was being led out of the work of the PSWG, without needing more policy development.

So the GAC viewed the authentication mechanism as a precondition for implementing existing policy recommendations

on the need for a timeline. So, while we do have our bilat with the Board, I believe, later today, so we'll hear a little bit more about what they have to say to the GAC about this, however, we do know that here at ICANN85, discussions between the GNSO Council and the ICANN Board helped clarify how we get from here to actual enforceability.

So, on the timeline, the Board told the GNSO Council it supports moving ahead with the 24-hour response standard and publishing it as part of consensus policy. We also heard this in our bilat earlier with the GNSO, so I think that this is very encouraging. We're really seeing some momentum on it.

And then on the authentication, the Board suggested it would prefer to treat this as an implementation detail, perhaps through an IRT. The council, however, indicated it may lean towards a potential other option, potentially providing supplemental policy recommendations through the upcoming SSAD supplemental policy work, so hopefully we'll know in short order.

But basically, in short, there seems to be alignment on the 24-hour response timeline, and it appears that it is likely going to be published as consensus policy. So, the GAC will need to stay engaged and track the ongoing discussion about whether authentication is purely an implementation step or needs additional policy guidance. So, this is certainly something we can clarify with the Board later today. And I think that's it for the policy piece. Thank you, Nico.

NICOLAS CABALLERO Thank you so much, Canada. Let me give the floor at this point to Gabe, and then at the end of his presentation we'll take questions and comments. Gabe, all yours.

GABRIEL ANDREWS Thank you, Nico. This is Gabriel Andrews, for the record. And just to set expectations, I'm going to speak, and then we're also going to have my counterpart Matthew Errington of Interpol speak, and Eleeza Agopian of ICANN Org, all on the same topic of law enforcement authentication.

So to start off, let's flip to the next slide. As you just heard, we have been asked as the public safety Working Group of the GAC, following that trilateral agreement with the GAC, the ICANN Board, and the GNSO, we were asked to come up with options, come up with potential mechanisms, or just to help with the challenge of authenticating law enforcement requests.

Now this came out of the discussion of the Urgent Requests, but I happen to think that this is just useful in general, too, for other requests. It's helpful to know if someone claims to be police, that they actually are. We recognize this is important work, and so we've been working very hard since on this. That work has taken the form of creating a law enforcement authentication practitioners' group. It's just a way that we can keep the community abreast of the discussions that we're having.

And those discussions have involved feasibility discussions between the law enforcement agencies such as Interpol, my own in the United States, and with the staff at ICANN, whose cooperation is absolutely essential for this ongoing work.

Let's go ahead and flip to the next slide. Because we had the opportunity to talk about this in the meeting with the GNSO, I'm going to just succinctly remind you, we're talking about two potential mechanisms that could be helpful for this. The one that we are getting consensus from the community around, or at least that's how I'm interpreting it, is that the long-term mechanism we're discussing is going to be necessary.

This is the mechanism that we contemplate where employees will go through either existing or aspirational law enforcement portals to connect to ICANN, the RDRS, and then an authentication token being passed to them will accompany the RDRS request thereafter.

The other mechanism, next slide if you would, was also contemplating whether or not it would be helpful if we can, as law enforcement agencies, give to ICANN and the contracted parties lists of all the known law enforcement agencies that we can easily put together in a list and their known email domains that they use.

And that was thinking that potentially it could be helpful if those contracted parties are getting a request from some agency, they're not familiar with, at least they can check against that list and see, well, this matches or it doesn't match. This isn't the same as the

authentication mechanism just discussed, but I want to just make clear that we're exploring both options.

Now, I think it would be very helpful now to be able to turn the floor over to my colleague, Matthew Errington of Interpol, who is connecting at 6 a.m. his time, so thank you, Matthew, for getting up so early. And thank you again for connecting and being able to share Interpol's thoughts as you create your own law enforcement portal. And I look forward to hearing more about it.

MATTHEW ERRINGTON Thank you, Gabe, and thank you, everyone, for hosting us. Again, my name is Matthew Errington, and I'm a Product Manager at Interpol based in Lyon, France, the Secretary General. For those of you who may not be familiar with Interpol, our role is to enable police around the world to work together to fight international crime. And with that comes a truly global structure.

We work with 196 member countries who each maintain an Interpol Bureau around the world. You can see some of the offices here based in Lyon and Singapore. And then we have six regional bureaus, three liaison offices, and three representation offices.

Our national central bureaus act as a center through which international police cooperation is steered. They are the essential link between police in the field and the global law enforcement community. All of them are connected via an I-24-7 secure global

communications network that provides access to all of our databases.

And these offices are often connected to the ministry in charge of national law enforcement or the national police body and work directly with all domestic police agencies internal to that member. They contribute to our global criminal databases on behalf of their society and cooperate together on cross-border investigations, operations, and arrest.

Our national central bureaus in different countries have different structures, capabilities, authority, and are subordinated to different agencies. But they all have one common thing in mind, and that's to fight global crime. Our governance is made up of the General Assembly. It's our ultimate decision-making body, and it meets annually. And all countries participate. And we have a 13-member executive committee, which meets several times a year.

Our main product is our Interpol notices, which are requests for information or cooperation or to warn of threats. You may have seen some of these in the past. And where does that bring us with law enforcement authentication?

Interpol has been a long-standing member of the Government Advisory Committee. And we want to be able to think through how we can leverage our global network of 196-member countries, sub-bureaus, and regional bureaus to help be a point of contact within each country when registries and registrars have difficulty

understanding if a person making a request is, in fact, genuine law enforcement or not.

So right now, Interpol is building a secure and user-friendly platform to enhance law enforcement ability to cooperate and share information and access specialized tools and applications. So, we hope there'll be some goals here to improve response to global threats, enhance operational efficiency, strengthen collaboration and data sharing, simplify access to specialized applications, and ensure the security of sensitive data.

Now, all of this is governed by strict guidelines through our point of contacts, the National Census Bureaus, who are governed by our Constitution, our rules for the processing of data, our General Assembly, and must respect the UN Declaration of Human Rights.

So, we thought of a very similar workflow to what Gabe just shared. So, thank you, Gabe, for sharing those slides just a few minutes ago. But we have the idea that authentication at a global scale would look like a local law enforcement officer making a request through their hierarchy, seeking approval from the manager, who would then federate that request to either regional or national police, who would then authenticate to Interpol's identity platform. That would allow them access with specific permissions to access Interpol services, or in the case of ICANN's context, to make a verified or an authorized access request on the RDRS system.

So, this is how we want to leverage the existing network that we have. In terms of strategic phases, right now we're looking at doing

a technical SAML integration as a pilot between a few of our member countries with ICANN and setting up the appropriate legal frameworks. Step two would be to onboard Interpol's membership, so our 196 member countries. Then we would look to encourage national central bureaus to partner with local law enforcement agencies.

And final stage would be to continue to improve the authentication and authorization mechanism. So, just want to thank you for your time. If you want to see our list of member countries, there's a link here. If you have any questions, this is the email to the product that I'm working on now. Thank you for your time.

NICOLAS CABALLERO: Thank you so much. But please stay online in case we have questions here in the room or online. Thank you so much. Again, we have a good10 minutes for a Q&A session right now. Unless, Gabe? Oh, sure, sure, sure. We can go to Eleeza. Yeah, yeah, yeah. Sorry. No problem. Eleeza, over to you.

ELEEZA AGOPIAN: Thank you, Nico. Thank you, everyone. My name is Eleeza Agopian. I'm the Vice President for Strategic Initiatives at ICANN. And my team is leading our RDRS Project Initiative. And as part of that, we've been conversing with our colleagues here about how we could potentially test authentication mechanisms with RDRS and,

of course, how that fits into this broader discussion about Urgent Requests.

So, I'm here to share with you a bit of an update on where we are and how ICANN has participated in these conversations. So, as David explained very well at the beginning, the Board split up work on Urgent Request into two tracks at the GAC's request.

The first track, which was focused on a timeline, we believe is now complete, as you know, and we'll be discussing today with the Board. The second track, of course, focused on authentication mechanisms. So, as mentioned, the Urgent Request timeline, we believe, and thanks to the GAC for participating in these discussions, is now settled at a 24-hour timeline.

And our team now is working on a timeline for updating the registration data policy to include that. But importantly, that timeline, though the policy work is complete and we've agreed upon a timeline, we also agreed that it couldn't be enforced until an authentication mechanism is in place. And so, in parallel, we've been having these conversations to understand what is out there.

We've learned quite a lot from both Gabe and Matthew, and thank you for that. In terms of what's available and how it could potentially work, at least with RDRS in a test situation, until we have completed policy for an SSAD or whatever a long-term mechanism might be for requesting registration data. So, as Gabe shared, we've been participating in conversations with the law

enforcement practitioners' group within the public safety Working Group.

We really joined these conversations to learn more about the technologies, and as I said, we've learned quite a bit. We've asked process and operational questions and have really heard from the community members who have participated. So, not just law enforcement, but we have registries, registrars, civil society, others from across the ICANN community participating to understand what their desired features are for an authentication mechanism.

So, based on these conversations and what we think we're hearing from the community, we're really committed to continuing in the discussion with both Interpol and FBI and anyone else who has available authentication mechanisms. I think to cover this on a global scale is a big challenge. There is no one agency that can do that.

So, the more we learn and the more we engage with trusted partners, I think is helpful for all of us. Particularly, we're working toward what we hope will be a live proof of concept. And when I say live, that's really just a test bed for us to understand how the connection would work, what information ICANN could receive, and go from there. That would kind of allow us to identify requirements for any identity providers, whether it's FBI, Interpol, if another agency comes along and is interested.

Once we have policy and both clear policy requirements as well as technical requirements, we don't have a clear picture of that just

yet, that would allow us to publish those and potentially onboard a broader swath of identity providers. So, as I said, we really appreciate the willingness of anyone to participate and I welcome conversations with anyone in the room here today or online. And of course, we're also very interested in hearing the community's input in all of this as well.

So in terms of what we have discussed with FBI and Interpol, we're asking a number of questions and some of these are coming from our community members. So, for example, who has access to the tools in question? Matthew just spoke a little bit about that now. But in other words, how does an identity provider verify that a user represents a law enforcement agency? How are those agents vetted or audited and how often? That's a particularly important question. What information from the tool, from that actual authentication tool, could or should be passed to a registrar together with an authenticated request?

And lastly, and I think this is particularly important both for the requesters and for the registrars to understand, is how do we make it clear that use of this system is not equivalent to authorization for registration data disclosure? So, as we all know, per ICANN policy, registrars must still assess each request to determine whether or not to disclose the registration data.

Of course, with an authenticated request that provides a certain level of information that currently doesn't exist and could be very helpful to registrars is what we understand. So, ICANN is

committed to continuing to facilitate an open and transparent dialogue on this. So, we really recognize the importance of this, particularly to get us to an enforceable timeline. I know we've agreed on the timeline. We want to make sure we can enforce that in a clear way.

And so, in addition to the long-term mechanism, as Gabe shared, there is a short-term mechanism is what we're calling it, which would not be authentication. We should be very clear about that. It would provide additional information for registrars, which some registrars have shared with us could be helpful. But we still have a few questions about it. And we also want to be sure that the registrars who would receive requests that have validated domains, as Gabe described earlier, are receiving these in a way that provides them with information that they understand and can use.

So to confirm this, we actually sent out a questionnaire to registrars who are currently participating in the RDRS, which is still voluntary. I'll remind all of us here. To help us determine whether the investment of resources to implement this domain validation mechanism would be worthwhile, we received feedback from two registrars and the Registrar Stakeholder Group, which indicated that registrars broadly agree that the law enforcement email domain validation process has some operational value and would be helpful if limited, helpful or, sorry, it would be a helpful if limited incremental first step.

The registrar has also noted to us in their feedback that the process does not verify proper authority, jurisdictional standing or legal basis to request nonpublic registration data and would need a clearer accountability framework, governance and stronger security concerns. So, we got a pretty good range of feedback from just three groups. And I've heard a little more discussion about it in the hallways this week.

So, we would welcome that conversation to continue with us as well as in the law enforcement practitioners' group so we can determine how to move forward. And I'm happy to answer any questions. Sorry for speaking so fast.

NICOLAS CABALLERO Thank you very much, Eleeza. So, let me open the floor for questions or comments at this point, both online and in the room. And I do have a question already, if you don't mind, of course. I assume that the system will be using open standards. I'm asking you this because let's say the case, let's say the government of Annapurna or Antarctica wants to participate and wants to communicate with the FBI's system, the U.S. system or the Canadian law enforcement system.

Would that law enforcement agency from Antarctica be forced to use a new version of Postgres that was bought by some super millionaire? I'm asking you this in terms of interoperability, which

would be a concern. What are the standards that you're previewing to implement the system?

ELEEZA AGOPIAN

So, this is Eleeza Agopian speaking again. Let me start by saying I am not a technical member of our team. We have technical staff here. But a couple of points I want to make, and I think Gabe and Matthew hopefully can speak to the standards in their system.

So, RDRS is obviously a web-based system that we're offering to the community for requesters and registrars. On the registrar side, we're using ICANN's NSP Naming Services Portal. But in terms of the actual technical standards and how the system would integrate and work, we mentioned for the pilot, we're looking at a SAML authentication token.

And part of the whole purpose of this test is to define the requirements and how it would all work. So, I'm going to stop there before my technical colleagues get upset with me. Go ahead, Gabe.

GABRIEL ANDREWS

Yeah, I'll jump in here, too. I think the key piece is that, yes, to your point, Nico, we're not recreating wheels. There are two different technical authentication protocols that are being discussed. SAML is one. I think the other is called OpenID Connect. Like Eleeza, I'm not an engineer. I just have to talk to them a lot. And this is what eventually penetrated my thick skull. But they are using these

standards that any other entity that wants to act as an identity provider for their members should also have available to them.

And once we pave this path and show that, yes, it works and do the work of helping to set both the technical and the identity provider agreement template, we hope that this will be replicable by others, right?

And so, you mentioned Antarctica. If there's an Antarctica law enforcement agency that wants to do the same for the polar bears and penguin constituencies, that they will be able to do so just by following the same path, by adhering to the same agreements. And thus, it should be, in a perfect world, scalable beyond just the first two parties that you see on the screen testing now of the U.S and Interpol.

NICOLAS CABALLERO Perfect. Thank you so much. So, I assume it would be kind of like a GPL license, GPL-V2, GPL-V3, something like that?

GABRIEL ANDREWS See, now you're already more technical than me.

NICOLAS CABALLERO Anyways, thank you so much. I have India next.

SUSHIL PAL

Thank you. I understand that we have some kind of a consensus regard to the 24 hours timeline. But I think it would be an inactive recommendation, so as to say, because the second track, I mean, which the IRT split into, I mean, because that is not final yet. So, we're more interested to know as to how does the authentication track. Thank you, Gabe, for sharing this.

The two models both seems fine. But then how would this go in the ICANN process? Will it go through the implementation recommendation? Will it go through supplemental recommendation? Will it go through another IRT or through another PDP process? Because, you know, I mean, that's what I'm interested in, which one would work faster and what time frame we have in mind.

GABRIEL ANDREWS

Hi, this is Gabriel Andrews for the record. So, the work that we're doing to have engineers talk to engineers and to do the testing doesn't have to be limited to whatever policy discussions are occurring. We broke that apart to try to enable the technical discussions to proceed on their own timeline as fast as possible.

Now, it's not instant. But we're having those discussions and then that will presumably involve later this calendar year, we hope, the ability to start testing and actually sending the protocols and prove that it works. This is what we're referring to as the proof of concept.

Now, I think Matthew had a very useful slide on his presentation about where he envisions the Interpol piece of this to continue from there. But there will be opportunity, I feel, the most important message I want to give you is there will be opportunity for you to engage your respective national central bureaus to make them aware that Interpol is standing up this service that could help them with the challenge of connecting and authenticating to RDRS.

Start contemplating how you might reach out to those entities if you have questions about how to do so. Matthew and I can help with that. The thought, though, is there will probably have to be some amount of user education and getting the people that are familiar with ICANN talking to the people that are familiar with the national central bureaus and Interpol and how you would connect.

I think that's valuable. But I do not see, to your point about where this fits in policy, I do not see policy being a roadblock to any of this. This is proceeding as fast as we can to establish the technical means, and that's why I think we were splitting those two tracks apart. I hope I answered your question, though.

SUSHIL PAL

I think most of the agencies from various countries, they're already communicating on a daily basis with Interpol, right? With regard to sharing lots of other data, I think that's a very pretty established process as regards Interpol is concerned. So, now Interpol only has to hook on to the RDRS. That's it.

So, I guess the technical part is not that big a challenge. It's already going on, right? It's only plugging in in the RDRS, which is, but that, I don't think, I mean, maybe Dave can answer that. Maybe that lies within his domain. Will that have to go through which process of ICANN, another IRT or another PDP? God knows. Or, you know, once that's demonstrated, it's done, and the Board is on that. I mean, that clarity, that's what we need.

DAVID BEDARD

Yeah, I think that's a good question, and I know that I touched on it a little bit during my remarks, but I think it's still an ongoing question on whether it will need to be part of that SSAD revisitation or if it will actually be an IRT. It's certainly something that we can ask the Board whether that's --

SUSHIL PAL

Sorry. No, please. Sorry. But that's where we should hit on, right? Technical part has never been a challenge. We are already moving everything on a very sequential basis. We started with the Urgent Request. We broke into two activities. We make it two sequence. We solve one sequence with 24 hours timeline, which completely remains unimplementable because we haven't solved the second sequence now for the authentication.

So, I completely appreciate Gabriel's approach for testing it on technical basis. But then, by the time we do that, meanwhile, we should have a full clarity as to how quickly we implement through

the ICANN process. Otherwise, that will be another sequential step, which will go down for another one and a half year. Just emphasize that. Thank you.

NICOLAS CABALLERO: Thank you. Thank you so much, India. Thank you for the comment. We don't have an immediate answer right now. But certainly, the point is well noted. Thank you so much. So, moving on and switching gears a little bit, we're going to be talking about registration data, I mean, RDRS and SSAD next steps. And for that, I will give the floor at this point to our esteemed colleague from the European Commission, Gemma Carolillo. Over to you, Gemma.

GEMMA CAROLILLO: Thank you very much, Nico. I hope you can see me and hear me correctly. This is Gemma Carolillo from the European Commission. I take the opportunity that I'm taking the floor on RDRS and SSAD, but also to reply to our esteemed colleague from India that this is precisely an Urgent Request where we are hitting on.

The colleagues from the GAP who are involved in this process are really, as David presented, raising the questions on the follow-up on the authentication mechanism with the Board, with GNSO, and with all the appropriate counterparts.

Now, we move to a topic which is a bit of a bridge between history and future. Allow me to say that, because the issue of having a system inside ICANN for ensuring that the requests on registration

data are properly channeled is there for a long time. The SSAD, which is the system for standardized access/disclosure, is the result of one of the expedited policy development processes on registration data. Now, we are discussing about the evolution between SSAD and RDRS, which is the system for requests. There is not any longer the reference to the access, because this is not a part of the system.

There have been recent developments. So, the RDRS, the system for the requests from requestors to contracted parties, in particular to registrars to access registration data, has been there for two years as a pilot. It's been tested. It's been analyzed. There's been monitoring around its functioning. And at the end of this pilot, the two years pilot, precisely at the ICANN84 in Dublin, the ICANN Board has resolved to continue the operation of RDRS for up to two years.

Also, because there was something pending, which was the deliberations of the communities regarding what to do with the SSAD, which is the system that has been approved, in a way, as part of the policy recommendations.

Now, the GNSO Council and the ICANN Board have, in the meantime, been discussing what are the next steps concerning the SSAD recommendations. There is a whole set of documentations about that. But where we stand today, there was a set of important recommendations which define the characteristics of the SSAD

system, that these are to be considered as the parts that the community has agreed upon.

Given the results, the assessment of the RDRS, it has been recommended that the SSAD recommendations may be revised. So, this means procedurally, in ICANN terms, that the ICANN Board would not adopt the pending SSAD recommendations. And this is done following two procedures which triggers ICANN by-laws. You have the references on screen, Annex A, Section 9.

The idea is not to discard the SSAD recommendations as such, but the idea is to give the opportunity to the GNSO Council to provide what are called supplemental recommendations. So, in the meantime, based on the results of the RDRS pilot, the idea is to improve the recommendations stemming from the EPDP Phase 2 process.

Now, what is important is indeed that this is not coming out of the blue, but there has been, as I say, the process of evaluation of RDRS. The standing committee on RDRS, which also saw the participation from the GAC, has elaborated a series of considerations on what works, what doesn't work, what would be in line with SSAD, what would not be in line. So, all this work that has been done in the meantime will serve as a basis.

What we still don't know is that how precisely these next steps will be taken regarding the SSAD recommendations. This week, on

Thursday, the GNSO Council will hold a session to discuss what these next steps are, and so we'll be able to know more.

We can go to the next slide, please. So, what is important from the GAC perspective? We have been providing comments to the RDRS review. We have also been providing comments to the policy gap analysis, which assess how much of a difference there was between the SSAD objectives and what the RDRS could actually deliver and what would be needed to bridge that gap. But we have been expressing the interest from the GAC to be involved in the drafting of the SSAD supplemental recommendations in any way that is appropriate, compatible with the way of working of the GNSO.

We have also raised this point specifically in the meeting with the GNSO on Sunday, and we have got a positive reply that the GNSO intends to keep involved all the interested communities in the definition of the supplemental recommendations. We also heard an encouraging message that this should not be a very long process.

So, we will continue to bring the public policy perspective in the production of the supplemental recommendations. If you can go to the previous slide, just to point out that this has been expressed in a really long series of GAC positions that were discussed in this group and presented to the attention of the GNSO, the Board and the wider community. Now, what has been the main gist of the GAC position?

Next slide, please. Thank you. So, we have developed over time as a group a position, first of all, on what is happening now. The RDRS is continuing for up to two years, and we have stressed that it is really important that while it continues to be in operation, it's important to enhance the system. We are talking about technical enhancement, but these are important to the fundamental goal that this system is useful.

It's useful for those who need to send over the requests, and it's also useful for those who are receiving those requests. This in particular concerns the better integration for the registrar systems and the request for systems with the whole portal, and also to ensure that there is a better user experience and to reduce user friction.

So, the ultimate goal is that we have in place a system that works. We have seen over time a decrease in the use of RDRS from the requester side. We have also seen reduced interest from the registrars to participate in the system, which is today currently voluntary.

We have really made the point several times to the ICANN Board to ensure that the system be improved now. Then there are, of course, I would say the final objectives concerning how the request and access system should look like. This is very important to note that there seems to be a shared vision with the ICANN Board, as it's been expressed by several locations, that we have in place a system that foresees mandatory registrar participation, because we

cannot have a system that is a tool that serves to implement part of the registration data policy, and hence it cannot become an obstacle to the implementation of the registration data policy.

There needs to be complete participation of the ecosystem to the system in order to make it work. Also, it's important, and you have heard about the developments on the Privacy and Proxy Service policy work, we think it's important there is a requirement for registrars to also respond to RDRS requests for the underlying Privacy Proxy customer contact data as part of their disclosure decision process.

Let me stress again, this is a disclosure decision. It's not an automatic disclosure, but it is important since there is a big part of the registration data that is covered by Privacy and Proxy Service that the accredited Privacy and Proxy Service are connected to the system. It is important that the RDRS links with ARDAP, which is, of course, the technical protocol for what we have always known as WHOIS, to promote awareness.

And also, this is something which we have proposed for a long time as optional, and we have discussed with the ccNSO, we have discussed sometimes with our own country code top-level domains to have the option so that it is technically feasible for country code top-level domains to voluntarily participate in the system, because we have seen from the analysis of the functioning of RDRS to date that there is a good number of requests that

actually cannot be fulfilled because they are addressed to the wrong actor, so the country code top-level domains.

So, this is where we ultimately want to end, and as I said, we are positively reacting to the fact that the Board has expressed similar goals for the system. We are going to have a question to the Board today. This topic is on the agenda for the ICANN Board today, where we are going to hopefully receive more updates in terms of where we stand in the announcement of the systems, and also where we stand from the ICANN Board perspective into completing the work, including for having supplemental recommendations in place. So, this ends my update, and I give back the floor to the Chair in Mumbai.

DAVID BEDARD

Thanks, Gemma. Really appreciate the update. I guess the Chair just had to step out for a moment, but I guess we can open the floor for any questions that folks might have at this time. Okay. I see no questions online or hands in the room, so we'll move on to considerations for ICANN85's Mumbai communique.

Next slide, please. So, we had discussed within the small group, and this is what we were sort of envisioning in terms of communique topics, so issues of importance for the GAC. This shouldn't be too surprising for folks that have been around the GAC for a little bit, but we were thinking on having text on Urgent

Requests, specifically the timeline and the authentication mechanism.

And then RDRS/SSAD next Steps, and PPSAI. And I just do want to note just a small bit on the accuracy component. Some of you may know that or may have noticed that it wasn't in our slides here. It's certainly something we continue to track. As we heard in our bilat with the Council a couple of days ago, they are working out a methodology for prioritization of their work, and they did specify that this will include the recommendations to examine the 15-day verification timeline.

So, we are certainly tracking that, and we know that it was included as part of the Small Team's work on accuracy coming out of that group. So, it does remain a priority here, and it's certainly something that we're tracking. But in terms of communique text, this is what we're presenting to our colleagues for consideration, and I think I will conclude with that in terms of this agenda point and see if anyone has any questions. Thank you.

NICOLAS CABALLERO Thank you, Canada. Questions? I see a hand in the room over there. Please just grab a microphone and go ahead.

MACIEK PIASECKI Maciek Piasecki, not a GAC member. I'm from EURALO. So, a question regarding the ICANN bylaws and the commitment in Article 1 to follow local laws.

I wanted to highlight that in Poland in 2020, when citizens were executing their constitutional law to express in mass gatherings, law enforcement was conducting hundreds of arrests, and in more than half of these cases, the Polish courts have ruled that this action was either not based in the law or explicitly illegal.

So, since the local laws have been broken in these cases, I wanted to know how ICANN will be monitoring these kinds of illegal actions by the law enforcement, and since this is very important to the users.

NICOLAS CABALLERO: Thank you for the question. We certainly cannot speak on behalf of ICANN Org, that's for sure. But other than that, I don't know if any of my distinguished colleagues would like to say anything in that regard. But right off the bat, I can tell you, we cannot speak on behalf of ICANN Org. That's an internal legal issue. Sorry, but I cannot help you at this point. And by the way, we're not familiar with that particular case. Sorry about this. So, thank you. The floor is still open for --

MACIEK PIASECKI: Just wanted to say, I'm happy to provide you an executive summary of this.

NICOLAS CABALLERO Oh, for sure. For sure. Thank you. And I see a hand from India. Please go ahead.

SUSHIL PAL Just to clarify from David, if it is about the issues of importance for the registration data, right? Then, because accuracy has been coming up regularly in the issues of importance. So, would request for inclusion of that, at least here, or maybe that's already being considered in a separate heading under the GAC?

DAVID BEDARD Yeah, thanks. I think it could be DNS Abuse or reg data, but certainly something that we did get that accuracy kind of update from the GNSO with our bilat a couple days ago, just in terms of the work on the verification timeline.

NICOLAS CABALLERO Thank you, India, for the question. Thank you, Canada, for the answer. The floor is still open. Any other question or comment? Okay. I see no hands online and no hands in the room. So, we're going to move on to the very last topic, which is topic number five, right? And for that, I'll give you back the floor, Dave.

DAVID BEDARD No, we did it.

NICOLAS CABALLERO: Oh, okay. Okay. Sorry. I just left the room. Okay. So, we're good then. Is there anything I'm missing here? Anything you would like to add, Dave? Sorry. Fabien, go ahead.

FABIEN BETREMIEUX: Thank you, Nico. Fabien Betremieux from the GAC support team. Just a quick comment.

Since we have a bit of time before the end of the session, and given that this afternoon, the GAC will start to draft its communiqué, from a support perspective, we'd like to suggest that this is probably a good time for those GAC members that are interested in contributing to potential communiqué text to let themselves know so that you, as topic leads on registration data, can potentially involve those participants. So, just a suggestion from a perspective of an efficient drafting of the communiqué.

NICOLAS CABALLERO: Thank you very much, Fabien. Well, noted. So, please feel free to -- they can provide the input directly on the link you circulated before. Is that correct, Fabien?

FABIEN BETREMIEUX: So, what we've suggested over the past few meetings is that those members interested in contributing to initial text connect with the topic leads to ensure that we do not enter communiqué drafting with two versions of potential text, and instead with an already --

so, initial text is already a level of consensus when we do consider the text in communiqué drafting sessions. Thank you.

NICOLAS CABALLERO: Thank you so much. Very good idea, indeed. And we can do that as a matter of fact, right now, we can wrap up the session and then they can approach the topic leads right here in this room. And other than that, I think we're okay to close the session, unless you have anything to add, Gabe? Owen? All good?

Any final comments or questions before we wrap up? I see no hand online. And no hand in the room. Okay. So, thank you so much. Please feel free to approach the topic leads in case you have text for the communiqué.

Thank you very much. And I'm giving you, yeah, a good 20 minutes extra for lunch. We'll reconvene. Let me see. Yeah, please be back in the room at 1:15 after lunch. Sorry, Janis, is there anything you would like to say?

JANIS KARKLINS: Yeah, thank you very much. I just would like to remind that at 12 o'clock in this room, we will gather all African GAC representatives for a brief conversation. For all African GAC representatives, please be back in this room at noon. Thank you.

NICOLAS CABALLERO	Thank you, Janis. Okay. So, with that, enjoy your lunch. Oh, there's one hand from Egypt. Okay, Egypt, please go ahead.
CHRISTINE ARIDA	I have a quick question. Are we going to have remote participation for the GAC Africa session at 12?
JANIS KARKLINS	Sorry, I made a mistake. African GAC representatives meet in this room tomorrow at noon. My apologies.
NICOLAS CABALLERO	Okay, I hope that helps, Christine. Okay, so thank you so much. The session is adjourned. Enjoy your lunch.

[END OF TRANSCRIPTION]