ICANN87 Bali | AGM – Joint Meeting: GAC and ccNSO
Wednesday, October 21, 2026 – 10:30 to 12:00 WITA

GULTEN TEPE

Welcome to the ICANN87 GAC meeting with the ccNSO Session on Wednesday, 21st of October at 10:30 local time. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior, ICANN Community Participant Code of Conduct, and the ICANN Community Anti-Harassment Policy.

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

I will now leave the floor over to Ian Sheldon, GAC Vice-Chair. Thank you.

IAN SHELDON

Thank you. Good morning. My name is Ian Sheldon. I am one of the current GAC Vice-Chairs. Unfortunately, our current Chair, Nico, has had to depart the ICANN meeting early, so he has asked

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.

me to jump in and help chair this meeting along with Alejandra. Welcome.

We have a fantastic session here with the ccNSO. If you have been following for the last couple of meetings, we have tried to take a wonderfully creative approach to our engagements. For this session, we will be looking to hear a little bit more from the ccNSO on disaster recovery. I am joined up here by my colleague, Jorge, and Marco, and I might pass to Alejandra for some other introductory remarks. Thank you.

ALEJANDRA REYNOSO: Thank you, Ian. It is always so nice to join the GAC. We are pleased to have a very good conversation together. This time, the topic that we are going to discuss is disaster recovery. First, I would like to tell you that the ccNSO ran a study group on disaster recovery and whether IANA should play a role or not. Later, we will have a World Café activity that I will explain the rules afterwards. We will finalize with a Mentimeter poll, and that will be the activity for today.

With that, I will hand it over to Peter Koch, who was the study group Chair. Peter?

PETER KOCH: Thank you, Alejandra. Good morning, distinguished delegates. Welcome, colleagues. I have the pleasure to introduce a bit of the work that the ccNSO did in this study group, the nature of which I will explain in a second, as a preparation for the further cooperative

work that we are going to engage in this morning. Can I have the next slide, please? Thank you.

Just to update you, because I understand that not all of the delegates will be familiar with the inner workings of the ccNSO, we usually do not do very much policy work, mostly because the ccNSO, the Country Code Names Supporting Organization, is comprised of 184 ccTLDs, and ccTLDs do their policy work at home, so to speak, within their local community.

At ICANN, in the ccNSO, we develop policy for the IANA, how IANA deals with the delegations or transfer, or more recently with the retirement of ccTLDs. In this case, in 2024, the IANA—the IANA function, the IANA President, Kim Davies—approached the ccNSO with a number of questions derived from observations in their operational day-to-day work, and suggested that there might be gaps in policy that the ccNSO then should explore and maybe fill by doing policy work.

For that, we set up a working group in May 2025—and we have reported about that on earlier occasions in this room or to the GAC—the so-called Policy Gap Analysis Working Group. That recommended a number of study groups to further dive into potential policy questions.

Last year, the ccNSO Council—the Council is the governing body for the ccNSO; Alejandra is our Chair, and we are 18 councillors there from all the five regions of ICANN—the Council established this

particular study group. The study group is the study group on a potential role for the IANA in disaster recovery.

In this year, after having been scheduled, we—the study group, and team members might actually be in the room and would also be available for questions during the World Café or later—the study group did two fact-finding rounds with the colleagues from IANA.

We developed a draft report that we shared with our community, and I will present a number of our findings during this session as an introduction to the World Café.

The important starting point is that there is currently no documented framework for the IANA for an involvement in ccTLD disaster recovery. Cases that you might have heard that happened in the past have been handled on an ad hoc basis, and then after these cases, discussions have come up, or conversations how to be probably more prepared for future invocations.

The mandate of the study group, of course, is scoping the issue and then making recommendations to the Council. The study group is not there to make policy; it is there to shape the question and then make a recommendation to the ccNSO Council whether or not a new policy would be necessary to deal with this question. Can I have the next slide, please? Thank you so much.

All in all, I understand this is a lot of material. The draft report is available. Team members are available; councilors are available if you have any questions on that. I will quickly go through these

findings, and there is also room during the World Café to discuss and explore these things.

Seven findings. First and foremost, business continuity and disaster recovery is a primary responsibility of the ccTLD manager itself. That derives from the independence of ccTLDs and from the managerial and fiduciary duties of the organization running the ccTLD, even if the operation is outsourced. There is always a designated ccTLD manager, and BC and DR, business continuity and disaster recovery, are among their responsibilities.

Another finding—and that might be not news to many—is that ccTLDs operate in a highly diverse environment, governance-wise, operationally, and when it comes to regulatory environments. I work for DENIC, the German country code top-level domain, and we are a private organization independent of the government. There are other variants: ccTLDs run by governments, ccTLDs run by other entities, and a lot of these dimensions. We explore more of that in the report.

Another finding: there is no current disaster recovery for ccTLDs within the IANA framework—we mentioned that already—and the exploration is: would one be needed? Would IANA have to be able to, or are there other ways to cope with the issue?

One of the core findings, though, even if it looks a bit like motherhood and apple pie, but it is important, we would like to stress this, that it is the preparedness rather than the severity or the scale of the disaster, the preparedness that decides whether an

involvement of IANA would be necessary at all. If there is a natural disaster, some other issue that incapacitates part of the registry, the preparedness helps us recover without external help.

Prearrangements for those cases, for example with other ccTLDs or other trusted entities, are the easiest way of intervention. Again, that is covering the preparedness, and that would also suggest maybe an IANA involvement is not really necessary, but it means that the CCs, the registries, need to invest in preparations.

Now, looking at the incidents that also have been reported to the GAC in recent years, the hardest cases are those where the authority of the operator is questioned by difficult situations in a country, to put it this way, or by unclear availability of an operator, say, after a natural disaster, when it is unclear who actually is in charge.

Can the designated ccTLD manager operate or not? But this is a policy decision and has little to do with the preparation part. The processes in those cases where we have a transfer process, for example, for ccTLDs, these processes are designed for smooth handover that takes time, and obviously they are not necessarily suited for emergency cases where communications might not work and also where time is much more pressing than in the regular case.

We came up with a three-tier response, and I think that might be on the next slide, and then we can hand it over. Can I have the next slide, please? Let us take this one, maybe that is okay.

From these seven findings, we derived two recommendations and two observations. For the sake of time, I will focus on the two recommendations here. The study group came to the conclusion that currently the ccNSO does not have to develop additional policy. We recommend to the ccNSO Council no policy is necessary because the preparation work can be done within the current framework. Maybe some procedural questions need to be added, but that does not invoke policy.

Second recommendation—and this might read like a contradiction to the first, but in fact it is an amendment—we do suggest a follow-up study, a next study group with a differently focused question, whether the preparation of temporary measures, invoking a backup operator or something in that direction, whether those methods would need a policy interaction. A caretaker is what we called it, but that was out of the scope for the study group, so we suggest follow-up work.

I guess we can get to the next slide. Yeah, and this is just the checkbox, so to speak. You can dive into this in the World Café if you want. We base all the recommendations and the observations on particular findings. You see that the recommendation not to have new policy is based on almost all of the findings, so we

suggested that has a very reasonable ground, and the same for the other ones. Next slide, please.

Okay. This is the introduction to the World Café, and for that I hand over to Alejandra. Thank you for your attention, and I am open for questions now and in the World Café. Thank you.

IAN SHELDON: Perhaps we can pause to see if there are any questions. Very interesting work here from the ccNSO. I see no hands. Yes, European Commission, please.

MARTINA BARBERO: Just to clarify -- and thank you very much for the presentation, that is very helpful. I just wanted to clarify in a standard situation, the intervention of IANA, I understand that the problem is that there is no emergency situation, that normally when IANA intervenes, it does it over several months or years or I do not know what is the timeline, and now we are trying to see whether in emergency scenarios there could be a short-term intervention.

I was wondering exactly what we are looking at in terms of what are IANA responsibilities in case of incapacity of a ccTLD. Apologies for my ignorance on that.

PETER KOCH: Thank you, Martina. That is a perfect question, actually, and no need to apologize. I understand this is about the emergency

situation and why in that case the standard procedures are not applicable.

The standard procedure, what we refer to as the standard procedure, is the transfer of the registry. There will be an involvement of the potential new operator, what we call the significantly interested parties, as in the local community, and IANA will also engage in some checks on the operator, and so on and so forth. That takes time, as you noted.

The examples that were presented, and LB was one of these cases, where the operator had literally passed away. In that case, the consent of the operator cannot be called upon, as one example. Also, if there is no candidate next operator, what can you do? The standard transfer procedure could not have been invoked. Same situation, imagine an operator gets completely incapacitated.

Emergency means getting the registry, or at least the name service up and running again, so that the infrastructure runs. That needs a bit of a handover, but also at some point, because the registrants might also be affected by the disaster, whatever nature it has, a registry function also needs to be up and running real soon. Again, this is incompatible with the timelines of the standard procedure.

Now, whether a transfer is the right method or what we call temporary measures where things might not be completely handed over, but some other entity gets in, that would be a solution. Had the ccTLD manager designated backup functions—and we suggested either another ccTLD, maybe not the neighbor,

but somewhere else, to cater for larger disasters—these things could or could not be implemented without, say, changing the delegation. Where it gets technical and needs more time to explain, the World Café might be exactly the place to do that. Happy to elaborate on that question. That is very much on the point. Thank you so much.

IAN SHELDON: Cool. Thank you. Absolutely, I think there is opportunities to dive a little bit deeper and have a more fulsome conversation as we work through the next session. With that, I will hand back to Alejandra to explain the next activity.

ALEJANDRA REYNOSO: Thank you. The activity that we will run today, it is a World Café. What that means is that we will have four stations. Station 1, it is over there by the entrance. Station 2, it is by this display. Station 3, on the other side. And 4, closer to our interpreters.

The idea is that we would like you to stand up and choose one of the stations to have a conversation regarding how the interactions of a framework in place or not affect the activities of ccTLDs regarding disaster recovery.

Please do take into consideration that our hosts are speaking on their own capacity, and that not one size fits all, because all ccTLDs are different. They have their own local governments and policies.

Keep an open mind on how ccTLDs deal with different situations, and get inspired by some ideas that might be shared.

The first station would be the combination of having a regulatory framework in place and an operation that is either partially or fully outsourced. Station 2, still having a regulatory framework, but the operation of the ccTLD is partially or totally in-house.

Station 3, it is where a regulatory framework may or may not exist, but the operation of the ccTLD is partially or totally outsourced. And the last combination is Station 4, where we will have no exact regulatory framework and a ccTLD with partially or totally in-house operation.

What we do is we choose a station, we ask our hosts to introduce the topic, we need to select a rapporteur because afterwards we will hear from everyone. After the 15 minutes, we will ask everyone to change stations, so you can hear other perspectives.

When you arrive at the next station, the hosts will recap what was discussed previously, so we can build upon that conversation.

Finally, we all return to our seats, and we will hear the reports from all four stations, so that we don't miss anything by not going to all four stations. If we are ready, let's go. Please stand up and choose your station.

IAN SHELDON Could I get each of the rapporteurs from the stations to join us up on stage, please? Yep, come on up. Bruce -- Two stations -- How many other stations are we missing?

ALEJANDRA REYNOSO They're here.

IAN SHELDON Okay. Great, thank you, all. I hope you had a good conversation. I know over at Station 1, we had an excellent discussion. We might take a little bit of time for each of the rapporteurs to report back about the key takeaways from each station. And perhaps we can kick off with Station 1 with Bruce Tonkin. Thank you.

BRUCE TONKIN Thank you, Ian. Number one, first off the rank here. We had two groups come through with some interesting questions and comments. We talked a bit about the fact that for disaster recovery, you want to have your primary site a long way away from your secondary site. Generally, if your primary site fails, you want to be able to bring the registration system up on a secondary site.

For big countries like Australia, it's pretty easy to do all that within one country because the distances are vast. The difference between Melbourne and Adelaide is a plane flight away, basically. But we noted that for some other countries that are much smaller, such as countries in the Pacific where they're an island, if there's a natural disaster, it will affect the whole country, not just one city.

And so talked about that you might need to have an arrangement with another country where the data can be stored.

One of the GAC members had asked a question about had we looked at data embassies, and my understanding of that is that there are locations where people trust storing their data, and that the data is protected under some appropriate law.

For us in Australia, that we would look for another country that had privacy laws that are similar to our laws as an example. We also had questions about what happens if the cables get cut. There have been cases where Pacific Islands have had their cables cut, and therefore they're not connected to the rest of the world.

Australia has a limited number of cables, and it's probably possible that if you were targeting those cables, you could take them out. And so the concept is that you'd want to look at satellite backup. And I know some of the Pacific Islands also came from GAC members to say that they had arrangements with satellite providers to make sure they kept connectivity.

There was some discussion about whether the satellite would have enough capacity, and we noticed DNS generally uses a very small part of a link capacity, and then local content could still be operated within the local area, even if the cables were cut.

And then the final discussion point was DNSSEC, that you might have the ability to bring your registry up at another location, but how would you sign it with your digital signature? So that you need

to actually look at disaster recovery for your signing infrastructure as well as your DNS infrastructure. In other words, that you can sign the zone file or sign the DNS records from another location. I think that was a summary, Ian.

IAN SHELDON Thank you, Bruce. Perhaps we can go through all of the stations, and then if there's an open discussion after that, we can open the floor up. Station 2. Diego or Thiago? Please.

DIEGO ERNESTO LUNA Hello, everyone. My name is Diego Luna, part of the .co, and basically in our station, we told everyone that we are a government institution, that we run the .co, but we also have a three-arm model. And part of that three-arm model in place that we have a public policy, but also a contract with our registry operator, and we have some specifications and clauses with a very strong SLA agreement in that contract in order to comply that all our services of the time, the .co is running without any problem.

But if we have any problem, we have in this contract determined that if they breach an SLA, we will have an EBERO to run mainly EPP and all that kind of stuff, registry services. And what we have is basically a contract that determines that they need to inform us every single week, and monthly again, if they breach any of our SLA in order that we have an EBERO event, or if everything is turning good.

And also, in addition, every single year, we have an EBERO test that actually is with DENIC in order that we need to be fully in charge if something happens, and what are the communication that we're going to have with the EBERO in order to have the .co uptime in case of need.

In our station, the main questions was between the relationship that we have as a ministry with the EBERO. Basically, besides the contract that we have is between the ministry and our registry, and the registry with the EBERO, the contact in case of a disaster event is with the ministry. Actually, Thiago is the contact that we have for these matters.

Another question is what is the SLA that we have, so we have that in our contract, that as I told you is very strong, it's almost 99.9% that they need to comply every single day, every single month. After that, we determine if there is kind of a breach or no, that actually never turns out. And I guess that's it. Thank you.

IAN SHELDON: Cool. Thank you. Perhaps we can move on to Station 3. Over to you, Benjamin.

BENJAMIN HARBICH: Hello, everyone. I'm going to present you what we talked about on Station number 3, which is about the case of no regulatory framework on partially or completely outsourced operation. We have discovered that this mostly applies to the region of the Pacific

or Caribbean and Africa, that there is where this construction happens the most.

Then we talked about the important principles of this kind of operation, and one of the first things is that the accountability stays with the manager, and that this is not only a responsibility, but a very important task. Because you can delegate the operation, but you can't delegate your responsibility. You have to check that this work is done carefully and correctly.

Then on a second, that as there is no regulatory framework in place, then everything has to be fixed in contractual agreements, and there the manager has to be very careful to do this work as good as possible to be able to have his accountability and outsource the work correctly. There you also have to define all the performances of uptime, downtime, what happens in case of a disaster, who will be responsible of what.

And finally, we talked about exterior influences that are outside of the ccTLD, for example, other large TLDs that might hinder your possibility to make disaster recovery, and also connection with other smaller ccTLDs when you all rely on the same service provider. There's a diversity of providers necessary to be able to do disaster recovery. Thank you very much.

IAN SHELDON: Thank you. Very interesting. And finally, Station 4. I can see Everton's joined us. Please.

EVERTON T. RODRIGUES

Thank you very much. On Station number 4, we have presented the case of .br for Brazil, and as we have been running the service since 1989 without any interruptions, and since 2003, we have NIC.br operating the service in a private entity.

Our main point during the presentation was to say that we have built partnerships over the years with several institutions, several ccTLDs all over the world to ensure that our services will be running, and theirs as well because we shared this infrastructure with them by receiving their copies as well.

Brazil is not a country that could be affected possibly by one single natural disaster, but as we have copies also of .br in every single internet exchange point, and NIC.br operates 40 of these internet exchange points in the country, if a given location is unavailable, whether by a natural disaster or by any other instability, it can be reached by another facility that we have in our internet exchange points.

.br itself operates in two different buildings in São Paulo, so we have a multi-user building that we have been working since 1996, and more recently, in 2015, we have built our own infrastructure, also building another one which will be launched soon. Those are initiatives that allows us to keep the service operating without any interruptions.

From the discussion that we had, two topics that emerged, and which are very interesting, and that I would like to highlight among the many that we have had, two of them that I would like to bring to the table is that one of the considerations was that you must also be aware of where you are going to put your data when you are considering the business continuity of your own ccTLD.

For example, if you have privacy concerns in your ccTLD and you would like to have a backup data elsewhere, you should ensure that you have a likewise or a like-minded institution that will process your information in that other location. Otherwise, instead of having a business continuity program, you may end up with a point of failure for your continuity. This should be taken into consideration.

Another one which is very interesting is that, especially for smaller ccTLDs, perhaps this could be interesting, that you may not have all the data and all the instructions to keep your service running on hand, but ISOs may be a very good point for helping you to know more about business continuity programs.

Those are the two topics that I would like to bring to the table. Thank you very much.

IAN SHELDON Thank you. What we're going to do now is perhaps open the floor for a discussion, but while I wait for everybody to think of their questions, we are just going to put the Mentimeter QR code, so

please take out your phones, join the Mentimeter, and we'll get to this point after we've had a little bit of time to discuss.

With that, I might open the floor to see if any questions or other comments people would like to make or reflect upon from the -- Please. Over here, and if you could please introduce yourself and your affiliation. Thank you.

FATMA DEMIREL

Hi, this is Fatma from Türkiye, .tr ccTLD. Firstly, thanks to our ccNSO community for this session. It was very nice. And I recognized that Brazil separate their internet and the telecommunication infrastructure. It is interesting because when an emergency occurs, how can they communicate? I'm wondering, and also we are nowadays thinking about separate telecommunication and internet infrastructures. Because of that, I'm asking that to whole community. Thank you.

EVERTON T. RODRIGUES

Thank you, Fatma. Internet services in Brazil, they have been -- Let's go to another part of it. Telecom operations are regulated by Anatel, which is the telecom regulatory in Brazil, and internet services have their own regulations which are not subject to Anatel. This allows us to have internet services being flourished in the country.

But on the other hand, Anatel has a seat in CGI.br, which is the Brazilian Internet Steering Committee, so that allows this

communication to happen between both parts in the country, and in a monthly basis CGI.br meets to discuss internet-related aspects and development in Brazil. This is one point of interaction that they have.

IAN SHELDON Thank you. Any other asks for the floor? Martina, European Commission, please.

MARTINA BARBERO Sorry for taking the floor again, but if no other question, I'll ask Bruce, because you mentioned disaster recovery for signing infrastructure, I think. And I wanted to know how it looks like, because it's the first time that I hear about that.

BRUCE TONKIN Thank you for the question. DNS is often spread around the world through what are referred to as Anycast nodes, so you have a number of nodes that have a copy of the DNS. Only a few nodes have got the capability of actually signing the zone and then being the distributing zone. Typically, in your primary site, you have a primary site and it also has the primary signing infrastructure. If you're going to fail over to another location, you also need to have signing infrastructure at that location.

IAN SHELDON Thank you, Bruce. Any other questions? Giacomo, please.

GIACOMO MAZZONE My question is simply to understand if this exercise is starting from concrete cases and example, or is just a theoretical exercise that you are doing expecting that something could happen? And if there are concrete cases from which we have started, could you mention which ones?

PETER KOCH Thank you, Giacomo, for that question. As I introduced in the slides, the whole exercise was initiated by a question from IANA based on their experience. I referred to the Lebanon .lb case. There were a number of others. Off the top of my head, I'm not exactly sure which they are, so I'm not putting anyone on the spot right now in here.

The team, though, did not investigate these particular cases, just because not for all of them the information was publicly available, and we were not in a position to go into details.

More on the methodology, though, we were flying at a different level of abstraction, so we grouped these things, and the report has a bit more information on this. We grouped the kind of disaster, and that could be natural disaster and other reasons. Again, I'm sorry, I can just point to the report at the moment.

But the cases, the use cases that we have in there or scenarios, as we called them, they were fictitious. And as they usually say on TV, any similarity with real cases would be coincidental, and we all

know it's a lie. But we weren't lying; we were doing the abstraction. I hope that helps in a bit.

So the task was also not to investigate -- Maybe to clarify that, the task of the study group was not to investigate these cases, but to make policy-making suggestions from that abstract level. But it was definitely initially informed by questions on the table. IANA's experience was real; that was not a table exercise. Hope that helps, but happy to elaborate offline. Thank you.

IAN SHELDON Thank you. If I see no more hands, perhaps I can give the floor to Alejandra who will take us through our final exercise.

ALEJANDRA REYNOSO Thank you, Ian, and thank you, everyone. In case you have not been able to join Menti, the details are in the Zoom chat, or below in the slide you can see the code so you can join.

What we want to do with this Mentimeter is gather the sense of the room on the activity that we did today. I'm happy to see that it has been mostly interesting, useful, interactive, and insightful, which means that we accomplished the goal for today, so thank you for your input.

With that, I see they're still incoming, some more responses, but we can -- I think we can move to our next question.

So this one has four questions where we would like to know whether you strongly disagree or you strongly agree, still on the method and format of this activity: Did you enjoy the networking? Did you like the format? Did you learn something useful? Did you value the dialogue? And if you would like to do this again.

Part of the goals that we put on ourselves with this particular type of session is that we want to get our communities closer together. We want the ccTLDs and the GAC representatives to know each other, to talk to each other, and learn from each other.

It's the basis of what the ccNSO is all about. We are a platform for information sharing because we know the world is diverse, and it's good to know what others are doing and get inspired from them and adapt what we can to our own local realities.

Seeing very positive feedback. Thank you so much for the input. And then if we can move to the next one, please.

We will have this open a little longer. We, as I mentioned, like to stay in touch with the GAC, and we would like to meet as often as the schedule allows, and for this, we would like to know which topics are of interest for us to discuss, whether in this format or similar format. But I think topics are in -- we want to be able to give you what you want and not what we think you want.

And some of the input is getting here: DNS abuse, data embassies, best governance model for ccTLDs as in best practices,

cybersecurity and resilience, okay. How is the registration policy developed in your country for the ccTLD?

More information about existing policies for ccTLDs, DNS abuse, cooperation between ccTLDs, geopolitics, governance and models diversity.

Maybe we can scroll a little bit down to check what's incoming. Thank you. What the landscape really looks like. What should cooperation look like with governments? That's a good one. Debate between different ccTLD operators.

If anyone would like to speak to any of this or they would like to describe it a bit more, in particular, that debate, it would help to know which topic in particular would you like us to debate. I'm trying to make sure I have my Zoom open to see for hands. There we go.

Engagement, labeling domain names owner as critical according to NIS critical sectors. What governments do to encourage their citizens to support the local country code. The involvement of ccTLD operators in internet governance. I'm not reading them all, only some of them, but just to keep some on the record. We will publish this result, so we all have them available.

Are there any more incoming? Just -- Oh, yes, thank you. IDNs and universal acceptance, DNS abuse, ccTLDs, UA, DNS infrastructures, okay. That's a good way to put many topics in one. How to handle transition as some of the older members of the community that run

ccTLDs for their country die, okay. Thank you so much. I think we have good food for thought. Anything that catches your eye, Ian?

IAN SHELDON

So thank you for the input. I think we will go back out to the GAC once we've done some consolidation and certainly try and focus some of this input. I know a lot of these topics have come up in previous GAC discussions already, so it's obvious there is keen interest to continue to have this exchange with the ccNSO. So this won't be your only opportunity to provide your thoughts on where else this conversation should go.

ALEJANDRA REYNOSO

We have one last question, it's a very easy one, it's an overall evaluation for this session. So if we can go to the next one. And we can keep that open with our closing remarks. I'm very pleased to see that there was a lot of conversation flowing in all four stations and that the activity was well received. The summaries of all stations will also be published and shared with the GAC and the ccNSO. And we are hoping to keep working on keeping everyone updated with what we are doing, and with that, I'll give it back to you, Ian.

IAN SHELDON

Thank you very much. As I said before, the GAC continues to very much appreciate these sessions and the engagement we have with the ccNSO. As I've said in previous sessions, I think the ccNSO and

the ccTLD community have a lot to offer to the GAC, and they're doing a lot of really interesting creative work. So the more the GAC can get across some of this broader work, I think the better our positioning and thinking will be.

So with that, please join me in thanking the ccNSO for the session today. I should note that the memorial to Bertrand de La Chapelle will be on in this room at 12:10, otherwise the GAC will resume its communiqué drafting at 13:15. Thank you.

[END OF TRANSCRIPTION]