ICANN80 | PF – GAC Discussions on DNS Abuse and WHOIS
Tuesday, June 11, 2024 – 10:45 to 12:45 KGL

JULIA CHARVOLEN: Hello and welcome to the ICANN80 GAC Discussion on DNS Abuse Mitigation session on Tuesday, 11 June at 8:45 UTC. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior.

During this session, questions or comments submitted in the chat will be read aloud if put in the proper form. Remember to state your name and the language you will speak in case you will be speaking a language other than English. Speak clearly and at a reasonable pace to allow for accurate interpretation. You may access all available features for this session in the Zoom toolbar. And with that, I will leave the floor to GAC Chair Nicolas Caballero. Thank you and over to you.

NICOLAS CABALLERO: Thank you very much for that, Julia. Welcome everyone to this session on DNS abuse mitigation. I have the pleasure to welcome Martina Barbero from the European Commission, Susan Chalmers from the United States, Nobu Nishigata from Japan, and the guest speakers, Ms. Tomboye Ibrahim, who's online, if I understand correctly, Director of Domain Names, Information and Communication Technologies Development Agency of the Republic of Chad, Mr. David Kanamugire, and I hope I'm pronouncing the last name well, who's the Chief

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

Executive Officer, the CEO of the National Cybersecurity Authority of Rwanda, and Mr. Barrack Otieno, General Manager for the Africa Top-Level Domains Organization.

We're going to be talking about current trends in DNS abuse on the one hand, policies regarding DNS abuse on the other hand, and possible solutions and next steps. And right after that, we'll get to the Q&A session with GAC members and I'll open the floor for comments, questions, or any thoughts you might have at that point. Hopefully we'll have enough time. So, without further ado, let me give the floor to Mr. Nobu Nishigata from Japan. Nobu, over to you.

NOBU NISHIGATA: Thank you, Chair. Hello everyone. Good morning, good afternoon, and good evening, according to where you are. My name is Nobu Nishigata. Thanks for the introduction, Chair. I'm a GAC representative from Japan and I do the intro of the GAC plenary session on DNS abuse.

Let us recall that the previous ICANN meeting in San Juan, we had a very fruitful discussion on this matter, including Q&As, and thanks to the ICANN Compliance team. And it was right before the amendment of the registry agreement and the registrar accredited agreement took effect. And one of the highlights was the presentation from our colleague from the United States, FTC, Laureen Kaplin. She presented the current situation of the online flows in the United States, and thanks again to Laureen. I don't know where she is, but [foreign language 00:02:57]. It's thank you very much, alright?

Today, since we've got only 45 minutes, so the colleagues just introduced, Susan, Martine, and myself, decided that we should take this opportunity the most, the opportunity that the ICANN meeting being held in Africa. So, thanks to the Rwandan government, and this session aims to be an opportunity for us to learn from African colleagues how they fight or combat, mitigate, and prevent DNS abuse.

So, there should be commonalities and differences compared to what we are doing in the capital, but that there will be the great sharing for us, and the colleagues hope that we can take away some learnings from them. So, we have three distinguished panelists today. Two are on the stage, and one is from online. Welcome to the session, and we appreciate your participation again. [Foreign language 00:03:53]

Today's plan is that, just briefly introduced by chair, but we start by each panelist for offering remarks. Then the panelists will present three aspects regarding the DNS abuse in Africa. The aspects are that the number one is a trend and cases of DNS abuse in Africa. Number two, it's a policy and a solution here. Then number three, the proposal or suggestion to the next steps for the GAC and ICANN from their perspective. So, after the presentation, we open the floor for questions and discussion, and including the discussion on our next step of the DNS abuse discussion in GAC. So, without further ado, I turn to Susan to moderate the session. Thank you.

SUSAN CHALMERS: Thank you kindly, Nobu. I think given our time constraints during this meeting, we'll just launch right into opening remarks. Do we have our colleague Tomboye on the line? Yeah. Okay. Hi, Tomboye. Would you please, over to you. We'll hand the floor to you.

TOMBOYE IBRAHIM: Good afternoon, everyone. Hope you are enjoying your stay in Kigali. I am a little bit sad to not be there in person with you, but I wish you a good stay in Kigali, and I hope that we will have more opportunities to host ICANN meetings in Africa. Let me take the opportunity to thank the team for inviting me for this panel. And as usual, it's always a pleasure to be in the GAC meetings and to be here with you, even if remotely.

Thanks to the ICANN diversity of language, I will switch in French. My name is Tomboye Ibrahim. I am the Director of Domain Names and IP Addresses at the ICT Development Agency of the Republic of Chad. We are a body which operates under the ministry in charge of digital economy. We also manage our ccTLD, the .td, since 2016 on an administrative level and technically from 2019, thanks to a technical partner.

Today, I will address the trends in terms of DNS abuse in my country. Also going to look at the different attacks that are perpetrated against our ccTLD. I'm happy to learn about colleagues from neighbouring countries to know if they have certain trends or if they have also undergone DNS abuse attacks on their ccTLD. I reached out to a number of countries, and only one of them has an operational website, and I will share the data that they've given to me.

We've also carried out proof-of-concept studies, and in some cases, the regulator or IT regulation agencies were able to intervene, but we did not have any further information for these other countries because we had to reach out to other entities, and I did not have the contact details of this agency. As for Chad, we have an agency for digital certification and IT, and this agency has uploaded a form that allows people to register attacks. However, this service is not widely used, and we do not have enough reporting. Further down the line, I will address this a bit further.

SUSAN CHALMERS: Thank you, Tomboye. Just to confirm, okay, I think we'll circle back to you after opening remarks, but thank you so much for that introduction. Again, Ms. Tomboye Ibrahim, Director of Domain Names, Information and Communication Technologies Development Agency of the Republic of Chad, and a GAC colleague. Now, I have the pleasure of turning to Mr. David Kanamugire, Chief Executive Officer of the National Cyber Security Authority of Rwanda. We're so pleased that you could join us today. Please, over to you.

DAVID KANAMUGIRE: Thank you, Susan, and thanks, everyone. I can clearly see Charles listening in Kinyarwanda helped the panelists spelled my name right. So, thanks, Charles, for the introduction lesson. But what I can say at the beginning is our pleasure to really host this distinguished meeting. We acknowledge the critical importance of really governing and securing DNS infrastructure as vital to internet as we know it.

But I think this is particularly important for Africa because as a country that is quickly relying on internet to do most of the services that did not happen in the past, we're becoming increasingly reliant and dependent on it. So, our ability to really secure DNS infrastructure is vital for young economies that are quickly getting online, but that also brings a lot of challenges. One is that even though we are increasingly becoming reliant on DNS infrastructure and security, we do not have commensurate capacity to guarantee any of the challenges we see in abuse. So, that is already one big gap.

But we're also concerned greatly because even the traditional DNS abuse problems which were already hard to grasp with are now being increasingly sophisticated due to the new technologies, particularly AI, other means of abuse that are now being super complicated, both in scale and in scope, and the ability to even not be able to pinpoint what nature of abuse is. So, I think maybe in further discussions we'll look at the challenges of even being able to accurately define what type of DNS abuse that is. Some abuse that could be one type will now come as another, so there is also a challenge of accurately identifying which type of abuse, how to mitigate it, and now not having the capacity to deal with it.

So, we really look forward to this increasingly important discussion, and I hope maybe through these discussions the trends that we have seen in the past are likely not to be the trends that are going to continue into the future. How do we then migrate from the traditional well-known DNS abuse threats to one that are going to be fully automated, highly sophisticated, and very powerful? So, I don't have answers, I don't think we even have statistics, but we are increasingly getting scared when a lot of our national assets and economies and resources are so dependent on this infrastructure that we don't have full capacity to protect and control.

So, I don't have answers, but I'm really eager to learn from all the participants on how we as Africans, and a couple of our colleagues, can now tailor our policies to deal with these increasingly sophisticated challenges. So, we really thank the opportunity to be here in the room and look forward to hear from our other panelists. Thank you.

SUSAN CHALMERS: Excellent. Thank you so much, David. And now let's turn to Mr. Barrack Otieno, General Manager, Africa Top-Level Domains Organization. Over to you, Barrack.

BARRACK OTIENO: Thank you, Susan. And good morning, good afternoon, good evening, everyone who is following this conversation. With respect to the subject at hand, a lot is happening on the African space. Firstly, let me give a brief introduction in a minute of Africa Top-Level Domains Organization.

Of course, it is the regional association of country code top-level domain registries. In the last 13 years, we have been working specifically to ensure that African country code top-level domain registries are run in a secure, stable, and resilient manner. Before 2010, over 50% of African country code top-level domain registries were actually run outside the African continent. And we came up with a strategic plan with a deliberate intention of bringing the management of these country code top-level domain registries into the continent. And I'm happy to report that as we speak, over 85% of country code top-level domain registries in Africa are now run from within the continent.

The other issue was many of them were manually run as per a study that we did in 2008 conducted by Dr. Paolo Nyirenda, one of the executive committee members of Africa Top-Level Domain's organization. We found that most of the country code top-level domain registries were manually operated. And we also sought or embarked on a journey of automating this country code top-level domain registries. And I'm happy to report that with the support of the Internet Society, ICANN, and many other partners, again, over 90% of this country code top-level domain registries are now operated with automated systems.

And our current focus is on sustaining them. Our current focus is on building a local Internet value chain. And with this, we get to have issues of DNS abuse. So, I don't know whether I'll be going ahead of myself, but in preparation for this conversation, AFTLD did a desk survey. As we know, DNS abuse is an evolving conversation or something that keeps mutating on a daily basis. And we reached out to 12 country code top-level domain registries randomly from all the subregions of Africa.

And one of the questions we asked them is, have you encountered DNS abuse in the recent past as a ccTLD? 75% of the respondents indicated that yes, they have encountered a form of DNS abuse. We further went ahead to ask them what forms of DNS abuse they had encountered within their ccTLD. 50% indicated that spam was the major form of abuse that they were facing. 10% indicated that they had challenges with botnets. 20% indicated that they had issues with phishing. There was no one who indicated issues with farming, as an example.

In terms of measures that they are taking to mitigate or to deal with the issue of DNS abuse, many of them have enacted or implemented various abuse guidelines to deal with the unique cases that they are dealing with. There is also increasing internal staff awareness, as well as implementation of DNSSEC, which is being done by ICANN. I think later on I'll also speak about the African ccTLD and DNSSEC program that AFTLD started implementing in 2012 or 2013.

But just for the interest of the audience, before I embarked on this journey, I went to one of the Kenyan banks, and as I sat patiently to be served, I overheard one of the staff members say that he's been caught and he needs to go for training. Basically, a phishing email was sent randomly, and I think she clicked on it, and immediately she was the subject of a training program by the bank. And I think these are low-hanging fruits that we can be able to implement. There are technical interventions, such as integration of firewalls, as well as reporting the incidents in various computer incident response teams and cyber security departments within the regulatory framework or within the national frameworks.

The last question that we ask is whether they consider DNS abuse a major issue that requires attention from key stakeholders, and all the respondents indicated that yes, they consider DNS abuse as a major issue. So, those would be my opening remarks, Susan, as I bring the floor back to you.

SUSAN CHALMERS: Thank you so much. And on behalf of all of the topic co-leads, thank you for undertaking a desk survey to be able to share this valuable information during the session. So, we have heard opening remarks from our distinguished panelists, and now we'd like to move into specific questions. We'd invited the panelists to consider several discussion questions. I'm not sure if the next slide may have--

Just to give you a flavor of what we had asked our panelists to consider, we'd asked about DNS abuse trends and cases. We've already heard a little bit from our colleague Barrack here on that. Thank you. We've also asked a few questions on policy and solutions, and also any thoughts on next steps for the GAC and ICANN. And so may I invite our colleague Tomboye to take the floor. Tomboye.

TOMBOYE IBRAHIM: Yes. Thank you very much, Susan. As far as solutions and policies that we implemented in order to reduce the number of DNS abuse attacks, as far as we're concerned in Chad, we have not implemented any policies or solutions. However, with a few banks that we came into contact with, we started setting up systems, or they set up systems.

In the past, they didn't have any way to detect whether they were under attack or not, but there was a requirement for those banks to set up computer security systems, and so with that, they ended up mapping risks in order to identify the different risks, to detect them, and to follow up. They also set up different software to detect events in order to trace all of the different movements so that they had a global view of what was happening on their system.

Those measures were undertaken after botnet attacks and malware attacks that had come into their networks through staff at the bank, unfortunately due to outside persons. And so, those banks were able to secure their network, at least to secure it a little bit more, and to have a better outlook on potential incidents and to undertake the different measures in case of attacks.

As far as ccTLDs are concerned, we are raising awareness on those different DNS abuse attacks. We are raising awareness so that people actually report those attacks because what we realized when we did our research is that people don't mention those attacks because they are not aware, and even if they are aware, they don't report them. So, the issue is that the attacks are there, but they are not reported, and so we don't have good data, reliable data, in order to identify the different types of attacks that occur.

And so, the idea of raising awareness was to improve the reporting of those attacks. We will also set up trainings in cooperation with ICANN, and we are going to try to use the tools that are available currently in order to have better solutions to offer to reduce the number of DNS abuse attacks. So, this is just an overall summary. Sorry about that, but that's what I have to say at this point.

SUSAN CHALMERS: Oh, thank you so much. I'm so sorry to interrupt. Do you have anything else that you would like to add?

TOMBOYE IBRAHIM: No. I think that's it at this point. Thank you.

SUSAN CHALMERS: Thank you kindly. So, there's some very interesting comments there on reporting. I'll just take a minute right here to note that it's very useful to have feedback of experiences in ccTLDs. Of course, the contract amendments that the GAC has been following focus on efforts by gTLD registry operators and registrars to mitigate and disrupt DNS abuse.

But I think having these illustrations of practical examples of DNS abuse in the ccTLD realm is very instructive to our consideration of DNS abuse activity in gTLDs. May I turn to you, David, now to see if there are any specific questions you'd like to respond to?

DAVID KANAMUGIRE: Thank you so much. I think I'll speak briefly about the trends we have observed of DNS abuse, particularly in the financial sector. We've seen an increase in phishing emails and other types of spamming and botnet malware, but particularly phishing has been quite a prevalent problem.

And what we have done as a cyber security agency is to work with our partners, particularly the people who regulate the financial sector, ISPs and telcos, to have specific technical safeguards to guarantee better policies and implementation of those policies. We have also run awareness campaigns, particularly targeting helping increase awareness within the financial sector. We've seen more in the financial sector, probably because there is so much motivation for people to target the banks, but also an increase in small microfinance organizations that lack technical capacity to put in these safeguards.

So, we've done a bit of awareness, and last year we released the minimum standards for financial and microfinance institutions to help them deal with these challenges. At a national level, we're trying to do more comprehensive standards, looking at not only the financial sector but other areas as well. So, it's a new area we are still grappling with, but we are seeing increased threats, particularly that use either not so secure infrastructure, but also we are moving towards having a more resilient infrastructure in case some of the things succeed.

So, the financial sector has done so well, it's possibly ahead because of the volume of threats they have met, and increasing our resiliency of our internet infrastructure and protecting critical and vulnerable services like microfinances has been vital for us. Thank you.

SUSAN CHALMERS: Thank you. And just noting the commonality across all of our contributors here, our focus on phishing and the financial sector, so I think that's quite notable. Now, Barrack, may I turn to you please to address any of the questions that you'd like to address? Thanks.

BARRACK OTIENO: Yeah. Thank you, Susan. I think something that would be of interest to the audience is question number three, which I would like to tackle. Around 2015 or thereabouts, we had an interesting incident that I think is in the public domain, where three African ccTLDs, the management or the stewardship was taken over by Freenom, who were then giving out these names for free. And at AFTLD, we went before the African Union to request for their intervention.

It was a matter of concern because at that particular time, while the names were being given for free, these names were also being used to perpetrate a lot of malware activities, phishing attacks, and the rest. And unfortunately, there wasn't much that we could do at that particular time because these were long-term contracts, I think 10-year contracts, that were between the administrative contacts, which were basically regulatory agencies or governmental agencies that are the administrative representatives of ccTLDs within the countries and the particular entity.

And I think this issue came to a screeching halt late last year or early this year when Meta, I think the holding company for Facebook and Instagram, took Freenom to court over the malfeasance or activities that were perpetrating a lot of DNS abuse, which forced the company to wind down. And currently, the conversation we are having is how do we help these ccTLDs to build back? And so, I think this conversation is really relevant to the audience in this room because if we don't understand the responsibility of the administrative contact, we end up in contracts that then not only endanger our countries but really put the whole global Internet ecosystem at risk.

Because a lot of registrations were made under the free ccTLDs, actually millions of registrations, but unfortunately, most of them did not bring much benefit to the local communities. They were actually used to perpetrate DNS abuse activities online. At the risk of maybe going deep into a matter that had been litigated, I don't want to say much more, but I would say that most of this is online and available for comments, but I would speak to that at this particular point.

Again, on item number A, on the same question, as I mentioned, we went before the African Union, but it appeared that there's nothing that the African Union could do at that particular time. Again, drawing us to the attention that ccTLDs come into being as a result of ISO 3166 standard, which defines what a country is and what a territory is.

And again, the representatives, the administrative representatives in most cases are from governmental entities, most of whom are seated here. Whereas 80% of the work is technical, I would say that the administrative representatives have a strong responsibility in stewardship of these ccTLDs and in understanding how their responsibilities or irresponsibilities can affect the global Internet ecosystem. Thank you.

SUSAN CHALMERS: Thank you so much. Just again to note another point for consideration, the correlation between the cost of the ccTLD and the ability or propensity of the registry to respond to DNS abuse reports. I believe we touched on this in ICANN79 a little bit with our presentation from our colleague, Mr. Rodriguez, who administers .pr.

Thank you so much, everybody, for your responses to the questions. I might just ask, if possible, if you could keep in mind, there is question nine here. It would be interesting to have your perspective on what positive impacts do you think that the new ICANN contract provisions will have on DNS abuse activity in the Africa region? Keeping in mind, of course, that these responsibilities are for gTLD registry operators and not ccTLD registry operators. So, if something does come to mind, please do share it with us.

For the time being, we would like to open the floor and invite GAC representatives to raise questions or add comments. Nico, do we have?

NICOLAS CABALLERO: I don't have any hand in the chat room. I don't see any hand in the room. Sorry, I have Papua New Guinea. Go ahead, please.

RUSSELL WORUBA: Thank you, Chair, and thank you, esteemed colleagues, for the wonderful exchanges and the presentation. I have a question or more so a comment seeking insight from our esteemed colleague from Rwanda, David. Would you be willing to share with us how you are structuring your response in terms of your cybersecurity mechanism, in terms of your SOC and your CERT, especially in how you are engaging with the industry and the community with respect to this kind of work? Thank you.

DAVD KANAMUGIRE: Yeah. Thank you. I don't think we have any unique situation, really, from anybody else. But the last three years, Rwanda decided to establish a dedicated cybersecurity agency because, increasingly, the country observed the significant investment and trends that were happening in the digital space.

So, the agency is responsible for coordinating national efforts on cybersecurity response. And it's a policy organ that coordinates private and public institutions to ensure that we have a resilient cyberspace. And we accomplish that by working very closely with our partners in government and industry. In the industry, we work closely with telecom companies, internet service providers, and in the public, we do a lot of working on policy.

So, for example, in Rwanda now, we have all standards that government entities must comply with. We also have minimum cybersecurity standards for key sectors like telecoms like healthcare, and financial sector. I mentioned that. But also, two years ago, we also passed another law for personal data protection and privacy, which is an increasingly important element that we see converging with cybersecurity, but a lot of personal privacy.

So, we do a lot of coordination work, a lot of policy, and a lot of partnership and coordination and engagement like these ones. So, what I can see emerging as a trend is that increasingly African countries are realizing the importance of internet security, information security, and the overall cyberspace security. Realize that most of the challenges we are trying to come up with, we did not even appreciate the internet infrastructure when a lot of these things were being built. So, in a way, we are doing a catch-up game, and we are not really, I can't say we are even fast.

So, I think one of the things we have to do is, since our economies are so dependent on the internet that we don't have mastery or control or tools, how do we make sure that they serve our people effectively without being vulnerable? Our economies now, our telecom companies, handle more money than our commercial banks. And that is not a situation we could even foresee 20 years ago. But mobile money, which is a financial transaction we use for every single payment, is purely digital.

And all the regulations we had were in financial sector, meaning for banks and others. How do we now make sure that our financial sector is resilient in the internet economy when the policies and laws and regulations were of 20 years ago? So, these are challenges we don't claim to have answers, but at least we've put policies and structures to at least understand them. So, I would love to hear, really, maybe experience from other countries. Thank you.

NICOLAS CABALLERO: Thank you very much, David, for the answer. Thank you, Papua New Guinea, for the question. The floor is still open for comments, questions, anything you would like to add at this point. I don't see any hand in the chat room. And as a matter of fact, I don't see any hand in the room either. So maybe we can move on, Susan, to the next topic, which is possible future developments.

SUSAN CHALMERS: Sure. Thank you. Just really quickly before we move on, I want to ask if any of our panelists here, including Ms. Ibrahim remotely, have anything that they would like to offer in conclusion. Barrack, please.

BARRACK OTIENO: Thank you very much, Susan. I think to answer the question on whether there's been a positive impact of ICANN contract provisions, or rather whether the ICANN contracts provision will have a positive impact on DNS abuse, I would say yes.

I have also participated in the registrar ecosystem on the African continent, and especially for the ICANN accredited registrars, they are subjected to the same requirements as any other global registrars. And I think there's a positive effect in some of the rigorous processes that they have to go through to be able to comply in that this knowledge is then transferred locally to developers who are then building systems that are providing access for end users to the domain name systems. So, I would say that the answer is yes.

I think one conversation that we are continuously having is what it takes for a registrar to become ICANN accredited. In 2013, again, we set out on an agenda to ensure that we increase the number of ICANN accredited registrars on the African continent. We had a soft target of 25, but unfortunately, we've only been able to get to just about 10 or thereabouts. And the issue is the costs that are involved, and many of the registrars keep questioning whether there is additional value in the spend, in what they have to pay for them to be accredited. So, I believe this is a conversation that we should keep having.

The other point that I would wish to submit to the audience is, as I mentioned earlier, when we embarked on the African ccTLD and DNSSEC initiative or program in 2013, there are a number of projects that we sought to implement, and I believe that some are still relevant to date. Some partners or some stakeholders took up responsibility on some of the issues. One of them was the establishment of a ccTLD observatory, to be able to provide the data or the content that is relevant for policy makers to make intervention.

I have started the conversation with a desk survey, but I have to indicate that there is an observatory, the Africa Domain Name Observatory that Africa Top-Level Domains Organization has developed to track such issues. The other issue is, we also embarked on improving governance of the country code top-level domain registries and community engagement. I have to indicate that most of the African country code top-level domain registries operate using the 3R model, registry, registrar, and registrant system.

In this model, in most cases, the regulator remains the administrative contact. In many cases, the regulator is actually licensing the people that actually operate the country code top-level domain registries. So, I believe that we need to have greater conversation, and probably because this is a GAC session, maybe later on we could have the conversation at African level. But also, the issue of community engagement was flagged as an important part of this.

Remember, we have registries, but we have registrants. And we are only as strong as our weakest link. So, if we are not engaging our communities well, then they will be the ones who are perpetrating most of these abuse activities. There is also a lot of capacity building. I've had an opportunity in the past to participate in sessions such as this. And thank you, Susan, once again for the invitation to be able to share what's happening in the community. And I think we need more of these sessions and focused capacity building sessions to various key opinion leaders.

And lastly, we established a community of practice, which is the Africa Domain Name System Forum, which brings together registries, both from the ccTLDs and the gTLDs, registrars, registrants, and anyone who is interested and involved in the domain name ecosystem on the African continent to discuss issues such as this.

I conclude by saying that I think Africa is on the growth path. Looking at the recent statistics presented during the study that was conducted by ICANN, there are just slightly over 4 million domain names registered across all ccTLDs in Africa. Country code top-level domain registries are still leading. And I have to indicate, if I compare this to the global scenario where we have slightly over 350 million domain names across all TLDs, I have to indicate that Africa is the growth area.

So, if at all there is a place where DNS abuse is going to be a key issue, then it's going to be within or from the African continent. And I think it's a call to all stakeholders. I think we have started the conversation, but we can mitigate it before it goes far. Thank you, and back to you, Susan.

SUSAN CHALMERS: Wonderful. Thank you so much, Barrack. Mindful of the fact that our registration data session is also within this period, what I'm going to do is quickly ask Tomboye and David to share some concluding remarks, though rather briefly, and then I will turn it to my colleague, Martina, for some next steps. But if we would just be mindful of the time. Thank you. Tomboye, over to you.

TOMBOYE IBRAHIM: Yes. Susan, thank you for the floor. So, I wanted to say that there are best practices in order to mitigate DNS abuse. We can better circulate them at a number of levels for registries, registrars or registrants. I also want to encourage African ccTLDs. I want them to foster collaboration. We share similar realities, and if we talk with one another, we'll better be able to solve our issues and we'll be able to thwart these threats to our DNS, and we will uncover solutions together. And let's also collaborate with the AFTLD. I believe collaboration is in order. Finding solutions together is in order. Thank you very much for giving me this opportunity. Thank you.

DAVID KANAMUGIRE: Thank you. I think first we really have to appreciate the unique position and strength of ICANN in ensuring really the security and resilience of Internet for the rest of the world and see a way that the technical capacity and experience and resources they have at a global level can trickle down to helping African ccTLDs to make sure that that weakest link that was mentioned doesn't happen.

So, capacity building is vital. I very much liked the comment by Otieno about engagement and the community. We have to find a way of maintaining engagement as a community to make sure that whatever abuse and threats we meet, we also have the capacity to mitigate them and address them quicker before they cause these challenges. So, I think ICANN, we need to rethink how we collaborate across the continent and how we can bring down the expertise and experience and resources to make sure we build a more resilient DNS infrastructure. Thank you.

NICOLAS CABALLERO: Thank you very much, David. Before we wrap up the session, let me give the floor to Martina Barbero from the European Commission. Martina.

MARTINA BARBERO: Thank you very much, Chair. And very, very briefly, Fabien, if we can skim through the next three slides incredibly fast. So just to say that we heard from our distinguished guests the DNS abuse is a never-ending threat, so the work of the GAC never ends, right, on this topic.

And this summer when we were discussing the contract amendments, we were looking at possible ways of continuing to address this phenomenon. So, you see listed on the slide some of the ideas that we discussed in this room and which might still be of relevance, but if we go quickly to the next slides. So, this is an open question for the GAC, and we will have hopefully more time to discuss it in Istanbul, what we need to do next, keeping in mind that there was going to be the next gTLD round opening.

And then on the last slide, just to say that we had a very nice session, we learned a lot I think today, so as topic lead we will offer some text for the communique in the issues of importance to reflect on these discussions, and of course the text will be offered for consideration to all the GAC members, but we hope that it will reflect the key learnings from today. And I would like to go back to our distinguished chair. Thank you very much, Nico.

NICOLAS CABALLERO: Thank you very much for that, European Commission. We need to wrap up the session. Thank you, Martina, Susan, Nobu, European Commission, United States and Japan, Chad, Rwanda and the Africa top level, TLD organization, Mr. Barrack Otieno, Mr. David Kanamugiri from the Rwanda government, and Tomboye Ibrahim from the Republic of Chad. Thank you so very much. So, with that, let's get ready for the next session.

So, welcome again everyone to the WHOIS and Data Protection Policy session. This is going to be a short session, as a matter of fact, only 45 minutes, and I'll make sure we can add 5 minutes at the end in order to make sure that we'll have enough time for discussions in the Q&A session. Let me welcome Gabriel Andrews, who's the co-chair of the Public Safety Working Group from the FBI USA, Laureen Kapin from the US Federal Trade Commission, Kenneth Merrill, if you can join us here, oh, here, from the US Department of Commerce, NTIA, and Melina Stroungi, I hope I'm pronouncing your last name well, Melina Stroungi from the European Commission.

I understand Gabriel, Laureen, and Melina are online. They're not in the room, so they're going to be participating online. And the agenda for today's session is some background on WHOIS and data protection, urgent requests for disclosure of registration data, RDRS and the impact of privacy proxy services, and finally, considerations for ICANN80 Kigali Communiqué. So, with that, welcome everyone again, and let me give the floor to you, Kenneth, is it, or who's going to start? Laureen, sorry. Laureen Kapin, who's joining us online. Laureen, please go ahead, the floor is yours.

LAUREEN KAPIN: Hi, folks. Looks like my camera is-- There we go, now it's popped in. I'm sorry that I couldn't join you in person, but I'm happy to be here speaking in my capacity as a member of the Public Safety Working Group. I wanted to give some brief background about what WHOIS is and why it's important to the GAC with patience for folks who have heard this before, but I also know that we always have new members in the Governmental Advisory Committee.

So, we always make sure to provide this context and background because these principles and goals really serve as a foundation for a lot of the current policy discussions. So, why is this important to the GAC? Well, the GAC has actually set forth some principles regarding WHOIS services. And just briefly what is WHOIS?

That is an informal name for domain name registration data that tells you who the registrant is, their contact information, their name, telephone number, address, technical contacts, if something goes wrong with the domain. So, all of that is part of, again, the informal term, what is the WHOIS record. Another name for that is domain name registration data.

And that information is very important on a practical level for many different stakeholders, including law enforcement, who can use this information to investigate, for example, DNS abuse, the topic of the last session. It also can be used to notify a registrant if their domain is being used for bad acts that the registrant doesn't even know about. So, this information is very important for both investigating and enforcing both criminal and civil laws that deal with misleading conduct or criminal conduct related to domain names.

But it's not just law enforcement who relies on this information. Businesses and other organizations look to this information to combat fraud, so they can comply with relevant laws and to safeguard the interests of the public. And we see this a lot when businesses are trying to combat impersonation scams, people pretending to be them, people pretending, for example, to be Microsoft or some other entity that might be pretending to help you repair your computer. So, these businesses have an interest in trying to find out who is behind domain names that are pretending to be them, because that hurts their reputation, it hurts their customers.

There are also, of course, intellectual property holders who are interested in making sure that they can defend their rights. And we know that IP holders, consumer protection authorities, and law enforcement authorities are folks who are currently making use of the registration data request system, RDRS, which we'll hear about later in the session. And then, last but not least, there's you and I, Joe and Jane internet user who might want to check out a domain to try and figure out how long it's been in existence, if it has someone who's associated perhaps with bad behavior, because that can help us as internet users figure out if we should trust that domain name.

So, those are just some examples of reasons why this information is important and how it is used. And of course, it all relates to public policy concerns. And even though the landscape has changed very much with regards to how this data is protected, there are now very robust data protection laws that protect privacy, which is also very important because we know when this information was fully available to the public, that there also were certain abuses of that information.

So, the landscape has shifted to protect this information more robustly and also create a balance between protecting this information and its possible misuse with all these uses by stakeholders. And so, one of the things that the GAC has emphasized is keeping this information accessible for security and stability purposes and also keeping it accessible for legitimate uses, especially when fraud and deceptive conduct is involved.

So, that's a brief overview of WHOIS is information is and why it's important, and also the balance that was striking between protecting privacy and also permitting the information to be used for legitimate purposes. This is the wonderfully complicated timeline slide. And what I want to direct your attention to are the red areas. Those are the ongoing efforts that relate to domain name registration data.

So, you'll see we have ongoing activities with regard to accuracy, and this is the subject of several questions to the Board and the GNSO. That is still currently paused and hopefully will resume in some form. But also in the lower right-hand corner, we have our current activity that focuses on the registration data request service. And this arose as a result of the System for Disclosure and Access for Data, the SSAD. There were concerns that the policy recommendations that arose in that regard might be too expensive and too complicated and may not be used.

And so there was a pilot program that was developed, the RDRS, to do on a smaller scale some functionality that could help us gather data to determine whether the system is likely to be used by whom, how long things are taking, what issues and complexities that may arise, essentially to give us some more data to decide what makes sense going forward. And that's where we are now. That launched in the fall, in November. It will go on for two years, and we'll hear some very interesting information about how things are going so far later on in the presentation. So, stay tuned for that information. But that is the part of the pilot--

NICOLAS CABALLERO: Apparently, there's some sort of issue with-- Go ahead. Go ahead. Sorry. Go ahead.

LAUREEN KAPIN: Is there an issue with progressing the slide? Let's start with that. Okay. So, urgent request, I think that is Melina. Do we have Melina online?

NICOLAS CABALLERO: Yes, Melina is next. Melina Strougni from the European Commission. Should I give the floor to her, Laureen?

LAUREEN KAPLIN: Yes, Melina is on. Thank you so much.

MELINA STROUNGI: Thank you, Laureen. And hi, everyone. I hope you can see me well. And, Nico, you pronounced my name correctly, which is a rare thing to do. So, Melina Stroungi from the European Commission for the record. I'm going to give you a debrief on the issue of urgent requests.

As a quick reminder, urgent requests were part of the EPDP Phase 1 policy recommendations, which were approved by the ICANN Board and then were temporarily removed from the resulting registration data consensus policy. As you may recall, this registration data policy is a policy that lays down requirements concerning the collection, transfer, and publication of gTLD registration data. And it becomes part of the ICANN contractual requirements.

It was drafted back in 2022. The GAC provided input at several stages during also the implementation review process, but the work stopped in summer of 2023 over disagreement on the issue of urgent requests. Now, urgent requests are defined as limited to circumstances that can pose an imminent threat to life, bodily injury, or critical infrastructure or child abuse, exploitation. And so, there has been a bit of a debate, what is the appropriate timeline to respond to urgent requests.

The GAC believed that it should be treated as soon as possible in no more than 24 hours, a position that was also expressed in our GAC Communique in Washington in June 2023. The contracted parties on the other side had suggested that such 24-hour deadline should be extended by two business days plus one business day for complex requests or a big number of requests. Something that if you add weekends and public holidays could even result to a one-week response to an urgent life-threatening situation.

As an agreement could not be reached in the end, in January of 2024, the registration data policy was published, but without the section on urgent requests. This was put in hold so we can see if an agreement can be reached separately. And to give you some timeline ever since, as you see on the slide, in a letter to the GAC in February of 2024, the ICANN

Board concluded that it is necessary to revisit the recommendation on urgent requests and that consultation with the GNSO is required.

Then in March of 2024, in ICANN79 in San Juan, we, the GAC, issued advice to the ICANN Board and we advised that they act expeditiously to establish a clear process and a timeline for the delivery of the policy on urgent requests to respond to vital public safety interests related to such requests. So how did the Board reply to our GAC advice? As a response in May 2024, the ICANN Board determined to defer action on this advice, noting that it plans to discuss the issue with the GNSO Council.

In the most recent letter to the GNSO Council, which was sent one week ago on the 3rd of June, the ICANN Board welcomed the GNSO Council's next steps and noted that this is an unprecedented situation because neither the bylaws nor existing procedures account for a situation where a policy that has been previously adopted would be revisited. Also, among the other concerns, ICANN Board stressed the importance of the urgent requests, mentioning that to respond to true imminent threats, a much shorter response timeline, minutes or hours rather than days, would seem to be more appropriate.

And then there were some new elements added that have not been raised before during the initial discussions on authentication of requesters to such data. So, ICANN noted that there is an issue of how to authenticate whether a requester is truly a legit requester, for instance, whether a law enforcement authority is who they say they are, and that an authoritative legal cross-border system for authenticating users globally is not available to ICANN, and such a mechanism cannot be created without the assistance of law enforcement and governments.

Now, the latest update we have from this morning bilateral with the GNSO is that unfortunately they didn't have the time to review the letter from the ICANN Board yet, and that they don't see a clear process yet on how they can move with this and whether indeed they agree with ICANN Board concerns. It is a pity that this issue has not been addressed earlier.

From GAC side, we support finding a solution, of course, to the issue of authentication, as this is not relevant only for urgent requests, but to any type of requests in general, and the Public Safety Working Group within the GAC has already started reflecting on this topic, and will investigate with law enforcement authorities to see whether there are any existing tools that can be leveraged and explore solutions.

At the same time, we hope that these discussions and work will not add to any further delays in the policy for urgent requests, and that we can all work together to address this issue as swiftly as possible. I'm happy to take any questions or remarks at the end, and now I think Gabriel Andrews will give you an update on the registration data request service, the famous RDRS, and the impact on privacy proxy services. Thank you.

GABRIEL ANDREWS: Thank you, Melina. This is Gabriel Andrews. Thank you, Nico. I hope you feel better soon, by the way. So, this is Gabriel Andrews speaking for the record on behalf of my capacity as the co-chair of the Public Safety Working Group. I am going to be talking a lot about ICANN's system to request unredacted registration data, which is the registration data request service, RDRS for short. Some call it red dress.

Before we go into that, however, I wanted to make sure that we all understand the status quo without a functioning RDRS. What you see on your screen now, this is what redacted data looks like. You can query a domain name using any tool that you prefer. This shown is ICANN's lookup tool on their website. And when you get the response back, where once you would have seen administrative data or technical data or registrant contact information, now we often see the words redacted for privacy. The data is still there. It's just not shown to the public.

And I'm waiting for the next slide to progress. Thank you. ICANN has launched in their registration data request service. It is now six months into its two-year pilot. This is the service that has been advertised as the tool available to request that access to the non-public gTLD registration data. It's been advertised as a free global one-stop shop to submit the registration data requests to the participating registrars worldwide. Of course, a number of registrars are voluntarily participating, for which we're very grateful.

Both Ken and myself, and this is I'm referring to Ken Merrill on the stage now, are participants in the standing committee that is tasked with reviewing the data that's coming out of this RDRS pilot. This means that we are following a number of assignments specifically to identify the trends and the monthly data that's coming out of it, to suggest updates to the RDRS, as well as to how it's being promoted, and to take any lessons from it that might inform a successor system like SSAD.

I say this because if there are any GAC members who know you have colleagues in your governments that are trying out the RDRS, we encourage you to reach out to Ken and myself to ensure that we're tracking any feedback you may have as part of our engagements in that standing committee. You may also be interested in knowing that right this moment, apparently, is scheduled a presentation by the Registrar Stakeholder Group about their experiences using the RDRS. I am told that that's being recorded and will be available to be viewed after the fact.

I'm going to turn now to the data that has been coming out of ICANN's monthly reports. This is a graphic that I made using that data, which tries to show a very high-level overview of all the RDRS requests that have been made from start to finish. What you see here is, on the left, the total number of domains that have been looked up in the RDRS, and then the various ways in which those domains have broken down into various outcomes.

When you first log into the RDRS, after submitting your username and logging in so that they know who you are, the first thing you do is you input a domain name, and that's the 7,677 on the left. Go ahead and click to the-- Yeah, thank you. You're at the right point. When the domain name is input, about one-third of the time, we can see that

RDRS is capable of handling the request. The other two-thirds of the time, it's because either the registrar isn't participating in the pilot or the top-level domain isn't supported, which probably means it was a ccTLD that was entered. What we see here is that this shows a very strong demand from the requesters, both for increased registrar participation, but as well as for an inclusion of ccTLDs, if a mechanism to do that can be found.

If the domain was supported, we see that occurred 2,400-some odd times. About half of those 2,461 times a request has been generated. Now the other half, and I'm going to have you click through again please, of the 1,246 times underneath-- sorry I'm waiting for slide 13 to catch up with me. We don't know necessarily why about 50% of the requests appear to be abandoned midway through.

This is an open question but there has been feedback to the standing committee from different requester constituencies that the RDRS form can be kludgy to use, clumsy, and it's possible that user friction contributes to this 50% drop rate, but we really just don't know. But much of the feedback that's been provided to the standing committee thus far has been aimed at improving the RDRS user experience.

And so, we see that of the 7,677 domains that were input into the RDRS in the first six months of reported data that we've received from ICANN, some 3% resulted in either approval, which means data is disclosed, or partial approval. And it's an interesting metric to take. I note again the registrar speaking now in their session might be speaking to why they feel the number of denials versus approvals have played out as they have. I'm not going to speak to that. I think that's more their role.

But at a very high level, I feel that this is something that is very useful to see the big picture in terms of the total number of requests coming in and the room for improvement perhaps in terms of how this tool can be made more useful to the requesters which we're directing towards it. Speaking of directing users to the RDRS, I wanted to switch gears and talk about the awareness that has come from our promotion and messaging efforts. And this is going to start with sort of a confession.

My day job working for a law enforcement agency, I've been working hard to try to raise awareness of the RDRS as a useful tool within my own agency. And I have to come to terms with the fact that six months in, when I talk to agents on the ground, analysts, investigators, more often than not, they haven't become aware despite all of the efforts that I've put into organization-wide email blasts, education sessions, et cetera, which means I'm failing to get the word out.

The push messaging that we've been trying to send out these awareness messages, it's not hitting all of the users that need to hear it. But thankfully, having contemplated this more, I think it's important to recognize that we have a tool available that actually can reach 100% of all the users of registration data. And that is the data itself. So, this slide is the very same slide I showed you a few minutes ago.

This is what it looks like when you do the domain lookup for the registration data, and you're first being made aware that that data is redacted for privacy. But this is also the perfect opportunity to communicate not just that the data has been redacted, but this this could also be the very same mechanism by which you can direct the users of this data to the RDRS to make them aware that this exists. So, with the very same breath, you could be telling them, yes, this data is redacted. And here's the mechanism that we as a multi-stakeholder community have created to allow potential legitimate users to gain access to that data if they have that legitimate need.

We gave advice to this effect in San Juan. You can see that highlighted at the bottom. Actually, this might not technically be advice, but we did strongly encourage the inclusion of information about the RDRS within the WHOIS and RDAP responses. And the Board responded, as you can see on the next slide now, please, that there was agreement that the information and links to RDRS can be added to the RDAP outputs either from registries or registrars. And the GAC suggested that this option be brought up specifically with the GNSO Council as potential policy. This is certainly something to be considered.

As we consider it, I think it bears mentioning that we have 18 months left of the RDRS pilot. And so, any potential policy discussion might end up being more helpful in how we might promote or message successor systems such as the SSAD. Not entirely optimistic that policy could come in time for RDRS awareness, but it is worth noting in the meantime that both the registrars and the registries don't need new policy to voluntarily take this action to use WHOIS and RDAP responses to promote the RDRS. They can do so now without the need of ICANN's permission. And in doing so, they might assist by using the single most effective means of achieving our community's shared goal of ensuring that all potential users of the RDRS are aware it exists. A goal that unfortunately I think we have yet to achieve.

I'm going to pivot now to proxy services and update on where we stand. And as a reminder here, proxy services are not the same as the redaction for privacy. I know this is well understood by many in the room, but I just want to make sure that we're all starting from the same page because it can be a little bit confusing. But the key distinction here is important that when a proxy service is employed, most often we see the registrar themselves are inserting their affiliated proxy name as the registrant. So, the key distinction is the registrars are treating their own proxy services as the registrant.

This means that when a registrar receives an RDRS request and when they've made that registration using their affiliated proxy service, the most common response the registrar then gives is this information is already public because they're referring to the public display of their affiliated proxy info. Thus, while we're aware that there are 88 now, I believe, registrars voluntarily participating in the RDRS, we are currently aware of none who are doing so on behalf of their affiliated proxy services. And you can see then that dealing with these complexities that arise when a registrar provides the proxy data in place of the underlying customer data will be critical to developing an SSAD that is fit for purpose.

So, the policy development on this. We had in 2016 policy on the privacy and proxy service accreditation, which was approved by ICANN's Board and has been on hold since. There is again now, at long last, noting there's a small typo in ICANN at the top, but there is again now finally movement on this issue and that ICANN just last month on May 20 issued a call for volunteers to join the PPSAI implementation review team.

We just discussed why this is important and how critical it is in a number of our current ongoing work streams with RDRS, upcoming SSAD. So, it's important to call out that the very first meeting then of this PPSAI implementation review team is going to be held this Thursday at 9:00 AM, your local time. And with that highlighted for your awareness, I'm going to flip the microphone over to my colleague, Ken Merrill, for the final topic.

NICOLAS CABALERRO: Thank you very much for that, Gabriel. We already have a queue. We have Iran and India, but I just want to make sure we have enough time to finish the presentation. So let me give the floor to the US. Ken, please go ahead.

KENNETH MERRILL: Thank you, Nico. Kenneth Merrill, United States Department of Commerce for the record. I'll be very brief to leave time for the questions. So, I'll just offer a few points for consideration for the Communique. A couple of the topics that may be ripe for advice is the RDRS that Gabriel mentioned and the privacy proxy accreditation implementation policy.

And here I just wanted to follow back up on a couple of points that Gabe made that there are sessions ongoing this week relevant to both of these topics. So, it could be worth just thinking about those as well. And then finally, just sort of a question for the GAC as well to put on the table is sort of what issues we may want to consider for issues of importance as well. So, with that, I think I'll hand it back over to Nico and we can get to the questions.

NICOLAS CABALERRO: Thank you very much, USA. I have Iran, India and the UK. So, for the sake of time, please take into account we only have eight minutes. So please try to be very straightforward and specific. India, please. Sorry, Iran. Iran.

HOSSEIN MIRZAPOUR: Yes. Hello. First of all, thank you, Chair and others for this informative session and hope the best of health for you, Nico. Actually, my question is regarding Melina's presentation. I thought it was mentioned that in Communique of Washington, DC, there was some phrases about the 24-hour deadline. I don't know if maybe I misunderstood, but unfortunately, I missed that forum personally. But as I have consulted the Communique, I did find nothing. Just that was my question.

NICOLAS CABALERRO: I can get back to you with that later, Iran. It's not directly related to this, but I can get you that information later on. It is I don't know exactly which page, but I can get you that information. No problem. Do you have any specific question about this?

HOSSEIN MIRZAPOUR: No, no. My question was from Melina. Thank you.

NICOLAS CABALERRO: Perfect. Thank you, Iran. I have India.

T. SANTHOSH: Thank you, Chair. This is T. Santhosh for the record. Now, coming to this slide, that is urgent request for disclosure of registration data, how it is made? If a law enforcement agency of a country wants details, should they contact through RDRS or is it a separate mechanism? This is the question number one.

Now, question number two is related to RDRS. The presentation was fine, good, but how many registrars are actively contributing in this RDRS is not exactly mentioned. It has mentioned that only 3% of the request has been approved, but how many registrars, that is only gTLD registrars. So, from the GAG side, the last question made by the colleague from US.

GABRIEL ANDREWS: I can answer that quickly.

T. SANTHOSH: So, the request, the last question from my side is, as a GAG, in order to mitigate the DNS abuse, WHOIS has to be accurate. Unless and until WHOIS is not accurate, we will not be able to provide solution to RDRS. And even if it is a privacy proxy thing done, the solution could not be provided to the requester. So, my request to both GNSO as well as the ICANN is to have a quick and timely WHOIS accuracy done. Thank you.

NICOLAS CABALERRO: Thank you, India. Gabe?

GABRIEL ANDREWS: Thank you, Nico, and thank you, India. So, at last count as of the, I believe it was the April reporting, perhaps May. Sorry, I'm losing track of which month it was. There were 88 registrars that were participating in a voluntary basis with the RDRS, and that was accounting for approximately 57% of the total number of domains under management in the gTLD space, not including the ccTLD space. And I hope that's helpful.

NICOLAS CABALERRO: Thank you, Gabe. I have the UK Home Office. Karim?

KARIM GREGORY: Hi. Karim Gregory, UK Home Office. I just wanted to comment on urgent requests. So, firstly, thanks to those in the Public Safety Working Group and GNSO Council that are working hard to deliver a solution on this. However, I guess my concern or my question to the group is whether it's enough of a priority for ICANN and the pace at kind of what we're-- the pace that we're working on now to deliver a solution. Is it fast enough, given that this is a provision to protect the public from serious harm? So, are there any ways to expedite this and should we be pouring more resource to implement a solution for urgent requests?

NICOLAS CABALERRO: Thank you for that. Who exactly is that question for? For Gabe? For Kim?

KARIM GREGORY: Probably for the ICANN Board to see if we should, as a group, whether we should take it more to a priority in negotiations, because obviously it's quite important.

NICOLAS CABALERRO: Okay. Thank you for that.

KENNETH MERRILL: I don't think I'm in a position to answer that, but I'm happy to take it offline.

NICOLAS CABALERRO: Okay. Again, thank you, UK. I have Argentina and then the European Commission.

MARINA FLEGO EIRAS: Well, thank you, Chair. Thank you for this quite informative and illustrative session. This is not a question. It's just a response to the question of the Iranian delegate. As far as I'm concerned, in the 0.7 of the Washington Communique, there was a specific mention to the 24-hour time limit. Okay? Thank you.

NICOLAS CABALERRO: Thank you very much for that, Argentina. I couldn't remember from the bottom of my heart, so to say. So, Iran, is that okay with you? Perfect.

HOSSEIN MIRZAPOUR: Yeah. Thank you.

NICOLAS CABALERRO: And thank you again, Argentina. I have the European Commission next. Melina?

MELINA STROUNGI: Yes. Just to echo what was heard already, and I see it's already projected on the screen, but it is in the Washington Communique, page nine, I think. Yes, page nine, the mention of the 24 hours. So, hope this clarifies. Thank you.

NICOLAS CABALERRO: Thank you very much, European Commission. Any other comment, question, thought? I don't see any other hand in the chat room. Sorry. Ken, go ahead. Yeah.

KENNETH MERRILL: I just wanted to respond to our India had a second question there regarding accuracy and didn't want to go without answering. But I just wanted to that question, I think that in our last session with the GNSO, we proposed a question to the GNSO on when we might be able to pick up on the work of on the accuracy work again. And so, there are some process hurdles between where we are now and getting back to that work. But I think we as a GAC, I think we're on the same page in terms of a need to continue to look into accuracy. And so, happy to follow up with you on developments there.

NICOLAS CABALERRO: Thank you very much for that. Any other comment, thoughts, questions? India?

T. SANTHOSH: Thank you, Chair. So, my first question was related to the urgent information related to the registration data. What is the process to be followed?

NICOLAS CABALERRO: Thank you, India. Ken?

KENNETH MERRILL: Yeah. And I may also have my colleague Gabe chime in here as well. But the issue of urgent requests came out of the phase 1 work on the new registration data policy. And so, that's where that issue sort of resides. If there are, of course, impacts on registration data more generally, but in terms of the RDRS itself, it's not directly sort of situated within that work. But let me have my colleague Gabe come in as well to clarify that if you'd like to.

GABRIEL ANDREWS: Sure. And so, this is Gabriel Andrews again speaking for the record. I note that when the RDRS was originally contemplated, there was thought that it might be able to handle urgent requests. But that was a decision that was since changed, noting that, and I'm speaking from memory here, but I believe the determination was made that the timeline that the RDRS operates on wasn't appropriate for requests of that type of urgent nature.

So, the open question of how law enforcement agencies make that request then is not one that is answered by the RDRS or currently by the policies that are in discussion. It's something, though, that the Public Safety Working Group is actively hoping to assist with in our discussions. We have some initial tentative conversations that we're engaging with, but it is a bit too early for us to offer suggestions. But we did hear loudly and clearly the messaging that was given by the Board in San Juan that this is going to be an important issue for us to collaborate on. And the Public Safety Working Group is eager to be constructive and helpful in this regard. But I don't have anything, I'm sorry, concrete to offer at this moment.

NICOLAS CABALERRO: Thank you again, Gabe. Thank you, India, for the question. We need to wrap up the session. Thank you to the panelists, Gabriel Andrews, Laureen Kapin, Kenneth Merrill, and Melina Stroungi from the European Commission, US Department of Commerce, US Federal Trade Commission, and US FBI. Thank you so much for your time and for your detailed explanation.

And just keep in mind, and this is for the full GAC, these two last questions right at the end of the presentation, because this is something we need to take into account, especially when we start drafting the GAC Communique. That's for granted. The first one being, is GAC advice needed on the topics of RDRS and or PPSAI? That's the first one. The second, which topics should the GAC highlight as issues of importance? So, we have two different things here, GAC advice itself and issues of importance. So again, let's wrap up the session. Any final words, anything you would like to add? No, and I don't see any other hand up. Nigel?

NIGEL HICKSON: Yes. Thank you very much, and thank you everyone for a really excellent session. I know it's lunchtime, but just to echo Nico's thoughts, I know some GAC members are new to this whole process, but the Communique, which we'll be hearing about tomorrow, is all important, because this is where we give our views. And so those that have concerns in this area should talk to their colleagues, and when we come to the meetings tomorrow, express their thoughts on whether we should give advice or whether we should highlight our concerns on some of these issues.

NICOLAS CABALERRO: Indeed. Thank you very much for that, Nigel. So, to my distinguished GAC colleagues, we'll reconvene here in the same room at 1:45 for the next session, which is session number seven, GAC Capacity Development session. Enjoy your lunch. Thank you so much.

[END OF TRANSCRIPTION]