ICANN85 Mumbai | CF – GAC: Discussion on DNS Abuse Mitigation
Monday, March 9, 2026 – 16:30 to 17:30 IST

NICOLAS CABALLERO Welcome back everyone.

JULIA CHARVOLEN At an unreasonable pace to allow for accurate interpretation, please make sure to mute all other devices when you are speaking. With that, I will leave the floor over to GAC Chair Nicolas Caballero. Thank you, and over to you.

NICOLAS CABALLERO Thank you, Julia. Welcome back, everyone. Welcome to the GAC session on DNS Abuse Mitigation. We have a fantastic lineup for today's session made up of our GAC topic leads: Martina Barbero from the European Commission, who is joining us online; Tomo Miyamoto to my right; Gabe Andrews from the United States government, also our Public Safety Working Group co-chair; and of course, Susan Chalmers from the US government. Our guest speakers today are Devesh Tyagi from the .IN ccTLD manager and Manju Chen from the Trusted Notifier Network. This session is going to be running for one hour, and I really hope we will have enough time for a Q&A session right at the end of the presentations. The idea is to have an interactive exchange with all of you. With that, let me hand the floor over to Susan. Please go ahead.

SUSAN CHALMERS

Thank you, Chair, and good afternoon GAC colleagues. My name is Susan Chalmers, and I represent the United States. I serve as a topic co-lead on DNS Abuse alongside my colleagues from Japan and the European Commission. This is the GAC session on DNS Abuse, which is a priority issue for the GAC. Because of the staggering impact of phishing, malware, and botnet attacks, it is a concern of governments, and that is why we are focused on it.

The Governmental Advisory Committee's annual plan is focused on two work streams. The first work stream is advancing ICANN policy work on DNS Abuse before the further delegation of new gTLDs. Then we have the capacity building work stream, which is building the subject matter capacity of GAC members on DNS Abuse.

At ICANN, DNS Abuse refers to types of malicious cyber activity that most governments would consider to be cybercrime, for example, phishing, malware, or botnets. However, there is a very specific definition within ICANN: DNS Abuse means malware, botnets, phishing, pharming, and spam, when spam is used as a delivery mechanism for any of the foregoing categories. Threat actors make use of many different internet services beyond internet domain names to execute these types of attacks, for example, website hosting, internet service providers, SMS, and VoIP. In the GAC, given ICANN's remit, which focuses on the security and stability of the internet's unique identifier systems, including the DNS, we are focused specifically on policy for the registries and registrars that

have contracts with ICANN. This ensures these contracted parties can proactively take steps to prevent domain names from being instrumentalized by threat actors for DNS Abuse.

Generally speaking, at ICANN, gTLD registries and registrars are contractually required to respond to reports of DNS Abuse. ICANN compliance audits and enforces these contract requirements. Personally, I think about the two as two sides of the same coin. These DNS Abuse obligations were specifically established by a landmark set of amendments to the agreements between ICANN and domain name registries and registrars, which went into effect in 2024. This slide gives a bit of history here, which is not exhaustive. I will just pause for a minute. I understand we have 19 new GAC representatives since Dublin. Do we have the opportunity to have any of them in the room today? You don't need to be shy.

NICOLAS CABALLERO Please raise your hands. The new GAC representatives, would you please raise your hands?

SUSAN CHALMERS Welcome. Very exciting. Just a pro tip: our GAC support staff develops briefings for GAC representatives in advance of our sessions. They have managed to squeeze the history of DNS Abuse and the GAC's engagement in it into a very short fifteen pages. It is a great overview, and it can give you a much more comprehensive history on the subject matter here.

The milestones here, outside of the contract amendments and for the purposes of the GAC, include our advice from the ICANN 83 Prague session. I won't read it as it is on the screen, but that is what the GAC delivered in Prague last year. More recently, and to our delight, the GNSO adopted a new PDP charter for an Associated Domain Check. During the middle part of our program, my colleagues will address the current activity in that ADC PDP.

In terms of the programming, before and after that GAC update on what is going on at ICANN, we have the pleasure of receiving two different presentations that will inform our collective understanding of different policy and operational efforts to counter DNS Abuse, both outside of ICANN. First, our Indian colleagues and gracious hosts from NIXI, the administrator of the .IN country code top-level domain, will present on the policies they maintain for .IN registrations to prevent DNS Abuse. Second, building upon our last session in Dublin during ICANN 84, we will receive a presentation from the Trusted Notifier Network. This is tied to our GAC annual plan of capacity building. Trusted Notifier programs generally take place outside of ICANN's remit, but the TNN, the Trusted Notifier Network, is more than a program, and we will hear from TNN's Director of Policy, Manju Chen. Without any further ado, let's turn first to our presentation from Devesh Tyagi from NIXI, the administrator of .IN. Over to you.

DEVESH TYAGI

Thanks. Good evening to all. We have been operating the .IN registry since 2012. In the last one or two years, we have taken certain initiatives based on actual experience on the ground and the abuse which we were witnessing. These initiatives include domain name keyword verification and WHOIS verification. In cooperation with Indian LEAs, we had certain discussions and received many suggestions. We incorporated many of them to mitigate the DNS Abuse which we were witnessing.

First of all, we started identification for foreign nationals who were onboarding on the .IN registry. For this, we put a policy in place wherein the .IN registry is now verifying registrant details using documents such as passport, citizen ID, and other accepted relevant identification. Another thing we have done is the revision of the registrar accreditation agreement. Under that agreement, we put a new clause, 4.4.15, wherein foreign applicants requesting a .IN domain must demonstrate a legitimate business connection or purpose in India. Through this, we are able to mitigate certain challenges which we were having in .IN domains.

Other initiatives which we had put in place since October 2023 for monitoring include monitoring domain registration. For this enhanced monitoring, we put in place measures like placing well-known and sensitive keywords such as GOV, NIC, and Bharat on a reserved list to prevent misuse. We had witnessed that abuse was generally coming in the name of government schemes, government initiatives, and government departments. Primarily,

we put all these names in our monitoring list so that whenever these domains are registered, we undertake a detailed scrutiny.

Another initiative we have taken is that since May 2024, we implemented a real-time mechanism to flag and block domains made by repeated offenders using email IDs or mobile numbers. We created a database for all the abuse from mobile numbers and email IDs that has taken place in the last few years. If another registration request comes from either that email ID or that mobile number, it is immediately flagged by the system, and we go into further details.

We also started manual verification of the domain name WHOIS details because we were finding that sometimes misrepresentation is done in those fields. We started manual verification for these suspected domains. We are also reviewing and acting upon domain lists received from agencies such as CERT-In, the Indian Cyber Crime Coordination Center, and other LEAs. In consultation, we found they have certain reserved lists that were found to be creating abuse. We put those in our reserved list so they are flagged in real-time for us.

We established a regular monitoring mechanism for domains registered on a daily basis and are systematically scrutinizing them. This is done to prevent cybercrime, phishing activities, and potential reputational damage. A keyword list has been developed on input received from LEAs, the Ministry of Electronics & IT, and NIXI. The list includes very sensitive terms like PMO, Reserve Bank

of India, and Central Bureau of Investigations. Most fraud took place in the name of government departments and government-run schemes. Through this continuous monitoring of domain registration and flagging contents, we were able to proactively identify and mitigate potential threats by reporting them to the concerned institution and the Indian Cyber Crime Coordination Center. We also put RBI and CBI-related keyword domains on the list, as we found they were mostly used for abuse purposes.

This is a snapshot of the implementation. As soon as an already misused mobile number and email ID is flagged, it is flashed in real-time. Through these initiatives, I would like to share the statistics of how we are able to prevent malicious activities. Statistics from law enforcement agencies, the Indian Cyber Crime Coordination Center, CERT-In, and manual checking of eKYC show results. In 2024, we were receiving 78 threat reports. In 2025, it dropped to 23. This year, we have received only one such report. The initiatives we have taken are showing results.

The Indian Cyber Crime Coordination Center is a major cybercrime prevention agency in the country. In 2024, threats were at 2011. In 2025, they remained at seventeen. This year, to date, we have not received any threat reports. Regarding CERT-In, 506 threat reports were received in 2024. It dropped down to 177 in 2025. This year, we have received seven threat reports. The number of incidents has dropped considerably.

A major initiative we have taken is implementing manual KYC, and we are now going into the phase to implement eKYC. More than 3,000 domains are registered per day in the .IN registry. Through this verification process, we found that around four percent—around 150 to 200 domains—are malicious. Once we put them on hold and give reasonable time to prove their identities, only four percent are able to conduct verification. Ninety-six percent of the domains that might have been created for misuse or abuse have been mitigated by us. Currently, we stand at serial number 58. You are all aware of the SerVal report, and we have progressed very well in that as well. Out of four million domains which we are running currently, 2,276 are identified as malicious domains. That is very good progress for us.

We revised the registrar accreditation agreement. Under that, we directed all registrars, including international registrars, to implement mandatory KYC requirements. We collaborated with LEAs during major international events and sensitive occasions, such as G20 and Ayodhya, to ensure cybersecurity preparedness. We developed an SOP and best practices for the .IN registry and submitted them to I4C. This initiative has given very good results. The new registrar accreditation agreement has made our .IN domain more secure. Key clauses include mandatory eKYC for all registrants, maintenance of IP and financial transaction logs by registrars, appointment of a grievance officer by each registrar, and appointment of a local representative with a registered office in

India. These initiatives have sensitized all our registrars, thereby allowing us to mitigate potential malicious domains.

The High Court of Delhi has appreciated the eKYC verification process that NIXI has put in. They acknowledged the process and said it has strengthened compliance, enhanced transparency, and safeguarded the interest of the registrant within the digital ecosystem. Even the LEAs have appreciated NIXI support in mitigating cybercrime in the country. I thank you for this opportunity. Thank you very much.

NICOLAS CABALLERO: Thank you so much, Devesh. [audience applauding] Thank you very much. We have three to five minutes for questions. For the sake of time, we are going to give priority to governments. If we don't have questions from our distinguished government representatives, we can open the floor for other participants as well. At this point, let me see if we have—I don't see any hands online. Let's see if we have questions in the room for Mr. Devesh. Please go ahead.

UNIDENTIFIED SPEAKER: Thanks for your awareness in the registrar. I want to understand better what you mean by threat report.

DEVESH TYAGI: A threat report is basically from law enforcement agencies. Based on their own analysis tools, they analyze different domains. On a daily basis, .IN registries share all created domains with all law

enforcement agencies across the country. Based on their tools, they analyze those created domains and give us the threat report.

NICOLAS CABALLERO Thank you so much. Any other question? I have Chinese Taipei. Please go ahead.

PEI YING Hi, I am Pei Ying from Chinese Taipei, and I also work with TwNIC. We have similar measures, but I just want to request you to share more experience as to whether the measures you described just now are actually taken based on the Indian national law or local law, or if it is just a voluntary system provided by your organization? Thank you.

DEVESH TYAGI We signed an MOU with you today, so whatever our best practices are, we are ready to share them with you. Regarding your questions, we abide by Indian law. These are proactive initiatives. In previous years, we were responding to threats; right now, we are trying to act before that happens. Out of the total 3,000 registered domains, we are able to identify four percent as potentially malicious. Only four percent of those were able to justify the details as per our requirement.

NICOLAS CABALLERO Thank you very much, Pei Ying, for the question. The floor is still open, and please remember that preference will be given to GAC representatives and only then to the rest. My apologies, of course, but for the sake of time, that is what we need to do. Please go ahead.

BANGLADESH Thank you. This is the GAC representative from Bangladesh. I just wanted to know that you have a very good initiative within the country of India regarding threat analysis. Within India, you are getting the information about the DNS Abuse and you are taking certain actions. How about the DNS Abuse of registries which are beyond India? Do you also receive a certain amount of threats like that on a regular basis? What is your action on that?

DEVESH TYAGI That is under discussion. We are discussing the modalities at the highest level, and it is still in progress. I cannot reply to you at present, but we are working towards mitigating that as well.

NICOLAS CABALLERO Thank you, Bangladesh, for the question. I saw a hand over there. We can take one more question. I saw a hand to my right. Please go ahead.

MELANIE ALDONCE: Thank you. My name is Melanie Aldonce. I am from Chile, for the record. Thank you, Dr. Devesh, for your presentation. I would like to ask you if you analyze domains that are registered but not activated immediately—that is, they are not assigned to any host—because it is known that many of the domains that end up being abusive are registered and remain inactive for a long time. Thank you.

DEVESH TYAGI: That is a very fair question. We are aware of this, and I would like to share with you all that we have now automated this process. Every month, we use an AI tool we created to analyze all the domains the registry has. Another report is created and shared with the LEAs as well. We know that certain domains become active after some time, so every month we analyze each and every domain with the registry using automated AI tools. We find those domains and report them to LEAs.

NICOLAS CABALLERO: Thank you very much. Julia? Sorry.

JULIA CHARVOLEN: I do not have a question, Nico, but I am going to read the question in the chat from Jorge Cancio, GAC Vice Chair. Question: How many registrars are commercializing the .IN ccTLD? And do you see malicious registrations related to a wide range of registrars or from just a few?

DEVESH TYAGI Please, can you repeat that?

JULIA CHARVOLEN How many registrars are commercializing the .IN ccTLD? And do you see malicious registrations related to a wide range of registrars or from just a few?

DEVESH TYAGI Each and every registrar has commercial activities through the domains registered through them. For foreign registrars, we are seeking their affiliation with the adopting domain. For all other Indian registrars, we do not go into that detail. Whenever a domain is registered by either a foreign registrant or an Indian registrant, the basic requirement of the registry is that they use that particular domain with total KYC.

NICOLAS CABALLERO Thank you again. Moving on, and for the sake of time, I will give the floor to Martina Barbero from the European Commission and to Gabe Andrews from the FBI. They are going to give us a report on DNS Abuse policy discussions. Over to you, Martina.

MARTINA BARBERO Thank you very much, Nico, and I hope you can hear me fine. Greetings from Brussels. I am sorry not to be with you. In the next

couple of slides, Gabriel and I will update you on the progress we are making on the PDP discussions.

Since the launch of the PDP, as Susan indicated, we decided to formalize the way in which the GAC works by setting up a specific DNS Abuse Small Group. This is the way we prepare for the PDP discussions. The idea to formalize this group followed the examples on registration data, where there was a similar cohort. This group meets very regularly. We collaborate on text, and then as representatives of the PDP in the GAC, Gabriel and I bring this position to the PDP. Since there is going to be a lot of work on DNS Abuse with this PDP and the following one, we thought that establishing this group was a smart idea to ensure that whoever is interested in the GAC can participate in the DNS Abuse discussion without using the wide GAC mailing list for little things that can be burdensome. At the moment, we have seventeen GAC and Public Safety Working Group participants in the group. The group is always open for new members. If you are interested in DNS Abuse and want to join, please let GAC support know and they will add you immediately. We are going to meet very frequently in the near future, so I am looking forward to seeing new faces.

As Susan already mentioned, the launch of the PDP was decided by the GNSO Council in December. The first meeting of the PDP group was held a couple of days ago, and we met for the first time at ICANN 85. The first PDP focuses on Associated Domain Checks, which was one of the three items prioritized in the issue report released last summer. The second PDP will be on safeguards for API

access for new customers, and we do not have a timeline yet for when that will be launched. For the first PDP, we have a delegation of the GAC which is composed of two full members: Gabriel Andrews, who is the chair of the Public Safety Working Group from the FBI, and myself. We also have two other roles. Wolfgang from the German Federal Police is a participant, which means he can intervene in the PDP discussion but does not have a right to vote. Naum from the Greek Police is also participating in the PDP as an alternate in cases where Gabriel or I are not present. He does not have voting or speaking power at this point. We are a strong group and have a long list of observers from the GAC, which is really helpful.

The kickoff meetings at ICANN 85 provided information on the work timeline. On the slide, you see an highlight of the main milestones: an initial report from the PDP is expected in February 2027, the final report is expected in September 2027, and then the GNSO would consider the final report in October or November 2027. Earlier today, we received presentations from subject matter experts on how they conduct Associated Domain Checks, eventual best practices, and concerns. The most important thing to retain from today is that we will have to provide early input to the PDP charter by March 20th. This is right behind the corner, especially considering that ICANN 85 continues until Thursday. We have started preparing this GAC early input within the small group. We have a live Google Doc where input has been provided by different members, and we will continue working on it to make sure we can

meet this very ambitious deadline. With this, I can give the floor to Gabe, who can go into more detail about the next steps.

GABRIEL ANDREWS

Yes, please. This is Gabriel Andrews. Can we flip to the next slide, please? For your awareness, these are the questions provided in the PDP charter that we are being asked to provide answers to. As Martina just highlighted, our deadline to provide this feedback is next Friday, March 20th. We are moving very quickly in this PDP. The chair, Paul McGrady, is keeping us on time. This is what we asked for: swift action in this PDP, and so we are providing swift responses. I wanted to flag for you that we are anticipating providing our draft responses sometime next week, but this may not allow for the longer review period you may be accustomed to. If you are very interested in these topics, please engage the small group that is collaborating on and drafting the responses to these questions.

As we turn our eyes to the future, the next PDP we anticipate will be dealing with API access. Some of you may recall that when ICANN published their informal report, which dealt with associating various attributes of domain registrations with observed abuse, the use of API access was the strongest correlator to abuse of any that they analyzed. This is of very strong interest to us. We are looking forward to engaging on this as well. We anticipate that work will follow the work we just described with Associated Domain Checks. In addition, the GAC has signaled in past conversations and

documents that we have additional thoughts for potential areas of narrowly scoped PDP or similar work that can include proactive monitoring and preventative measures, addressing registration data accuracy, increased transparency in DNS Abuse reports, and a consensus policy on subdomain abuse. We note that many times subdomains are used in phishing in instances where the domain itself might have many subdomain clients. We also have interest in a centralized coordination mechanism for domains that are created through the use of Domain Generation Algorithms, or DGA. Those are all topics of interest expressed by GAC members, and these are all potentially explorable in the future. I think with that, we are going to hand it over to Tomo.

NICOLAS CABALLERO Let me open the floor for questions for you, Gabe, before we give the floor to Tomo. I don't see—ah, there's a hand online from the European Commission. Gemma, please go ahead.

GEMMA CAROLILLO Thank you very much, Nico. I won't take a long time. I just wanted first of all to congratulate all our colleagues from the GAC who are providing significant input to this process. We are very happy to see that it has started on the right foot. I wanted to flag, taking the benefit of the presence of the chair of the PDP in this room, that we would really encourage the PDP group to revisit the charter with the view of shortening the expected timeline. We are seeing one year and a half for the initial report. We are talking about weekly

meetings and preparatory work, so this is going to be really resource intense. We have professionals involved from all stakeholder communities. The issue is very narrowly scoped and is considered non-controversial. This was the most consensuated issue, so we would really encourage that the PDP charter be revised as for what concerns the timeline. The other point I wanted to make is that it is very encouraging to hear from the GNSO that the other issues of importance considered in the issue report will be discussed in terms of methodology. As Gabriel presented, those are big priorities for us. I would flag in particular the issues of addressing registration data accuracy and transparency in the reporting obligations. Thank you so much.

NICOLAS CABALLERO Thank you, European Commission. I have India next.

SUSHIL PAL Thank you, Chair. I am Sushil from India, GAC representative. Congratulations to the GAC leadership for steering all this. I just want to highlight the importance of some of the other areas listed in the priority issues. We should focus on preventive measures, which are very important, especially on the concurrent validation of the registrant's data along with the registration. I understand that there are some concerns that we should not load the GNSO as they are already overloaded with work. We are trying to speed up the process and bring the target much before November 2027. The idea is that cybercriminals thrive on anonymity, and that is what

we should be targeting. We have seen the results shared by Devesh Tyagi regarding the methodology we have adopted in our country. Regarding the question from our Sri Lankan colleague about what we can do about those registrants outside our domain, mandating this validation and verification—taking away the fifteen-day period—solves the problem. I sincerely urge the GAC for advice to the board to expedite this process and bring a contractual amendment in the registrar agreement through whichever possible means. Thank you.

NICOLAS CABALLERO Thank you very much, India. Well noted. We will certainly have time to discuss that during the Communiqué drafting session. Moving on, at this point, I will give the floor to Tomo Miyamoto, who is going to walk us through the Trusted Notifier Network presentation along with Manju Chen. Over to you, Tomo.

TOMORI MIYAMOTO Thank you very much. Let me start by revisiting our annual plan and the Communiqué. As endorsed by the GAC on November 3rd at ICANN 84, the GAC annual plan takes a two-pronged approach. One is advancing the PDP, as Martina and Gabe said, and the other is capacity building. Capacity building includes the tutorial for new GAC members as we welcome nineteen or twenty members this time. We also share best practices which can contribute to DNS Abuse mitigation. One example is the Trusted Notifier programs.

As you might recognize, the scope of ICANN's contractual authority is fairly limited. As you see in the picture, the green box for the ICANN contract is fairly limited, and the definition of DNS Abuse is also limited to things like botnets, malware, and spam. However, the policy issues are much broader than that, such as CSAM issues or IP infringement. In Japan, manga piracy is a big problem. We need flexibility beyond the limit of ICANN's contract, and the Trusted Notifier is one example. I now hand over to Manju for the presentation on the Trusted Notifier Network initiative.

MANJU CHEN

Thank you very much, Tomo. Hello, everyone. My name is Manju Chen. I am the Director of Policy for the Trusted Notifier Network. You have heard presentations from Dublin by Edmund and Jo Fan from .tv NIC and dot Asia about their Trusted Notifier initiatives. We are based on the same concept, but we think bilateral agreements are too slow, so we want to build this network. Once you join, you are part of this network. If you are a Trusted Notifier, your notifications are trusted by all intermediaries in this network. If you are an intermediary, all the notices you receive from the TNN are already vetted and trusted. We are currently limited to ccTLDs in APAC. We have many ccTLDs in APAC who are already very interested and joining, but we are also talking to many gTLD registries globally, and many of them are showing strong interest. With the current interest we are receiving, we estimate to cover more than two hundred TLDs, which means at least sixty percent of domains. We are receiving a lot of interest from those who want to

become Trusted Notifiers as well, but we are currently focusing on getting the intermediaries—registries and registrars—on board. If we do not have the intermediaries, you have no one to send a notice to.

We see a problem with unfair cost transfer. Businesses and brands suffer from phishing attacks or cyberattacks, but they do not have the time or expertise to deal with them, so they outsource to takedown service providers. These providers do not actually have the authority to take down domains because they are not the registries or registrars. They send free notices to intermediaries, and because it is free, they send as many as they can. They are paid to send notices, not to vet them or ensure quality. Intermediaries, on the other hand, deal with this as a social responsibility. If they take down a domain per request, they sometimes get held accountable by civil society or customers. If they don't, they get blamed, and money is just flowing out of them. It is all costs and no incentives. To reduce this cost, they make requirements or criteria stricter. We see this as unfair to everybody.

Law enforcement agencies in your countries are swamped by attacks on your citizens. You feel like ICANN is not doing enough and should be faster. I want to show that we understand the government feeling pressure too. If their needs are not met, they feel they might have to come up with regulations to deal with this. Everybody is blaming everybody. Our solution is to reduce costs and risks for intermediaries so they feel more comfortable and confident to take action. To do that, we have to improve the quality

and accuracy of the requests. We also have to involve governments because you are important. I invite you to join us so we can work on this together. The policies of our network aim to be a multi-stakeholder process. I will share the policy document with the GAC, and we should have a discussion if you have opinions. Abuse is not only happening at the DNS level. To combat abuse across the online world, we will need cross-industry cooperation.

Notifiers will have to verify their notice before they send it to the TNN, and they will have to meet a set of criteria to become trusted. We have heard concerns that some notifiers are only trusted until they get the status and then become untrustworthy. We have policies about that too. Most importantly, we want to reduce the legal risk for intermediaries so they feel more confident in acting on takedown requests. We want to create a chain of contracts that ensures intermediaries have indemnity. All notices will be standardized and codified to make it easier for everybody and ensure there is enough evidence. Because of this chain of trust, intermediaries will prioritize the takedown requests they receive from us. This is how we plan to ultimately reverse the cost transfer.

We will treat law enforcement agencies differently because the requirement for a Trusted Notifier could be difficult for them. All official law enforcement agencies are qualified as Trusted Notifiers, but we in the TNN will help to verify the requests we receive from law enforcement. If you want to join, you must recognize that we follow industry standards in our reviews. Regarding the indemnity issue, we wish LEAs to provide this indemnity when they join the

TNN. We are starting with ICANN, but in the future, we plan to expand to every actor in the online world, including Web2, telcos, and cybersecurity experts. That is the end of my presentation, and I welcome any questions. Thank you.

NICOLAS CABALLERO: Thank you so much. Unfortunately, for the sake of time, we don't have time for a Q&A session. I am very sorry about that. You can contact Manju and her team directly later on. At this point, let me give the floor to Tomo for some final GAC Communiqué consideration suggestions. Over to you, Tomo.

TOMORI MIYAMOTO: Thank you very much. I would like to open the floor as soon as possible, but let me introduce the Communiqué considerations. We have three pillars at this moment. One is the Associated Domain Check regarding PDP 1, which might include the issue of the timeline. The second one is future DNS Abuse policy development, which might include the timeline for PDP 2 and other gaps identified in our input for the public consultation. The third one is the possibility for future efforts and collaborations, including Trusted Notifiers and any other efforts to deal with DNS Abuse. I would like to open the floor for your thoughts. Thank you.

SUSHIL PAL: Thank you. I have already made a comment, but since this is a specific slide on the GAC Communiqué, I would urge the inclusion

of the prevention mechanism for the reduction of the fifteen-day period for registration.

SUSAN CHALMERS: In terms of that suggestion, I believe that was an item included in the issue report. The GNSO, as we heard, is developing a methodology for prioritizing different areas for future work, so perhaps it could fit in there. We will certainly go through a process to develop some shared text for the issues of importance session.

SUSHIL PAL: Thank you, Susan. I think we get that. It has been mentioned as an issue of importance earlier as well, even in the last Communiqué. This is something tangible. If we are looking to expedite the PDP process for associated domain names, the results of which we are expecting a year down the line, let me assure you that this particular preventive measure will have far more impact than whatever we might have from the associated domain names or a subdomain name PDP process. I understand that topics like the subdomain name PDP process will take time and can be scheduled further, but we should sincerely urge this preventive measure as an advice to the board for suitable contractual amendments through whichever possible means.

NICOLAS CABALLERO: Thank you very much, India, and thank you, USA. We will certainly have time to discuss that during the Communiqué drafting session.

Well noted. That's all we have time for. Any final words you would like to add at this point, Susan? Go ahead.

SUSAN CHALMERS

For a few meetings now, the GAC topic leads have invited host country ccTLDs to present, and it is great. We had .rw for Rwanda in Kigali and .ie for Ireland. We really should maintain a library of all these presentations. To be clear, especially for those who are new to the process and this topic, there is a ccTLD policy process and then there is the gTLD space, which is very different and unique to ICANN. It is a multi-stakeholder process that certainly can be informed by national practices, but it is a separate, unique, and different process based upon consensus of all involved. For those who are new to this space, I just want to make sure we understand that these are two different policy spaces. I want to thank everybody for their engagement in this process.

NICOLAS CABALLERO

Thank you so much, Susan. India, is there a hand? I am closing the session at this point. Thank you so much, Devesh. Thank you, Gabe. Thank you, Manju, Tomo, and Susan. Thank you very much, everyone. We will reconvene tomorrow at 09:00 AM for the meeting with the At-Large. Thank you so much. Enjoy your coffee, dinner, or drinks. Thank you. Recording stopped.

[END OF TRANSCRIPTION]