ICANN85 Mumbai | CF – ccNSO: Internet Governance Liaison Committee Session
Tuesday, March 10, 2026 – 10:30 to 12:00 IST

CLAUDIA RUIZ

Hello and welcome to the ccNSO Internet Governance Liaison Committee session. My name is Claudia Ruiz and I along with my colleague, Joke Braeken, are the participation managers for this session. Please note that this session is being recorded and is governed by the ICANN Community Participant Code of Conduct, the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy.

Please observe the following guidelines to participate in this session. They will be posted in the chat for your reference. During the session, questions or comments submitted in chat will be read aloud if put in the proper form as noted in the chat. Interpretation for this session will include English, Spanish and French. If you would like to speak during this session, please raise your hand in Zoom and when called upon, virtual participants will be given permission to unmute.

On-site participants will use a physical microphone to speak. Please state your name for the record and the language you will speak if speaking a language other than English and please speak at a reasonable pace to allow for accurate interpretation. Thank you and with this, I will now hand the floor over to Annaliesa William, Chair of the IGLC. Thank you.

ANNALIESE WILLIAMS

Thank you, Claudia. Good morning, everyone, and hello to those of you who are joining from home in other time zones. My name is Annaliese Williams, I'm Chair of the Internet Governance Liaison Committee and this session has been organized by the IGLC. The IGLC has been established to encourage and facilitate discussion amongst ccTLD managers in Internet Governance processes, including those outside of ICANN. So, we sort of meet to share information and discuss national and regional policy and regulatory issues and their impact on ccTLDs.

For the past year or so, perhaps even a bit more, our focus has been very much on the 20-year review of the World Summit of the Information Society and the future of Internet Governance will probably continue to be a prominent theme for this committee going forward, but we have decided for this session that we would explore some of the regulatory developments from the perspectives of ccTLDs and also touching on a broader theme as part of this discussion about the importance of stakeholder collaboration in finding solutions to shared problems.

So, we are joined today by Devesh Tyagi, who's the CEO of NIXI, our local host here, so thank you for joining us. We also have Kristian Ørmen, Vice President of Registry Services at the Swedish Internet Foundation, Vivien Maidaborn, the Chief Executive of InternetNZ, and Jordan Carter, who's the Internet Governance and Policy Director at auDA.

So each speaker today will have about 10 minutes for a presentation and then there'll be a few minutes after each one for questions for that speaker and then before we close, there'll be an update on the work of the IGLC, our work over the past year and a progress report on our update to our forward work plan and there'll be an opportunity for you to provide input on and discuss the proposed themes for our future work plan. But now let me pass to our first speaker, Devesh, over to you. Thank you.

DEVESH TYAGI

Good, morning. Thanks for giving me this opportunity. I will be presenting regulation, good morning, all. I will be presenting regulations impacting ccTLD specific to the .in domain. So, about NIXI, NIXI is an organization which has been established in 1989, I would first brief this.

The National Internet Exchange is a not-for-profit organization under the Ministry of Electronics and IT and is dedicated to strengthening India's digital ecosystem. Primarily we operate in three domains, one is the .in registry, we are also operating internet exchange points across the country, and the third operation we undertake is the IRINN operation, that is we allocate IPv4 and IPv6 addresses.

So, we are typically looking after the digital ecosystem infrastructure in our country. And for us, the .in domain is more than a domain, it's India's trusted digital identity based on security, reliability and a strong foundation for self-reliant digital future. You

see our country is having more than 1 billion plus users currently and all the primarily services from the government to the citizen is given through this digital ecosystem that we have created.

So, primarily about the history of .in registry operations, we were allocated in 1989, we started our operation in 2003 and .in domain operations were started at NIXI in 2004. However, we made a significant progress after announcement of Digital India Program by the Honorable Prime Minister in 2015 and 2016 onwards we are able to get a growth, rapid growth in our digital ecosystem.

In 2020s we had created an environment that will be fulfilling, giving the services to our citizens through this digital ecosystem and today, we had made a good progress and we had created a digital public infrastructure as well for providing citizen services in our country.

So, legally structured in India that we are basically adopted as our constitution says that separation of power we had adopted and there are three basic key constituents to that. One is legislature, another is executive and another one is judiciary. And those all three legal infrastructures work independently of each other and that is the beauty of our constitution, and as per the legislature, they are for enacting the laws, they comprise the president, Lok Sabha and Rajya Sabha.

For executive we have implemented the administrative laws and it is led by the president, prime minister and council of ministers. Under judiciary it interprets law and safeguards of the constitution

which includes supreme court, high courts and the subordinate courts across the country.

And currently, our .in domain is among top four in Asia-Pacific region as per the DNIB quarterly report quarter 2025. And there is a shift which we had undertaken during the way we do the domain registration in our country. In the past there was no verification framework which we were adopting, there was no proactive monitoring of the controls that was put in and in present, we are having verified registrations and who is detailed is also verified as per the current norms and we have made the mandatory the KYC process to take the .in domain.

In the future, we are trying to adopt the emerging technologies as well as in the domain including AI in the domain allocation which will be, through which we will be doing AI powered who is monitoring, intelligent risk detection and productive fraud prevention as well.

Through a legal perspective that legal foundation of .in, .in is the India's most country code domain that is managed by us. The governance is through the registrar accreditation agreement that is executed when we onboard the different registrars. And these are the present concerns which we were witnessing under this particular old RAA, we were getting very misuse of our .in domain.

And for that we are now, in the last one year, we had strengthened or changed the RAA framework and under this we had made the following amendments that have been amended to tighten

compliance requirements. It has announced focus on KYC verification, data accuracy, monitoring security standards and time bound response to the complaint and the legal directions by the various court across the country.

We had witnessed that there were certain cases in which we were not getting the proper response from the registrars as to the registrar details, which we, in case there was some misuse and then some legal agency or our courts were asking for those details. And for that purpose, only we had strengthened the RAA framework that we had made certain KYCs mandatory to onboard on the registry system.

This is just for the use, misuse, avoiding the mitigating the misuse that was happening in the .in domains. So, I am happy to share you that recently under, there is a Dabur which is a very prominent powerhouse or business powerhouse in our country and under that we had received a judgment and they had also recognized the steps which we had taken.

In this particular case, the High Court has highlighted the need for structured India framework for domain governance and has appreciated NIXI's initiative that in the .in domain and it has observed that a nodal repository framework similar to NIXI system should serve as a template for the wider regulation strengthening.

So, we were able to, through this RAA amendment, we were able to put in place a framework wherein we were able to mitigate misuse of the .in domain. And through this, what we are willing to go in the

future that we'll be adopting various High Court directions and through which we'll be strengthening our transparent, accountable and legally lowest .in ecosystem, which will be providing clarity and a structured compliance environment, helping the registrars to mitigate risk and operate with a larger legal entity, sir.

And I would like to share that this is the regional scope for us, where we are having economic significance and I am also sharing with you the key industries which we currently dealt in APAC region. And what is the strategic importance for .in domain for all of us?

It is a major contributor for global GDP. It is critical for global supply chains and it is high growth and investment potential. So, we have to leverage that.

And I would like to share that how we want to proceed further, that we are facing today's challenges exceed the capacity of one single state to manage alone. So, I would call all the ccTLDs to help us in adopting the framework or to amend the framework as per the future requirements. It's left unaddressed those tasks in case we are not managing these, we are not addressing these things. It left the risk certain present and the future generations.

We are also endangering the welfare of our planet. Without proper management, technological advances, this will only be benefiting a few. And when responsibility is governed, knowledge and technology can create a better future for all of us. The goal is to build an environment that is open, stable, free, interoperable,

reliable, secure and inclusive for and sustainable for all of us. So, with this, I would end my presentation. Thank you very much.

ANNALIESE WILLIAMS Thanks, Devesh. Are there any questions for Devesh?

VIVIEN MAIDABORN Thank you, Devesh. It was super interesting and I particularly appreciated your slide on the strategic impact of the region. And I really agree the better all ccTLDs across the region are doing, the kind of the cleaner the DNA space is. So, what would be your top couple of hopes that we could do together across the region that you think would make a strategic difference?

DEVESH TYAGI Yeah, because there is the framework, the RAA amendment which we undertaken. I think there will be the same policies across the different ccTLDs. If we can share the details of that and then whatever best practices, we will find that and we'll be adopting that, it will make a great difference for all of us.

ANNALIESE WILLIAMS Any other questions? No? We may have time for further discussion at the end, so don't run away, Devesh. But thank you for that presentation.

DEVESH TYAGI Thank you.

ANNALIESE WILLIAMS We'll now pass to our next speaker. Kristian, over to you.

KRISTIAN ØRMEN Thank you. So, my name is Kristian Ørmen. I'm from the Swedish Internet Foundation. We are the delegated manager of .se, but we also run the registry for .nu. I'm going to try to talk about the most significant regulatory changes in Europe over the last 10 years. My own background is that I used to be a registrar. I have been working with domain names since I was a teenager. I was at the DNSO Council and the Registrar ExCom when we were implementing GDPR. So I'm going to include a couple of stories from that time as well.

But before I go to that, I really want to highlight how important it is that we cooperate with each other, especially ccTLDs and the government. We must understand what we do will have consequences in the marketplace. We also have to acknowledge that something might be better directly in the law to regulate and something might be better in the domain policy to regulate there. And together we should find where the best place is to regulate the different things and understand the consequences of the things we put into our regulations.

I'm a true believer that most governments and ccTLDs have a common goal of a secure and stable Internet. And to make sure

that is happening, we should work together. Most ccTLDs have expert knowledge and we should make sure to share that. And we should also make sure to hear the government, what they have on their mind. And also, so we understand very early in the process what might be coming in the future.

So, if we scroll back to GDPR in 2018, I was working at a registrar and we were quite worried about what will happen when GDPR goes into effect because we could see that a lot of, especially gTLD policies would be affected. And for example, that we wouldn't be able to do transfers. And for those of you that don't know the old transfer process for gTLDs, it worked the way that we would check WHOIS for the email address to the registrar and we would send an email to the registrar to ask for approval to do a transfer.

And since we could see with GDPR WHOIS might go dark, the emails might not be there, we can't do transfers anymore. And the ICANN policy process is quite slow. So, ICANN made a temporary specification very close in the game, very close to when GDPR went into effect and basically changed the transfer process overnight since we couldn't send these emails anymore. And the security went down a bit in that process.

Most ccTLDs though, especially in Europe, were ready. We as ccTLDs can change our policies easier, but of course we should do it together with others. So with WHOIS going dark, a lot of people were using that information for like, for example, abuse mitigation and so on. And it seems like the regulators in EU didn't understand

that basically WHOIS would go dark when GDPR came into effect. And they were trying to figure out how do we work with this in the future.

We get a lot of pressure from law enforcement and others to get access to this information. And I remember a specific conversation I had here at ICANN with one of the GAC members. And he was like, if you can't fix this, we will need to regulate it at some point. And I was looking, I do understand that, but I don't see how we can fix it with such huge GDPR fines. If we don't handle personal data correct, we have no way to just publish this data and give it out.

So that's what we did with this regulation in effect. So, if you follow EU, you would see that they then later came with a regulation that, well, is mainly focused on cybersecurity, but it also included a fix, so to say, to the problem with WHOIS going dark. And they have included an article that says that we have to collect registration details for the registrant's name, phone and email, so there's contact information.

And they do require us to disclose this information within 72 hours to request this with a lawful request. That still doesn't mean that we can just put the information out there in public, but we do have to disclose it within a reasonable time. For us, that means that we have to handle every one of these requests manually, because we have to make sure that it's a lawful request.

So, when I was preparing for this session, I just read up also on the article again, and I see I forgot something very important here on

my slide, but that's because it comes so natural to me. It actually also requires registries and registrars to cooperate, which I would say shouldn't need to be in a regulation. That's something we do every day already.

So, I would say some of this article is going a bit far in the sense that people haven't really seen how far it will go if you have to verify a registrant. Like, for example, if you know your customer type of requirements, it will be extremely difficult to register a domain. So, I would say everyone in Europe right now is trying to figure out where do we set the right level, and it seems like many countries are setting the needed requirements at different levels.

So, that will still be a work in process over the next couple of years, where registries and registrars are trying to find the right level and make sure to, of course, comply with this regulation.

There we go. So, one thing that they did not include, which was maybe a bit surprising, was the postal addresses. And since it was not included in these two regulations, but it was included in the Swedish law that regulates .se directly, we were talking with our government, and we're like, we actually don't see that we need postal addresses in our registers, so we would like you to take that away from the law, and we talked quite a lot about it.

We also looked at our data, and I was like, okay, a lot of this data is incorrect. We have the organization number of our registrants also, so we could compare the data with the official company database, and we could see how much of this data that was not updated and

incorrect. So, it didn't really help us, and we don't send letters to our registrants, so we didn't feel that we needed it.

So, we were quite happy that this was taken out of the law requirement, and we have started, because we want to give our registrars a long time to do any changes, so we started just making it optional by 15 of January when the new law was in effect. By June, we will start ignoring it if they keep sending it, so they don't get an error in their technical system, but we won't save the data anymore, and from September, we are starting to clean our database from all the old postal addresses.

Let's talk a bit about abuse. The NIS2 is also about cybersecurity, and of course, one of the reasons they have this focus on registering data is because if there is abuse on a domain name, we of course want to know who operates that domain name, so we can get the abuse stopped.

It's important to say, especially from our view, we don't want to be internet police. We don't want to take decisions that should be in court or police. We want to make sure that if a domain is closed down, it should be part of a good legal process.

It's also important to say that content moves even between TLD. There was a case in media quite recently where, for example, a domain by an American TLD registry was closed down because of a court order. In .se, it was closed because of incorrect data, and they just kept adding new TLDs to host the same content, so closing

down a domain doesn't necessarily mean that you remove the content. It will be darknet. It will be on new TLDs.

It will be directly on the IP addresses, so like a domain and content are two very different things. So, my probably most important takeaway today, especially if you are in Europe but also in other countries, is that EU have started to be, I would say, very happy to include domain deactivations and deletions in more regulations.

Regulations that it's not internet at all. For example, financial regulations and other regulations where they have conveniently added a single line that if, for example, a financial institution doesn't comply with this regulation, it could end up in deactivation of that domain, a direct regulation on registries to take down that domain, and we really have to watch this space, and we have to cooperate with our lawmakers and teach them about the consequences of taking down a domain, and especially because that one line can be so easy to add in a regulation, but it will have unintended consequences on a longer run.

Quite often, a domain will include a lot of legal content. At the same time, it could be illegal content. We see a lot of takedown requests that we get. For example, for domains like file hosting sites, they might host something illegal, but they also have a lot of legal material, so takedowns like that should go to the hosting provider and the owner of the site instead of the registry. Yeah. That was it. Any questions?

ANNALIESE WILLIAMS Any questions for Kristian? Yes, go ahead, please.

DAVID CHRISTOPHER It's David Christopher here from CIRA. Just you mentioned on the postal addresses and no longer collecting those, is that in part because of GDPR as well? I know I'm not a GDPR expert, but I know the principle is like don't be collecting and don't store information unless you need it for a legitimate business purpose, so just curious.

KRISTIAN ØRMEN We already did not show postal addresses in our WHOIS because we had no way to know if that postal address was personal information or not. Even though it could be a company, it could still be a personal address. It was taken away in NIS2 as a requirement, and for us, because of GDPR and minimization rules, if we don't need the data, we should not collect it, and that's also one of the reasons we were like we don't want that data anymore. So, yeah, definitely also because of GDPR. Thank you.

PIERRE BONIS First of all, thank you very much. Pierre Bonis .fr, for the record. Thank you very much for the presentation, and I think we share your vision on what is happening and the usefulness of these regulations. On the postal address, just to share another experience, as long as .fr has geographical eligibility, that he must

be a resident in the EU, we think that this is still a legitimate reason to collect postal address. Even if in the directive this is written that at least name, telephone number, and emails, when you have geographical eligibility, you can collect it.

KRISTIAN ØRMEN Yep, of course, but for both .se and .nu, we don't have any requirements on local presence, so you can register .se and .nu domain from anywhere in the world.

ANNALIESE WILLIAMS Any more questions for Kristian? No? Okay, we will move on to our next speaker, Vivien Maidaborn from InternetNZ. Go ahead, Vivien.

VIVIEN MAIDABORN Kia ora tatou. Good morning. I wanted to start with a proverb, "a whakatauki, from Aotearoa" New Zealand that we use in our organization often. Together we weave the mat in terms of the internet for future generations. And obviously, one of the reasons we come to ICANN is to weave the mat of the internet for future generations. So, I just wanted to share that, really in respect of our hosts here who have been weaving the mat of hospitality so beautifully for us at this ICANN.

Others today have been talking about regulation processes and their engagement in those. And I love that because in New Zealand, we're just really at the very beginning of potential regulation. In

fact, the cyber security consultation is just launched this week. So, thank you, all of you. I'm up for learning from each of you.

I wanted to look through a slightly different lens today. Can I make this work? Yes, no. I wanted to look through the lens of how a ccTLD prepares to be effective in this space, the regulation process, the engagements that are necessary. Both with government and indeed with the broader internet communities that we serve. We've become really conscious of this work in Aotearoa, New Zealand because we've had a dramatic change in our organizational context. And that's caused us to look carefully and strategically. I wanted to share some of those thoughts.

You know, what's the permission space in which a ccTLD develops policy positions to influence regulatory outcomes? And actually, while we're asking that question, what's the process of influencing regulatory outcomes? It's kind of a bit of an arcane art, as far as I can tell. So, that's kind of what I wanted to cover off today.

In Aotearoa New Zealand, we have traditionally had about 400 members of our incorporated society. We are a registered charity, and so the social impact we have as an organization occurs through our authoritative voice and social policy discussions in communities, through money that we disperse back to the community every year, through actually running the ccTLD for the good of all New Zealanders, to include all New Zealanders with a sense of being equitable.

And by and large, our members have aligned with those values. But in the last year, as politics globally has polarized, our membership has grown from about 400 to 5,000, and the membership reflects the same polarization. People who are very opposed to supporting our indigenous people, the Māori people in any way, who believe that anything said on the internet is fine to say without consideration for impact on other people, and who aren't interested in principles that we might all have talked about a lot, like connectivity to the last mile.

So, what happens in a ccTLD in the policy development or regulatory space when membership is so polarized on every issue? The danger that we identified was that we move from being a technical voice in those social policy or regulatory processes to more like an ideological lobby group for a particular perspective. And that felt like something we needed to add to our risk register and consider from lots of different points of view.

The question arose for us, how does a ccTLD develop responses to regulatory action of the government or indeed broader public policy positions when members who are the kind of legal owners of the ccTLD are so polarized?

I want to say to you that the very first thing that has happened for us is we've become much more conscious about those processes. And that consciousness includes why, what, and when. One of the interesting things about incorporated societies is that they usually are set up to add benefit to the members of the incorporated

society. But ccTLDs are a little different because we are set up to benefit all the people who participate in the internet in Aotearoa or even broader.

So, that's sort of a paradigm shift for members of an incorporated society. They need to think of themselves as being there to support the objects of the society rather than for the benefits they get from being a member. And I think we're just at the beginning of communicating that to our members effectively actually.

The risk in not having a really conscious approach to this is that public policy or communications can further cause polarization, be grist for interest groups, agendas, or even encourage Board members to seek to be involved in operational matters. So there are very good reasons why as a ccTLD we found it important to get very conscious about this work.

So, what do we do about that? And that caused me to think much more about what are the solid foundations in such a polarizing environment that many of us find ourselves in. And the question that sat with me for quite a few days was what is bigger, deeper, more important than membership views on any particular issue for a ccTLD registered as an incorporated society?

And actually, it's pretty obvious. What parameters guide and constrain the Board in this context? And the answer is of course the constitution. Our constitutions kind of rise and fall in our level of focus and attention in ordinary organizational life.

There's a cycle to reviewing, we refer in particular tricky moments, but in the context, we find ourselves in the constitution is like the touch base, it's the daily guidance for WHOIS, what role is WHOIS responsibility. And the objects in the constitution, the objects set out what we are there to do are way bigger and deeper and more important to an executive implementing or executing a strategy set by a Board than any particular membership views. And what I'm discovering is that takes some courage to communicate. So, the constitution is the first thing.

The second thing is the organizational values, again which can sometimes be a poster on the wall. But when you come to such deep polarizations in your community, the values provide a place to stand and about how we go about addressing regulatory and social policy conversations.

And finally, the foundation is formed from the Board itself and its role to develop an own organizational strategy. Because members can lobby for priorities or particular focus areas and it's way easier to find constructive and balanced approach to that when the Board is very clear of their ownership of the organizational strategy and the executive are clear about their role in implementing it. So then how do we have impact on regulatory processes and policy outcomes? I would just reflect that it's a little bit about like the conversation we've been having here with the TCCM work about how you can't turn up to defend multi-stakeholderism at the last minute.

And I think responding to regulatory initiatives of the government and social policy in the broader community, it's difficult to have impact if you pop up on issues without a reputation that's backing you, without having already developed trust, without a relationship or a track record or a game plan.

So by definition, effective regulatory work is a medium- or long-term proposition. The danger of not starting there is that you're just relegated to the list of people who submit on an issue rather than being seen as a person or an organization that has a policy position and you're not just submitting a view but you're influencing the outcome.

Which moves us to playing the long game. There are a whole lot of complex and interlinking parts that add up to effective regulatory input. Relationships, trust, networks, reputation, gaining information in the right rooms, being invited to the right rooms, understand the context and landscape, being in conversations that create influence that trickle through, understanding who your allies are and forming coalitions.

All that is part of such a simple thing as a complex game of interlinking parts. But also, it requires vision. I've been really struck by how TCCM kind of created a bit of a master class in developing influence and using it effectively based on long term reputations and trust but in a new coalition for a particular purpose.

We can really see key elements of influencing regulation in national contexts in this international example. Invite close allies, clarify purpose, invite broader support, articulate positions clearly in relevant environments, build respect networks and resource, decide what opportunities for influence, information and action exist. And not, of course, forgetting execute.

So just to wrap up, I think that part of considering influence in government regulation is really going back to basics and understanding your organizational context, your current strengths and weaknesses, being confident and clear about your purpose and aligning with it and building the relationships and networks and influence with outcomes in the long term in mind. Thank you.

ANNALIESE WILLIAMS: Thank you, Vivienne. Are there any questions for Vivienne? No, not at the moment. We'll pass to our next speaker, Jordan Carter. Thanks.

JORDAN CARTER: Thanks, Annaliese. Good morning, everyone. My name is Jordan Carter (.au). Aside from serving you all as Vice Chair of the ccNSO Council, I'm here just with my day job hat on today as Internet Governance and Policy Director to talk a little bit about this topic of the session which is about shaping the regulatory environment. Now, can I grab the clicker? I'm not good with clickers, so let's see if this works. Does anyone know where I'm meant to point it?

Yeah, there you go. You're on. I don't know if that was me, but it worked. So, auDA, we're the .au ccTLD manager. There're about 4.3 million domain names in this space and our purpose as a company is to obviously operate .au effectively and to be a champion for the open, free, secure, and interoperable Internet.

And we do that under terms of endorsement from the Australian government, so we've had that role since 2000, which gives us substantive day-to-day operational autonomy to operate the domain consistent with those terms. And, of course, we also, well, not of course because not very many CCs do, but we also do have a sponsorship agreement with ICANN as well.

And in a theme that's been consistent with many of the presentations like others here, we have been covered by security of critical infrastructure legislation, in our case, since 2021. There we go. So, compared to some countries, Australia takes a fairly interventionist approach to one particular aspect of policy that may be of interest, which is reducing online harms. And there's a lot of bipartisan support for that process, which is something I'll come back to as we go. And that political bipartisan support, center-left, center-right, matches strong community support for this approach.

Generally, if you ask people in Australia if they would like the government to do something about problems like online harms, they will say, yes, please. So, the political is moving with the public in this case.

And Australia was the first country to establish an online safety regulator. That happened 11 years ago in 2015. And that legislation was significantly updated and expanded in 2021. And the Online Safety Act that we passed then is one of the world's most comprehensive online safety regimes.

And then, I don't know if any of you saw the headlines. Probably some of you did. Late last year, the age limits on social media access came into effect. That was passed in legislation at the end of 24 and had a year-long plan for implementation. So, under-16-year-olds can't access social media in Australia as of December last year. There's also a strong focus on cybersecurity. And Australia has had several major data breach incidents over the past few years that have affected cybersecurity legislation, also privacy legislation updates.

And the approach to critical infrastructure legislation has been aimed both in sector-specific ways but also in uplifting cybersecurity practice across the entire economy. And that legislation, I think, was last updated in 21 as well. And in 2023, Australia launched the Australian Cybersecurity Strategy, which, again, tries to say cybersecurity is not just a technical thing that geeks do in the background. It's something that we all need to be paying attention to across our work and turning it into a really whole-of-nation shared responsibility with a kind of collaborative approach that doesn't just government issuing regulations but tries to be a bit more community-engaged than that.

There's more coming in terms of updates to our Privacy Act, which always takes a long time. And in the Australian policy context, as I guess in many other places, the topics of what to do with and about AI and what to do about the challenges of digital sovereignty in this changing geopolitical age, I will say, are to the fore as well.

So, a slide about the approach, really. As an organization, we're pretty comfortable with the overall policy thrust of a lot of these initiatives, the intention behind them. Sometimes legislation and regulation are an important part of the mix. Fundamental to our approach, I guess, is that early involvement in these processes is critical.

Once a draft piece of legislation is out there, once the minister has made an announcement or the prime minister has given a speech, your chances of changing it are much lower than if you get in the door beforehand.

And I mentioned earlier the bipartisan nature of that approach in Australia. Public pressure for doing more centre-left, centre-right, largely on the same page, can mean that consultation can be pretty limited. Sometimes legislation on issues can be passed in days rather than weeks or months. But we try and see that coming, and I think in a similar way to what Vivien was saying towards the end of her presentation, it's about maintaining the relationships that you need.

With government officials, with parliamentarians, to sort of help shape their work, to learn from them, to understand their

perspectives. And then when something happens, you're not scrambling to try and build a relationship from a standing start. You already know the people. You might learn about things a bit earlier than you otherwise would.

We keep a broad eye on the policy environment in Australia. Of course, we also are active in the international environment, and we try and draw those insights to see what might be coming and to inform domestic decision-makers as well. That's through conversations and meetings with people.

We do written submissions. And really, we take an approach of trying to bring an insight into the reality of the internet. So, that's kind of that technical expertise that sometimes gets lost in policymaking. And to really try and understand the problem that they're trying to solve with the policy. Because I don't know if it's like this in your own jurisdictions.

Sometimes political and legislative systems are better at saying, we're going to do X than really, really understanding what problem they're trying to solve. And that can be a helpful approach to policy-shaping as well. We try and build the capacity and knowledge of the government officials we work with. And the aim is to genuinely improve the policy and the problem that's on the table.

So, we don't take an approach that says, oh, what's in our short-term commercial interests or what would just manage our costs. We do try and take a sort of public-spirited approach to what we're

trying to do. And we try to be a bit transparent as well. Our approach is set out in a bit of a light public policy agenda document that we've published and our international approach in an Internet Governance roadmap that we publish.

I think we've spoken about those two documents in the ccNSO room in the past. And we've had some successes with this overall approach. I'll talk about two of them just briefly. One is the security of critical infrastructure legislation.

The government published draft legislation when that regime came into effect. We supported the policy objectives, but we worked with the department to understand their underlying intentions and to collaborate on refining the text of the draft legislation so that it achieved their objectives but also appropriately reflected both the international nature of the DNS, that it isn't just a system you can deal with in Australia, but you have to respond to the fact it's a global distributed system, and what auDA's role within that system was as well.

And that led to a much better niche for the WDNS inside that legislation. And we've been using similar approaches in the area of the online safety space. The Online Safety Act framework I mentioned, it gets reviewed by an independent reviewer every few years to keep it up to date. And the government published the latest review last February, 2025.

It made 67 recommendations across a whole gamut of areas of online safety. One of those was to legislate a digital duty of care,

putting obligations on tech companies as yet unspecified to look after the safety of users of their services. I'm sure we'll have more to say about that at a future ccNSO meeting because it just isn't defined enough yet. But they have promised over more than a year to implement that.

But one of the key areas that we're interested in is one of the proposals is to change the industry categories in the Act because the Act was a complicated beast. It has eight different categories of industry that sort of reflect how the tech industry looked in 2015. And obviously things have moved on a bit.

They've proposed to simplify that framework and to expand its coverage to almost everything from operating systems and hardware through to online services. And there's a new category proposed called online infrastructure services, which would explicitly call out the domain name system and domain name registries and registrars as parties that were of interest.

So, improving safety and being an appropriate part of that framework is something that we are comfortable with. But we do want to make sure that any legislation here appropriately reflects the roles and responsibilities of those providing the services and the infrastructure that support it. You do not want to have, we do not want to have a situation where, in terms of content moderation and so on, the same obligation applies to us as applies to, let's choose Instagram for one of a better example.

The closer you are to the content, and especially user-generated content, the more-sharp your responsibilities should be. And the further down the stack you go, the less you should do to be what Kristian called the Internet police. None of us want to be sitting there.

We don't have the skills or the mandate to decide what is and isn't proper content. And we don't think that the government wants that to be the case, but we need to help be part of this policy debate, at least in part to make sure they don't do that by accident.

So, we've reached out to government officials working on it and provided a bit of a briefing about how the DNS works. We did that mid last year. And trying to just really call out what the roles and responsibilities are of the DNS domain registries, not in a defensive way, not because we think, oh, God, we don't care about online safety. It's nothing like that. It's just to say, don't give us a job we weren't set up to do and would be the wrong people to do.

For all the reasons that many of us are familiar with, for the reasons that Kristian talked about in terms of what the impact is of taking down a domain name, which abolishes all the services, in a sense, that you can find through that label, a new label can immediately be applied. So, it doesn't fix the problem.

And like with our engagement in critical infrastructure, the aim is to make sure that anything that's drafted with a good reality check about what the right role is for organizations like all of ours. We've shared material that's been prepared by other organizations as

part of that. Center, in particular, has some useful material, including a video that explains the ccTLD's role in relation to content. We found that helpful.

We don't have a time frame for this implementation of this legislation or the review's findings yet, but we will engage in the consultation. We'll use those deep relationships that we've got in Canberra to deal with it. And, of course, a future ccTLD news session or appropriate IGLC session will provide updates. Particularly, I think the duty of care will be an interesting one.

A number of different jurisdictions in the room have got that or are thinking about it. I think it'll be a good topic to explore.

And with that, that is the end of my presentation. Thank you for your attention.

ANNALIESE WILLIAMS: Thank you, Jordan. I do have a question in the chat, but I'll just ask if there are any questions for Jordan. Yes, down the back of the room and then in the middle of the room, and then I'll go to the one online.

ANDREAS MUSIELAK: Andreas from Nic.at for the record. Jordan, one question. So, you mentioned the social media restriction in Australia for kids below 16 or teenagers. I mean, you're the first country WHOIS doing that. In Europe, we're discussing that a lot, and I'm pretty sure that will

come soon. Are you planning in this aspect to either count or evaluate if there will be a change in usage of the websites?

And do you start an awareness campaign? Because this is an opportunity for us, by the way, because normally they live in their bubble, in the social media bubble, and now probably they have to use again the old structure of websites and others. Any plans from your side?

JORDAN CARTER Not that I know of, but that's a very interesting idea which I'm going to follow up. Getting them out of the bubble and maybe onto the public internet for a change. Yeah, hadn't considered that one.

ANDREAS MUSIELAK So, probably there is something which we as a community should follow up, because if this will be broader, that's probably something we can build a Working Group or something on that.

JORDAN CARTER The other thing I'll just add, a bit of editorial license, is that the eSafety Commissioner did publish insights that something like 4.2 million accounts had been disabled or cancelled in the first month or so afterwards, and they're doing quite a lot of research into the impact. They're determined to monitor it. It's part of their compliance role.

I put a link in the chat to the Online Safety Act review findings, but I'll also put a link to the eSafety Commissioner, which will provide some of their analysis. But thank you for that question/suggestion.

ANNALIESE WILLIAMS Yes, in the middle, please.

PAULOS NYIRENDA Thank you. Thank you. Paulos Nyirenda again from Malawi, for the record. You mentioned that .au has a sponsorship agreement with ICANN. I think this was signed some time ago. I wanted to find out if it has evolved in any way. Has it changed in any way, or is it still as it was signed a few years ago? Thank you.

JORDAN CARTER As far as I know, it has never been changed or updated since it was signed, and I think at the time it was signed, there was a bit of an expectation that this would become a regular facet of ccTLD-ICANN relationships, and it hasn't really proved to be the case, I don't think. So I don't know what proportion of CCs have such a document in place, but as far as I know, it's not very high. So, no, it hasn't been updated, and I don't think we see it as a core part of the authorizing environment for our role.

ANNALIESE WILLIAMS Jordan, I've got a question online from David McCauley of Verisign. It says, Jordan, can you say more about the digital duty of care that

was mentioned in a recent review of the Online Safety Act? Does it have force of law? Is it defined?

JORDAN CARTER

I can say very little more about it. It is currently a proposal in the independent review of the Online Safety Act, and the government has said that it will legislate it, but they haven't promulgated legislation. I think I can go so far as to say that my understanding is that it would be aimed at content that is already illegal and potentially a content that is harmful to children, but I don't understand any detail behind the definition of either of those things, and I also don't understand the nature of the obligation.

I don't think there have been any policy decisions that indicate whether it's simply a broad you have a duty or whether it's something that is you have a duty, and these are some examples of how you might do it, or whether it's that plus, like, some rules about specific obligations to report or to give effect.

So, obviously those are absolutely critical questions in trying to understand the impact of such a duty, but at the moment there is no formal proposal on the table. The government did do a brief consultation about it at the end of last year by means of a survey that was open to the public, so I guess at some point we'll see the outcomes of that survey as well. Sorry, that's a long-winded way of saying not yet.

ANNALIESE WILLIAMS Thanks, Jordan. Yes, go ahead, please.

JOHN SIHAR SIMANJUNTAK Hi, I'm John from Pandi.id Registry. So, in your presentation, I think, yeah, you're not present about the governance model, especially because I understand that your member is quite many, so it's like Pandi, PASI, also a non-profit organization. We have limited membership. I'd like to know more about the governance model on your side.

I mean, how you influence the government, because you're saying that you're trying to make some influence before a decision is made. Are you setting up, let's say, the Working Group or something like that? Can you tell me more about that? Thank you.

JORDAN CARTER So, I don't know if this will exactly answer your question, but there are a few points. We do have a domestic policy or Internet Governance roundtable that we convene with other stakeholders and government officials sometimes to talk about mainly Internet Governance topics, and the government itself has done some work in pulling together consultation groups or roundtables when policy things come.

But in terms of influencing public policy decisions of the government on these issues, our main approach generally in that being proactive sense is relationship-based. So, we work out who the people are who are working on the policy or who the minister

is. It is something that we do broadly as the staff of the organization.

We don't take the approach of mobilizing our members to advocate on these issues to the government, and we don't tend to mobilize our membership base to determine our policy positions either. They're based on that purpose commitment of the company to support a free, open, secure, and global Internet. John, does that come anywhere near responding to your question?

JOHN SIHAR SIMANJUNTAK Yeah, just more clarification. So, since your member is quite many, I found your members are more than 300 members, right? So, I mean, do you setting up, let's say, the Working Group to set up your initiation for the policy, let's say, you're saying about the NSF, let's say, are you involving your member to setting up the policy? And then the Board maybe have consultation with the government, something like that, just to make understand.

JORDAN CARTER So, if I could put policy about the domain namespace into a different bucket, this presentation has had nothing to say about that topic. So, we set out the policy for how .au works and questions like DNSSEC or WHOIS eligible for domain and the licensing rules for the .au domain. And for those, we run an occasional policy review process.

And one of those is happening right now for the .au rules. And for those processes, we don't create any special role for our members. We treat all of the public equally. So, there's no member Working Group. There was an independent panel that was appointed by our Board to consider the issues and public consultations, meetings, physical meetings, and online town halls and webinars to be able to draw input and insights from people.

And then the independent panel will make a recommendation to our Board of directors for any changes to the framework, and then they will make a decision about it.

The government side is treated as an equal stakeholder in those dialogues. So, we had a round table with them and so on. So that's how we do the domain name side, no special role for members. Our members, we have around 6,500 members now. But their main role is to vote for our Board members, and we send them an email newsletter once a month. It isn't an engaged activist membership.

JOHN SIHAR SIMANJUNTAK Thank you, Jordan.

ANNALIESE WILLIAMS Thank you. And thanks for the questions. Thanks for your presentation, Jordan. David did have another question. So, we're going to return to Devesh. And, David, my apologies for missing this in the chat earlier. But, Devesh, David's question is, can you tell

us if the Delhi High Court case has been appealed? What is the current state of the case from the point of view of finality?

DEVESH TYAGI

The court decision is yet to be decided at the ministry level. We had forwarded it to the ministry since it will be a policy decision based on the legislature. So, we had forwarded it to the ministry and it is still under consideration.

ANNALIESE WILLIAMS

Thanks, Devesh, and thanks for the question, David. Jordan, can I grab the clicker off you? Thank you. Am I driving the easier car? Yeah. Okay. So, just before we wrap up this session, so the issues that have been raised, particularly around the online safety and other regulations, are a real sort of topic of interest in the IGLC.

I think it's something that is concerning governments in many, many countries. But just to give a quick update of the IGLC's work over 2025, but just a quick reminder about the purpose of the IGF and what we do.

We monitor regulatory developments that might impact on the ccTLD and come together via online meetings about twice a month, usually. It's quite an active committee and very regionally diverse. We have members from across every ICANN region as active participants.

So, we sort of share updates with the rest of the ccTLD community via sessions like this one at ICANN meetings, as well as webinars,

roundtables, updates in ccNSO newsletter, et cetera. And we also coordinate where we're relevant with other parts of the ccNSO community and other parts of the ICANN community as well on key -- sorry, Joke, are you able to show me?

So, this is just a reminder of what we discussed last year. We had two sessions, one at ICANN83, which was on 20 years of WSIS implementation, where we sort of explored from the perspective of ccTLDs how some of the activities that they are undertaking contribute to achieving the goals that were set out at the first WSIS. And then at ICANN84, we held a session that was sort of looking beyond WSIS and looking to the future.

We were joined at that session by one of the co-facilitators of the WSIS process, as well as Vint Cerf and some leaders from the CC community as well. And that session just sort of explored the role of the technical community in multi-stakeholder governance processes and how ccTLDs in particular are contributing. So, that was last year.

We're currently working on updating our forward Work Plan, which is a multi-step process, which many of you may have participated in, whether you're a member of the committee or not. We do an annual heat mapping exercise where participants are invited to just identify the topical issues that are being discussed in Internet Governance discussions in their country or in their region. And this is an information gathering exercise. It's not limited to issues that

the ccTLD might be dealing with themselves, more what's part of the broader conversation in their areas.

And the purpose of doing this is just to track issues over time, see how they evolve or see where new issues are emerging. And many ccTLDs are very closely engaged with their local IGFs and regional IGFs, of course engaging with their governments on policy and regulatory issues as well. So, once we gather that list, we then share it with the rest of the ccNSO membership and invite them to include any issues that may not have already been identified.

And then we sort of have a look and see, pick a handful of issues that are common across all regions or all of most regions. So, issues that are going to be of high interest to the committee membership. So this year's issues, the top issues that were identified were the future of Internet Governance, online harms, sovereignty and resilience. So, they're quite broad themes, but they were common across the regions.

The future of Internet Governance was a priority issue from last year as well, but sovereignty is a new issue that we haven't seen before. So, that's an interesting observation in itself that new issues are emerging. So, then after we pick the most popular issues, we then undertake additional analysis to explore what that issue might, or how this committee exploring that issue might benefit ccTLDs or the ccNSO more broadly. Is there a need or a gap that would be met by considering that issue further?

So just this past weekend, the committee met and has done an impact versus effort analysis of these themes, just exploring which ones might sort of give us the most value to the ccTLDs through exploring. There are some issues that come up year after year. The theme of resilience is one of those, and each time it's come up in the past, we sort of note that it is a very broad theme and lots of different angles to it, and we sort of note that other parts of the ccNSO are already considering the theme of resilience, and we haven't sort of looked at it in depth for quite a while, but there has been a proposal that we could perhaps work with some of the other parts of the ccNSO who are exploring this from a more technical perspective.

The IGLC brings the regulatory and policy perspective, so this is sort of an initial proposal that hasn't fully been thought through, but we are thinking that perhaps for the ICANN86 or ICANN87 meeting that there could be a joint session.

Peter is one of the chairs of the other group. Peter, did you want to say anything on that? And you don't have to.

PETER KOCH

Yeah, never let that opportunity be missed. Thanks. This is Peter Koch, DENIC, and as Annaliesa said, the chair of the Study Group on the potential IANA's role in ccTLD disaster recovery. I'd echo what you, Annaliesa, said about the idea. We would like to present that to the community. That's one thing. Two, maybe even better explain how the landscape is covered by, how and why the

landscape is covered by three different entities in the ccNSO at the moment.

There will be, and that's either this afternoon, I believe tomorrow afternoon, we'll have a session where the Study Group status will be shared with the ccNSO community. So, maybe you'll want to listen into that as well. Other than that, I think we are looking forward to supporting contributions from the community. Thanks, Annaliesa, for the opportunity to speak.

ANNALIESE WILLIAMS

Thanks, Peter. So yeah, we are still with the secretariat working through the results of the analysis that we did this past weekend. And we'll sort of be reviewing that, revising our draft Work Plan and presenting that to the ccNSO council. But before we did that, I did want to invite members to share any thoughts or comments on the proposed themes for this year, which, again, were the future of Internet Governance, online harms, sovereignty and resilience.

Any thoughts on the value of the IGLC exploring these or any ideas for what activities that we might pursue? Would you be interested in hearing from ccTLD members? Would you be interested in hearing from external speakers on any of these themes? Any comments or thoughts? And I would invite any other members of the IGLC to contribute as well, if they would like to. Pierre, go ahead, please. I'm not sure. I'll go to Pierre and then down the back. Thanks.

PIERRE BONIS

Pierre Bonis, .fr, for the record. Thank you very much for the presentation and for the plan that is very interesting. The vision maybe of IGLC is that whatever the topic that you want to discuss, it's always linked to the discussion that occurs in other fora, discussing about Internet Governance.

And if we are sticking to this idea, I think there is no overlap with other ccNSO Working Group. And TLD Ops is really ccTLD cooperation within ccNSO. When we are talking about the IANA function and the disaster recovery, we are still very much inside ICANN. IGLC opens the windows to other places. So, if we stick to that, I think there are very important topics and they cannot overlap. They bring information from, I don't know, ITU, OECD, or other fora where us, ccTLD managers, can participate as well. Thank you.

ANNALIESE WILLIAMS

Thanks, Pierre. And that is still very much the goal. And for those who don't know, Pierre was the first chair of this committee and I think it was probably established at your initiative. Yeah, that is still very much our objective. But just in terms of the prioritization, when we go through those exercises, we've in the past sort of prioritized issues where this committee has the primary interest. And in terms of adding value to listeners, we're exploring topics or prioritized in order of the preference that we work through them.

We prioritized issues where members might not have been hearing about those from other parts of the ccNSO. But the resilience one does keep coming up year after year and it might be worth exploring how the technical and the policy issues, how they all come together. So, we'll be looking at how we can do something interesting there.

Any other? Oh, there was a question down here. Sorry, before I forget, down the back. Thanks, David.

DAVID CHRISTOPHER: Oh, yeah, it's David here from CIRA. I think as we discussed at the weekend session, I think the four of these are all kind of interlinked and overlapping. Certainly, in Canada, the topic of sovereignty in general, digital sovereignty in particular, has really grown in salience of late, given the interesting geopolitical climate we're all in. Certainly not in any sense of isolation or solitude, but again, in terms of growing resilience. And I guess I'm curious. I think it's a very interesting topic. I'm curious to hear what experiences are happening in other CCs and other national contexts around the world.

ANNALIESE WILLIAMS: Thank you, David. I would invite you to join the IGLC and come and discuss with, you know, like these are, the sovereignty one is a new issue. We haven't seen that one before, but the online harm is another one that has a lot of interest from a lot of regions. But yeah,

I would encourage anybody. The IGLC is open to ccTLDs. So, if you are not already a member and you would like to be, I'm sure Bart and Joka will be able to explain how you go about joining. But yeah, we certainly do encourage new members.

There is a lot to discuss and there's a lot to learn from. It is a really regionally diverse group and it's always very interesting to hear the same issues being discussed in different countries and different regions and how those issues that are impacting on your ccTLD are being dealt with somewhere else. So, go ahead, Pablo.

PABLO RODRIGUEZ Thank you so much, Annaliese, and greetings, all. I've been listening to a number of things here that, well, first and foremost, thank you for putting this session, for making this happen. Excellent work. Thank you to all the panelists. Excellent and extremely interesting information that is needed to many ccTLDs.

I have seen some points that I very much concur with. From the point that Jordan made with regards to cybersecurity is the responsibility of all, not only of the programmers and the people behind the scenes, because, like Pierre mentioned, there are many dimensions to many of these topics. There are many dimensions to the topic of resiliency.

So we can look at it from the TLD Ops perspective, from the IGLC perspective, from so many other perspectives, and that is important to bring it to the floor. In addition to that, the point of

sovereignty, likewise, can be looked at from many dimensions. And I strongly believe and support that this become a forum where we can bring this type of information. So, thank you for that.

ANNALIESE WILLIAMS

Thank you, Pablo. And one of the active members of the IGLC, we always welcome your contributions. Thanks.

Any other comments on the proposed themes? Noting that there will be plenty of scope for crossover between the issues. They may not all be considered in isolation. We may look at what we can do that sort of touches on multiple themes. Any other comments on those proposed themes? We will share the Work Plan with the members of the committee once we've done the analysis from this past weekend. But I'll just check online before I -- No, I've got Pablo.

So in that case, I might wrap up, and I would like to thank the rest of the members of the IGLC, and particularly the small group, David, for helping organize this session. We're sorry that you can't be with us in person. So, I'd also like to thank Marta, our vice chair of this committee, Marta Dias from .pt, who was also unable to be here.

Thank you to our fabulous ICANN support staff, and please join me in thanking all of our speakers today, Devesh, Kristian, Vivien, and Jordan. I think the meeting is closed, and I acknowledge the remarkable timekeeping of all of the speakers. Thank you.

[END OF TRANSCRIPTION]