ICANN86 Seville | PF – ccNSO: Study Group Updates and Consultations
Wednesday, June 10, 2026 – 10:00 to 11:15 CEST

CLAUDIA RUIZ

Hello and welcome to the ccNSO Study Group Updates and Consultation 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. I will also post them 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. If you would like to speak during the session, please raise your hand in Zoom.

When called upon, virtual participants will unmute their microphone. On-site participants will use a physical microphone to speak and should leave their Zoom microphones disconnected. For the benefit of other participants, please state your name for the record and speak at a reasonable pace. Thank you, and with that, I will now hand the floor over to Jodi Anderson, moderator for this session. Thank you.

JODI ANDERSON

Thank you, Claudia. Hi, I'm Jodi Anderson, .nz, and welcome everybody to the ccNSO Study Group's Updates and Consultation Session. Well done for finding the room, realizing it was a different room.

Today, we're going to hear updates from the chairs of the two study groups on the progress of these study groups and get community feedback to shape further work on the study groups. Just before we hand over to the chairs, just a little bit of context and background for where these study groups came from for anybody who's new or anybody who's not new, who can't remember or has lost track. I'm always in that category.

As everybody probably knows, the ccNSO is responsible for the global policy framework that defines how IANA relates to the ccTLDs. So this is not policy that the CCs make for themselves. This is policy as between IANA and the CCs. And during, I think it was 2024-2025, Jordan will correct me if I'm wrong, the ccNSO had a policy gap analysis working group, which essentially looked at that global policy framework and identified some possible gaps in it, in policy or in guidance or in practices. And that working group identified about six issues that needed further investigation and decided that for each issue, we'd set up a study group to explore that further and make recommendations to council and the CC community on any future work needed for those issues.

And that working group identified two issues that were going to be first cabs off the rank, as it were. And those two issues were IANA's

role in ccTLD disaster recovery, that was the first one. And the second one was IANA public records. So those were the two study groups that were set up. And in this session, we are going to hear from the chairs of each of those study groups. Jordan Carter from, where are you from again, Jordan? .uk. And Peter from .de, ably supported by Katrina from .lv and Irina from .ru. So we're going to hear from them. They're going to present findings so far in terms of the work of the study groups and also get some input from you all to help shape any future work. So please do have your phones ready. We're going to be using Mentimeter and there may hopefully be room at the end of each presentation if anybody has any questions.

Just before I hand over, there is information on the website, on the ccNSO website, if you want to find out more about either of these study groups, go have a poke around. And also each of these study groups has a work session tomorrow. I think it's the first and the second session. So before morning tea and afternoon tea. So please come along to those if you want to learn more and engage in that discussion. That's all from me. I think Jordan is up first. So I will hand over to you.

JORDAN CARTER Thank you. Thanks, Jodi. Good morning, everyone. My name is Jordan Carter. Today I'm coming to you from Nominet, the .uk ccTLD; change of hat since I was at auDA last ICANN meeting. My task today is as Chair of the IANA Public Records Study Group of the

ccNSO. And I'm going to give you an update basically on what we've found in our first discovery phase of the study group's work. So if we go to the next slide, please.

As this shows, we're following the double diamond approach to the study group's work as the study groups are doing, supported by our wonderful secretariat. And this study group that we're going first started second. It started a few months after the disaster recovery group that Peter is leading. And so that's why we're just at the discover stage, the first stage of the work today. And then by the next time we gather for ICANN87, we'll be at the deliver stage. So we've got a few stages to go of what northern people often call the summer, but the rest of us call the middle of the year. If we go to the next slide, please.

We're going to give you a brief update on the findings and give you an invitation to give us some more feedback because some of you like to talk quickly and think quickly. Others of you like to read things and think about them. So you've got both options today. This is the sort of more quick feedback option today, but you do get to use your voices and your Menti skills. So don't forget that Menti is on the way. Keep your phone handy.

And the three areas that this study group is dealing with is what these IANA public records are for. And in a moment I will explain what they are. To look into the accuracy of the data that is in the records. And then to talk a little bit about graduated compliance or enforcement options to deal with challenges of inaccuracy. I just

want to say for the record that it does feel very odd to be addressing a third of the room in front of me and not the two-thirds behind me. I feel like I'm ignoring you, but I can feel you there anyway. So sorry about that. But it's the way it's got to be, otherwise the video will not work for the remote participants.

So if we go to the next slide, when we talk about IANA public records, we're talking about the delegation records in the IANA root zone, the published ones that go on the IANA website. And they basically, I should have taken a screenshot and put it in, but I didn't. But you can go to the IANA database and you can find what's there. It names the organization that is the ccTLD manager.

And then it says who the administrative contact is and what the contact details are. It says who the technical contact is and what their contact details are. And then it gives the host names and IP addresses of the authoritative name servers for the ccTLD. And then it includes a few other items down the bottom, the registry information, the link where you can go and get domains, what the WHOIS server is, the RDAP server, and so on. And it tells you when the record was last updated.

So when we're talking about the IANA public records, we're really focusing on the ccTLD manager name, the administrative contact, and the technical contact. We're not so worried and we're not looking into things like any reports of delegations or transfers. We're not really focused on things like, is the WHOIS server label right? We're not quizzing into the accuracy of the host names or

the IP addresses. That's not what this is about. So you can look at them on iana.org. On the front page on the left, there's a link to the database of top-level domains. This would be a good opportunity for you, obviously not while I'm talking, but sometime today to go and look at your ccTLDs records. And if it isn't accurate, talk to IANA and fix it up. But next slide.

That's what they are. Sorry, I've just talked through the slide without having it in front of me. And the purposes of those records, it's the first of our topics, allow you to identify the ccTLD manager and to show its link to the country or territory that the name is part of, because that is part of the framework to know that a ccTLD manager is associated with the country or territory that the TLD is associated with. To give contacts for administrative and technical matters, the host names and IP addresses.

And previously, it was also that those two parties named as admin and technical contacts were the people who were the authorities to make changes to the record. But in the past few years, as hopefully many of you know, IANA has developed a different contact record system where other people or roles can be given the authority in the IANA CRM to make changes to the records. So that's why that last point about the purpose and authorizing contacts for changes is superseded. And there's more details about this in a paper that I'll mention that's going to be coming out later. So that's what they are. And I think the next slide is a Menti slide.

And I know that if you're at the back of the room, that's probably quite a small QR code to zoom in on. But we're just going to take a small pause now to ask you what you use the information in these records for. And the reason to ask that question is simply that we're trying to ascertain the current purposes of the records. And purpose is often at least in part informed by the use. What do you use it for?

So we would love for people to log into the Menti and to share some thoughts about this. After this meeting, we're going to publish a paper that sets this up in a bit more detail and offers you the chance to share your insights with us through an email to the Secretariat or similar. So you might not have anything to share now, but you might think of some things later. So I'm going to have to look at it on my screen.

JODI ANDERSON: And Jordan, if I could just jump in there. For those who are too far away and aren't on Zoom, the Menti code is 24130419. 24130419 if you're at the back of the room.

JORDAN CARTER: And I think you can type that in by going to menti.com if you are wanting to do it.

BART BOSWINKEL And it's in the Zoom room as well. So if you log into the Zoom room, you can see it.

JORDAN CARTER So that is the Menti. And I'm just going to read through because it also may be the case that you can't read what's up on the screen at the moment. Some of the uses that have been mentioned. People occasionally check their own data. And these are for contacts. Check TLD steward contact details. Checking on which RSP, which registry service provider is used. I guess that's often ascertained by looking at who the technical contact is for the domain. Someone probably said I don't, which is great. Find the registry admin and technical contacts. Check the name server records for TLDs.

People check the data of other TLDs. Check details are correct. Evidence for auditors. That is a fascinating one. I guess whoever wrote that feels like speaking up, they can. But I suppose that's about being able to prove that you are in fact the organization that is entitled to claim that they run that TLD. Find the manager. To register a domain name. That's an interesting one. Check membership requirements for a regional organization during the application. Is it in the database? Check TLD information. Search for TLD operators.

Yeah. So that's a set of things. None of which are novel, I don't think. But it's good to validate this and see where the weight of opinion is. So thank you for those 23 responses so far. This is super helpful. And I don't know if Kim is behind me or in front of me. In

fact, he's in front of me. This is good. But Kim is saying in the chat, this is super helpful. It's sort of proving the community's interest in and use of these records. So that is good.

I think we might move on to the next question. The next subtopic. Remember, these are not your only chance to have a say about this. So those are the records and what we use them for. And there is a point that they need to be accurate. Accuracy matters because the records need to work. There's no point in having a phone number listed that has two digits wrong. Or an email address with a spelling mistake. Because it will not work.

So the inaccuracies that might happen have come in several forms. There could be mistakes in the contact details. There could be a changed operator for the TLD that hasn't been recorded. So the IANA database says one thing, but reality says something else. Out of date with consent is a bit of code that means that whilst all the stakeholders are significantly interested parties know that what is in the IANA record is not right, they're okay with that for whatever reason in the country.

And there is some evidence that IANA has shared with us of a lower than desired accuracy. Obviously those of us who are nerds on this would like it to be fully accurate all the time. It probably isn't. And IANA does share some evidence for us that there is a bit of a lag in some elements of inaccuracy. I'm not going to go into the details today.

But our next slide is going to ask you through Menti number two, if we roll over, do you have insights about how accurate the IANA public records are? So hopefully some of you by now will have looked at yours. But you may have insights about anything, about your record, about other records, about the degree of accuracy or not.

Can you share any thoughts you may have with us? If you wish to say something controversial about another ccTLD, perhaps don't do that directly by naming it in the thing. But if you want to let Kim or one of us know afterwards, that would be fine. And I'll just sort of gently read them out to context share as we go. Good enough for our purposes.

No, lots of people have no insight about this, which is fair because it's probably not a question that you have thought about before. It can be a pain to get records updated. Someone's own record is accurate. Some people just don't check, right? The information I often check is accurate. If you do find it painful to get them updated, I would suggest having a chat with Kim after the session in the break. Because it may be that it's painful for expected and appropriate reasons. Or maybe that's painful for unexpected or unknown reasons. And if it's the second of those, that'd be extremely good for the IANA team to know about.

Someone has said it's almost accurate, especially for gTLDs. Some ccTLDs seem not. And it's possible that that relates in part to the different authorizing environments for those records. While they're

all in the one database, obviously gTLDs have a contract with ICANN. Obviously ICANN has a different set of rights and responsibilities, as do Registries, compared with the ccTLD-ICANN relationship. Someone says it should be accurate on the purpose of the IANA record. Someone very patriotically says, in IANA, I trust. Good stuff, Kim and team. Yeah, Bart.

BART BOSWINKEL Very interesting one. Maybe you can ask the person who did it, on the LAC region. We are aware that some ccTLDs in the LAC region have changed [CROSSTALK]. And why they don't.

JORDAN CARTER And this information hasn't been updated. If the person who put that in the room is happy to chat to it, you could come up to the table. Just if you can say any more about it in a way that doesn't sort of identify anyone, come and sit beside Alan and grab the mic. Thank you. Good morning.

UNKNOWN SPEAKER Thank you, Jordan. And this is a topic we have been following in LACTLDs, so this is important to us. We are aware that in some cases, ccTLDs that are within government entities, governmental entities, have changes. And they go from one agency in the government to another one. And they are not really aware of the process to update their IANA records.

Then we have internal processes in our regional organizations, such as general assemblies, and we need to have a sort of validation of the new administrative and technical contacts. And we know there is a delay in that process. So, we are aware that we have the official documentation that there is a new agency in charge of the ccTLD, but this information is not reflecting in the IANA public records. So, I think that's an issue for us, at least in our regional organization.

JORDAN CARTER Well, it isn't just an issue for you, though it's good that you've raised it, but it's also an issue for IANA, because we want the records to be as accurate as possible. So, Kim, do you have any sort of thoughts in response to that situation?

KIM DAVIES Yeah, I think it speaks to an issue that I don't think is unique to your region. I think that there is a lack of familiarity with IANA's processes more broadly. I think from our side, from our position, we're not aware that these issues are necessarily happening. But it's not that they've applied for a change with IANA and IANA has rejected it. It's that it's never been submitted in the first place. And we don't necessarily have either the capacity or the mandate to proactively monitor every country's developments and reach out and remind them you've changed your security manager, you need

to like communicate that to us and go through a process of recognition associated with that.

But it's something that we strive to improve and that's sort of the nature of the work we're talking about here today. But certainly, if you or others have advice on what measures we can take that would have the biggest bang for buck, if you will, to raise awareness, we're always looking for those opportunities, whether it's, for example, in the GAC, ICANN level or other areas where we can make an impression on those that are not familiar with this so that they can get the advice that they need. That would be very helpful input.

UNKNOWN SPEAKER Thank you, Kim. And we do, we reach out to them and we tell them and we introduce them to LACTLD because these are new representatives for us as well. And we let them know that there is this IANA database and they should update this information. And we try to sort of raise awareness on that, but we are not able to do that for them, of course.

JORDAN CARTER Thank you. That's interesting and helpful to tease out. So I appreciate that input. Maybe we need a sort of easy fact sheet or something for governments doing a restructure that own a TLD or something similar. But let's carry that conversation on afterwards. Thank you.

If we look at a few more of the answers that have come up, there's other sort of helpful feedback there. CCs possibly forget to do it when contacts change. Difficult to get postal related updates to the ccTLD manager. There's an expectation the records are accurate. The process can be difficult if some ccTLDs and large entities, I guess that might relate to if you need a board resolution and you're a tiny slice of a tiny department, or if you're in a big university and you have to get something all the way to the vice chancellor's desk or something, that could be a bit of a nightmare.

And then someone else says, I wonder whether some ccTLDs may not be fully aware of the IANA database. I feel like it's likely that someone in the ccTLD is aware of the IANA database. It seems like a likely thing, but it may be that the people who are are not the same people who are the people who are in executive roles or similar. So that is an interesting point as well. The levels of awareness might be different.

So again, that's a super helpful set of data points for the study group in working through the work. If you do think of any other insights on this question, do let us know as we go. And let's go to the next slide, which is to deal with the matter of what happens if they are not accurate. And this is an area the study group has barely begun to consider yet. So it's super light at this point.

In terms of how you might enforce or drive compliance with the accuracy, there are no practical steps at the moment. There's nothing in the global policy that the ccNSO sets to guide IANA and

how it deals with ccTLDs that has sort of you must keep your records accurate. If you don't, this set of things will or may happen to you. So there are no consequences.

Informal approaches by IANA are made when an accuracy is identified. Kim's team don't just turn a blind eye if something is obviously wrong. But there's nothing in the policy to do anything else. There's no list posted that says these 10 ccTLDs are wanted because their info isn't up to date. Some of you will have been part of the ccNSO's finance review working that Alejandro chaired the review of last year, where there is a long spreadsheet that shows financial contributions. There's none of that kind of publication that's going on, other than obviously the fact that the RootZone database does have these records in public. But there's no scrutiny process of it, or any other way to do it.

So the next slide is going to ask you, I think, let's see what it says. It could say a couple of things. Are you aware of any inaccuracies that have been fixed through IANA? Or are the parties doing anything? If so, what was done? And really, we pose these questions just to get you thinking about these matters. But the thing that the study group is going to do, as part of landing its report to bring to you at the next meeting, is it might decide that it thinks that nothing should happen, that there shouldn't be any change to that lack of any compliance thing. Or it may come up with some ideas. So that's something to keep an eye on next time.

And because it's a study group, just to remind everyone, this is not a policy development process. If there was anything that came out of the study group that did require changes to policy, that would then require a ccPDP process, a ccNSO policy development process to implement it. The most the study group can do is make recommendations and perhaps suggest operational guidance for IANA. And people are not aware of any inaccuracies that have been fixed.

And they're not aware of any proactive effort on the part of IANA. That is because there isn't any. So it's good that you're not aware of it. It doesn't exist. Updating postal addresses after office moves seems to have happened swiftly. And people have followed the IANA update process when there was a change of contact info. So if you do know something that's happened to generate an update to something that was wrong, drop us a line. Someone has mentioned the case that created all of this work in the first place, the .lb case, which was solved through community IANA efforts. And it was that situation of .lb that led to the policy gaps analysis working group, which this is one of the study groups arising. So good to see that one mentioned.

Someone has said other parties can modify data out of IANA awareness. And if whoever wrote that can just maybe come and talk about it or something, that would be interesting because I'm pretty confident that no other party can modify the data in the IANA database other than IANA. But this might mean something slightly different. It might mean that the facts on the ground have changed,

which IANA isn't aware of. Someone suggests regular awareness training or raising might be helpful. And you'll update your records campaign from the ccNSO or IANA and or through the GAC. That's an interesting suggestion.

Kim, I think you have done over the years a few updatey type things. I believe there might have been Christmas cards at one point. Do you want to just fill in the room on the things you've done in the past about this?

KIM DAVIES

Yeah. So one thing that we've done over many years is we tend to both communicate to security managers by email at least once a year, often multiple times a year. And then historically, although we haven't done it the last couple of years, we would send Christmas cards to every TLD manager. And part of the reason we did both those things was to get the bounces, if you will. So for emails that bounce, we create tickets in our system for our staff to follow up and identify, try and make contact with the TLD manager and notify them that the email address doesn't work and see if it can be fixed.

Similarly, when we get returned mail to our office saying this is not deliverable with those Christmas cards, we would then also reach out to that manager and notify them we couldn't deliver this and see if their records are still up to date. Sometimes the mail service is unreliable, particularly when you literally post something to

every country in the world. But that aside, usually we catch some things we can remedy.

But with all that said, I think there's certainly more we can do. And the idea of us doing this sort of annual update, we were thinking even quarterly, something somewhat automated, where every TLD gets notified, here is your current records in an email. And perhaps a very easy, like, click this link, and it'll take you right into our portal that lets you immediately start a change request to make the updates. I think it's something we've considered in the past and might be an outcome of this work as well.

JORDAN CARTER Cool. Thank you for that context sharing, Kim. When was the last postcard round sent?

KIM DAVIES I'm going to say like two, maybe three years ago. But maybe I've fallen off everyone's Christmas card list. But we tend to not get them ourselves either. I feel that as a society, we've moved on from Christmas cards the last few years. But it's not something we've abandoned. It's just time pressures and things. We have to plan this months in advance. If we're to do it this year, we should probably start planning now.

JORDAN CARTER Well, you've got six months. We'll look forward to the cards arriving. Thanks, Kim. A few more things have come in on the Menti

while we've been chatting. And we've talked about the annual awareness campaign. The messages about IANA about opening times in December is a nice nudge to check contact data. So that's a nice piece of feedback there. And the card works. Contacts were updated following a Happy New Year card sent to the former contacts who left. And the manager updated the records after receiving this card.

So there's some evidence there that these efforts have made a difference. And someone noting that the creation data, the ccTLD, was wrong and was corrected. So there is some evidence there that's really helpful for the study group. So thank you for sharing those. If we can go to the next slide.

As I mentioned, we're going to publish a short paper, nothing too fancy, that sort of sets out in a bit more detail what I've talked through today. We will do that. I don't know exactly when we'll do that. It'll probably not be this week. And the exact format, not clear. But we'll send out a notice on the list when it's done. It'll go on the website. And we'll ask for feedback roughly around the middle of next month.

So you'll have a few weeks after this. This might be something you can do on your trip home if you're interested in this topic. And we'll send another nudge at the end of June, just to remind you if it's something that isn't top of your list after this meeting. But our next steps will be to consider the discussion that we've had here today and the Menti feedback. We'll move through the remaining stages

of the design process. And we'll complete the report to share at ICANN87.

Depending on where the group's head is at in terms of what we recommend, I don't know if it'll be a draft report that we're talking through with you at 87, or if it'll be that we've published a draft report earlier and we're sort of polishing it up at that meeting. But either way, come hell or high water, which is probably not quite an IANA-friendly expression, we will be finished by the end of 2026.

So those are the next steps. That's the report for today. Thank you for your attention and input. And I think that's my last slide. Let's find out. It is. So let's go back one slide. And Jodi, over to you if you want to take any questions or anything.

JODI ANDERSON Thank you, Jordan. Does anyone have any questions either in the room, at the table, online? If you're in the room and you have a question, please come up to the microphone. Yes, Bart.

BART BOSWINKEL Yes, we have a lot of people in the room. If you are interested, please contact to participate in the work of this group. Contact the secretariat. So there is still a room. The group meets approximately once every two weeks. And we have a rotating schedule still. So if you're interested, please contact us so we can get you in. Thanks.

JODI ANDERSON Thanks, Bart. I don't see any questions in the room or online. Am I missing anything online that you can see? Okay, thank you very much.

JORDAN CARTER Thank you. And thank you for the attention.

JODI ANDERSON Now we will hand over to Peter and team to tell us about the second study group, which is actually the first study group, which is the ccTLD Disaster Recovery Study Group. Thanks, Peter.

PETER KOCH Yeah, thank you, Jodie, for the second slot to present the first study group. Actually, not really the first, but the first coming out of the Policy Gap Analysis Working Group. Anyway, that said, good morning, everyone. My name is Peter Koch. I'm with DENIC, the top level domain registry, ccTLD registry for Germany. And I'm also the Chair of this study group. And the name is the Study Group on IANA Role in Disaster Recovery, ccTLD disaster recovery in particular.

So we present a bit of our work. We'll also have Menti. You can fill it in already or wait until the QR code appears. So similar to Jordan's group or the public record study group, we're using this double diamond scheme that we've presented before. Since we

had a head start, we are a bit further progressed in this development phase, so the first half of the second diamond. And we are going to present our work so far to you today and we'll ask you for feedback through Menti.

So that's the development phase and we build and have built options that we call scenarios and we're going to test them or have tested them and we'll present our intermediate findings. And this is a great point in time to give your feedback, understanding that that will be a bit on the spot, but probably as we've seen in the previous presentation or the previous walkthrough, the immediate reactions and the intuitive reactions are great. So we do that as well. Next slide, please.

And here we are. So let's get started with Menti. The usual question first. I hope people in the back of the room can use the QR code. Okay. Oh, it's the same code anyway, so just continue. Sorry about that. Yeah, the usual question. Are you affiliated with the ccTLD? The warm-up question. Wait a moment. Wait for a few more people. If you don't know whether or not you're affiliated with the ccTLD, there is no third option today, but you may still remain in the room. Okay. Yeah, thank you.

So keep that Menti session open for later. So what are we doing? This is the test building part of the methodology that we apply. So we're testing scenarios and why are we doing that? So currently, and this is why that study group was formed, currently there is no formal role for IANA in that disaster recovery. And very important,

the disaster recovery or any precautions and preparation is the responsibility of the ccTLD manager. So that's, we're talking about potential roles and starting from non-existent, which doesn't mean that IANA wouldn't have helped at some point in the past, but this, if you remember, actually inspired that potential gap in the study group.

And what we try to do is that we test based on some assumptions and preconditions and some structure and not just do wild guesses. So we try to model some scenarios, six that will be. That's not all potential scenarios that one can come up with, but we think we have covered the landscape quite well to address combinations that may or may not be realistic and have been seen in the past or might occur in the future. And that includes anything from failure of the hardware of the systems, natural disasters, and given geopolitics, of course, also armed conflict in different flavors.

And then any one of these scenarios that we are going to present will ask a particular concrete question. So we're not presenting the scenario and then ask, okay, so what should IANA do in this case? It's the other way around. So what could IANA do, but also what preparation would be. So it's not to hand the scenario to IANA for solution, but to think about it right now and in advance to prepare and then potentially, and remember that study groups don't set policies. Study groups make suggestions and recommendations to the community.

So talking about preparations and potential ways for IANA to help and these potential ways that enabling may or may not have to be supported by policy that would then be set up after this. But we're not there yet. That's for something else after this study group. And there's also the opportunity to shift some of the questions to one of the further study groups that are scheduled already, and you will probably see that.

So we looked at the landscape and there was a lot of desk research going on thinking about what makes us different and what things are equal and what might be different. And if you look at the box on the right, and we've seen that in yesterday's presentations, all these regulatory frameworks being more and more present in various regions of the planet.

So type of regulatory framework reaches from very strict, and the example is NIS2 or completely absent. And we found lots of those. We all know that there are very different governance models reaching from strictly regulated by the government to private sector and maybe no regulation at all and various things in between. The type of service, and it's not only the DNS service that can also be the registration service, everything in-house or parts or all of it outsourced to some other entity. So that's cases three and four.

And then finally, that's often the most obvious one, that we all differ in size or bands, say, and we characterize it as either micro or very large, lower than 5k or 5 million or more. And the idea was to shape

that risk and also might result in different types of help or support that may or may not be asked from IANA. So next slide, please.

Okay, so that's another training session. Please select the region for your ccTLD. And this is just a preparation for a fine-grained display of the responses to the subsequent polls. And I believe we had short of 40 responses the first time. Okay, thank you for that.

And now that we've gone through the… I've given you a sketch of these five different factors or dimensions, here's your first chance to give an reaction or an opinion. Are these five dimensions the right basis for the, and here it says use cases, we later change it to scenarios, and I'm using this interchangeably. So do you think that these five dimensions that we came up with are the right basis for further work? Or do you think we should rethink them? Or do you think we missed a bit or we split too much? And of course, if you're not sure.

And I understand that they're not sure yet, maybe due to the fact that this was a very, very short sketch of what we did. There will be more information in the report, of course. But if any one of those people in the yellow column would like to share what the one missing is, and maybe it's even too missing, you're welcome to join us here at the table microphone. If you want to add, or if you want to suggest what is missing, if you don't want to come to the table, we'd still be interested in learning that. Or you can put it in the chat if you're in the Zoom session. Nobody's coming to the mic, and I don't see anything in the chat, is there?

Okay, so we're not putting you on the spot. But please, if you think, and you've expressed that, that something is missing, we should add a dimension or maybe remove one. Please come talk to us after the session, or contact the Secretariat to share that information. Good. Thanks for participating in that poll.

Now, this is the six scenarios, and then potential six different roles for IANA. Again, we've come from the same set of dimensions, but we had different results. And we also found that the role of IANA, the potential role, might grow as the operator's own ability shrinks as a result of the disaster.

And to avoid that, I'm going to talk you through all of those, and also to support your memory, so that you can memorize or attach certain scenarios to certain voices. We'll do it with three people. Katrina is going to start with the first, and then later with the fourth scenario. Irina is going to present or talk about the second and the fifth, and I'll take this third and the sixth scenario. And we'll have our cheat sheets. And here we are. Do we need this for? Okay. Katrina, would you like to start?

KATRINA SATAKI Yes, thank you very much, Peter. And as an ordinary group member, I will face the community. Thank you. So, in the first disaster scenario, we looked at a ccTLD that is run by a private company. They have more than five million domain names under management. According to our radiation, they are considered a very large ccTLD. They operate under a very strict regulatory

framework. They have to follow NIS2. They have developed, fully developed, and also maintain in-house their DNS service and registration service. They're very well prepared. They have very thoroughly documented business continuity and disaster recovery plans. They have three data centers, geographically very dispersed.

So, what happens in this disaster scenario is that the country undergoes a very heavy artillery or drone bombing, and two of those three data centers are destroyed. Well, basically, they're not there anymore. And also, power has been cut and cannot be restored for more than 10 days. In our scenario, it's 11 days. Internet exchange points partially fail. And we also have issue with our staff in this scenario. So, they are either unavailable or maybe presumed they might be killed in those bombings.

So, what happens here? Since the registry is very well prepared, the third data center takes over within the allocated time, within two hours, so everything is running. DNS sex signing continues, and registration provisioning, yes, it degrades to read-only mode, but it's still there.

So, what we see here is that there is no need for IANA to intervene, at least at this point. Perhaps, at some point in the future, if it turns out that the entity, due to those heavy losses, is not able to continue operations, we might need to do some transfer requests, maybe at some point. But now, everything works, and apparently,

the registry has been very well prepared. So, in this scenario, we do not see any need for IANA to immediately step in here. Irina?

IRINA DANELIA

Yeah, thank you, and good morning, everyone. So, the second scenario considers a registry quite opposite to the one from the first. So, it's a small island with the registry run by governmental organization, some governmental agency. DNS and registration services are fully outsourced. There is not any formal regulatory framework there, and it's a micro-scale registry having 5,000 or maybe even less domain names under management.

So, this scenario, the hypothetical scenario suggests that a category 5 cyclone makes a direct landfall. So, the governmental ministry building is destroyed. Both staff members authorized as admin and technical contact are unreachable for days or even weeks, and the DNS outsourcing provider is also affected. A submarine cable is severed, and the ccTLD ceases to function as a registry. So, the outside DNS provider cannot receive authoritative instructions. There is no succession plan, no data escrow arrangements in place. So, the registry is going dark, and the country's government email, health systems, and emergency services that rely on the local ccTLD also go dark.

So, this is probably the scenario where the IANA involvement is really very needed, and probably this potential scenario requires a formal IANA emergency procedure to be developed and placed. Also, we noted that if any pre-arranged agreements or protocol

were in place for this scenario, it would make the situation much easier and outcomes not that strong and severe. So, with the third scenario, I'll give it to Peter.

PETER KOCH

Yes, thank you, Irina. And I should probably have mentioned that, of course, all these examples are fictitious and are not meant to mimic any precedent or anything. We've just tried to map the landscape here. So, if you recognize yourself, that is purely coincidental, or yourself or a neighboring TLD.

So, the third scenario is similar, in a way, to the second. We assume a ccTLD run by an academic institution, a university, and then there is a hurricane and the loss of key staff. So, the mapping on these five-dimension regulatory framework is emerging. So, there is something, and we have assumed the CARICOM guidance, which is an existing regulation, but probably lacks some enforcement measures and auditing without judging on that particular scenario.

The government's model is that it's a university, academic environment, and it's run by the university without any further, say, guidance or interference by other parties. The service is mixed in the way that the university runs the primary name service, but the secondary is outsourced or done by other parties. And the registration service itself is completely outsourced to a regional provider in a neighboring island. And it's a small ccTLD between 5,000 and 5,000. So, that's a categorization that we assumed for

this. So, between 5,000 and 5,000, university, and partly outsourced.

So, the disaster scenario, then, is a major hurricane floods the university campus. The server room on the ground floor is destroyed by the water, and there is only one person, a faculty member, that works as a DNS administrator, and that person is injured and hospitalized and cannot act. The vice chancellor, who is then formally in charge, has no technical knowledge of the ccTLD, and the outsourced registration provider on that neighboring island is also affected by the hurricane. So, the registration service is affected and is not operational.

The assumption what's going to happen in the scenario that we played is the DNS resolution will fail within 48 hours because the primary server is no longer available. So, the secondaries won't get any zone updates and probably don't keep the zone alive because of lacking pre-arrangements.

And then, the ccTLD goes offline, or actually, the service would respond to fail. The outsourced name service, well, outsourced secondary name service would principally be functional, so they are not affected, but they lack the updates and they lack the assurance that the zone is up to date. Registration provisioning stops because the registration provider is affected, and the university has no succession plan. And that regulatory framework, in that case, provides guidance, but it does not provide binding

obligations. And also, given that it's a university, the regulatory framework also does not provide emergency funding.

Observations on this, obviously, the risk here is that now that the person in action, acting person, is no longer available. The superiors don't have any knowledge, so there is no clear, or there is ambiguity about who can authorize changes, maybe to the root zone entries, in the absence of the named contacts. So, IANA would need a clear policy on what would support a sufficient authority in such an emergency, and in this particular case, a pre-existing arrangement with three parties involving IANA, the university, and some, maybe more regional backup provider, could have resolved the situation before that natural disaster happened. So, that's the part of the preparation. And with that, I'll hand the mic back to Katrina for scenario number four.

KATRINA SATAKI

Yes, thank you, Peter. So, scenario number four, here we have a government ministry running a ccTLD. It's a medium-sized ccTLD between 100,000 to 500,000 domain names under management. In this case, that country also has, to some degree, regulation that requires them to follow this national cybersecurity framework, which, again, is developed for any entity. It does not consider specifically needs of CCs. And our ministry follows it very diligently and ensures that, for example, their backup generator can run up to 72 hours, which apparently was required according to that cybersecurity framework. Their DNS service, they host it in-house

at the ministry's own data center, but registration service is partly in-house and partly run by a contracted provider.

So, what happens in this scenario? Here we see some nationwide infrastructure crisis where we lose power that lasts for six weeks. As you remember, ministry's own generator has enough fuel to run it for 72 hours. And in such a scenario, it's difficult to get additional fuel. So, yeah, basically, we are out of business here. Our cloud migration program is incomplete. It was in the development, but it hasn't been fully implemented. Staff technically can work remotely, but they cannot access any on-premise systems because of this power outage. Unfortunately, the contracted registration platform provider also is in the same area, and their collocation facility also loses power.

In this scenario, DNS resolution continues for approximately 48 hours on their cached TTLSs and then slowly degrades or maybe even quickly degrades. Registration provisioning halts entirely, and the ministry's disaster recovery plans were developed keeping in mind that, well, maybe they lose power for 24 hours. In this case, the power outage is much, much longer, and those plans are useless, basically useless in this case.

Here we also did not see any IANA's involvement that would help. Advisory role, yes, but not at the moment when disaster hits. This is something that should have been done perhaps before the event. The particular ccTLD, yes, they diligently follow their cybersecurity framework of the country, but obviously, it is not enough. Is there

a role to help people realize that there's something more that needs to be done in preparation for a disaster? This is something that is considered in this scenario. Irina?

IRINA DANELIA

Thank you. We probably need to speed up a little bit, so I'm going to be brief. The fifth scenario describes the mid-size private registry with moderate regulatory framework, having made between 500 and 2 million domain names and doing a service and registration data in-house. And this scenario describes the political crisis where the government changes and the new administration issues a decree nationalizing the ccTLD, appointing a new registry operator, but the existing operator, non-profit, refuses to comply.

So the services themselves work. However, registrars are not certain to whom they deal that, and there is a contested situation, and both parties contact IANA claiming to be legitimate operator. So this situation expects IANA to keep a gatekeeper role and maintain their status quo. And it is not technical role here, but more judicial administrative, and the study group actually is not sure whether this scenario falls within its scope, or probably it should be the subject of another study group. So next, back to Peter.

PETER KOCH

Yeah, thanks Irina, and also thanks for accelerating because of time. So final scenario, large government registry, active war, and

the operator is incapacitated. Regulatory framework is strong on a national level because it's run by government, so the government's model again is government name service and registration service run by the ministry in-house, and the domain is large, that means in this 1 to 5 million domain names.

The scenario is there's an active military conflict that results in the destruction of the primary state data center, and that affects the registration of course, and also the primary name service. The secondary site exists, but it is an occupied territory. The ccTLD leadership that can author or could authorize any changes is no longer in office, or has fled the country, or is not available in any other way, and then a government in exile claims authority. DNS resolution will start failing due to the technical failure, and a third party, a foreign operator, offers to serve the zone temporarily.

And then also to make it more complicated, the technical credentials to change root zone entries are held by staff, and are in that occupied territory, and are at risk of compromise. Now the DNS resolution completely fails, affecting millions of domains, 1 to 5 was the size, so that means all commercial, governmental, medical, and civilian services are at risk, or are about to fail because of lack of domain service, and the government in exile is internationally recognized, but has no technical capacity.

So the observation is, and you've probably observed that as well here in the room, this is the most complex scenario, and it's the one with the highest stakes. IANA acting here is unprecedented, and

would also carry geopolitical risks, because it would mean recognizing or not that exile, or that previous government. So as a study group, we could potentially explicitly address that situation, but we were also wondering, or asking for advice, whether it is better to defer that particular scenario, or some criteria that we distill out of this, to defer that to one of the other study groups that are scheduled, since this is more about recognition and authority than it is about disaster relief.

And that's it for the scenarios. Thanks, Katrina and Irina, for jumping in. Should we have one minute for questions?

JODI ANDERSON: We've got about eight minutes until the end of the session.

PETER KOCH: Okay, then let's continue. I love you, too. Okay, so then let's look at this, and there will be a Menti opportunity later anyway. So what you've probably noticed is that the preparation is key, and in these scenarios that were presented, the result and the extent of the outages depends much more on the preparation than on the type or the severity of the disaster. That's a finding, and I'll refer to the first and the second scenario here.

The second one, also a quick win, is that obviously these pre-arrangements, and that resonates with the first finding, the pre-arrangements are the cheapest and the best fix. Backup deals with other ccTLDs, backup operators, backup data centers far enough

away from an incident will help and also will not have to involve IANA intervention or support. And obviously the questions about authority are much, much harder than anything that has to do with the technology.

And if you remember the two last, the two final scenarios, you'll see that the real challenge is recognizing a new operator or new government or dealing with the fact that the authorized sources, the ccTLD manager is unable to work. And we do have transfer and revocation policies, but they are not designed for emergency. The work there is in detail and can take a lot of time, but this is not fit for these purposes. So that might be worth addressing in future policy work. And finally, the size is not so relevant for the risk and it might actually be misleading. The 5,000 domain registry can be more important to the environment than the 5 million registry. And obviously anything purely on size would be misdirected. Next slide, please.

And again, that's our preliminary findings and we'd like to have your input on this. There will be two slides on these. So first, we would like to ask you to rate these statements, statement by statement, that were these four findings. And we'd like to know if you disagree or agree or are neutral about any one of these four. And then we'll take it from there. And yeah, let the party start. Here we are.

Interesting about the preparation. That seems to be a quick win. Pre-arrangements. Give it another 30 seconds because it's four

sliders to move on this slide. Okay, 35. Okay. Thank you so much. Let's keep that slide for a second.

Quick interpretation is, yeah, the preparation point, pre-arrangements. Interesting that the authority versus technology question is the one that has a distribution where some people strongly disagree. That would be interesting to know after the fact. So please put things in the chat or contact the study group afterwards. It'd really be interesting what your views are. And then yes, the size misleading to guide the risk is. And also on the pre-arrangement part, some people seem to deviate, but that's in a different shape than the. So on the second and third, we'd be really interested to get your say written input can be a short sentence. I mean, it come back to you. Thank you so much.

And the next slide will also deal with these four. And we'd like you to -- and that's a different dimension to these. We'd like to rank these from the least to the most compelling. And that's also a consistency check, of course, in a way, assuming that the same set of people votes, and these are the five options. And you do have the options that none of the findings stand out to you. And you give it another 30 seconds or so, maybe reach 30 again, one more minute. Okay, and that's okay. I think the picture is clear and also consistent with the previous one. Thank you so much. And let's have the next slide.

Okay. So that all said, what guides the work is also the question, what do we want to achieve? Or when can we declare mitigation of

the disaster? And we phrased it as, do you or did you return to normal? And normal means both the DNS and the registration is working again. We all, obviously the DNS is especially critical, but then the domain, the registrants might be affected by the crisis themselves. So they have lots of them will have the need to make changes to their own delegations, which is why both are very important.

And after the recovery, which is based on the pre-arrangements, you're either back to normal in terms of both work again, because your disaster recovery and business continuity did its job, or you aren't. And then the question is, is there a chance to resolve the issue? But it just takes more time.

And in that case, a predefined protocol would help, or we might be in a situation where the whole disaster recovery fails, say because the organization is completely gone or that territory that we're talking doesn't exist anymore. And that's probably a failure, what we call the failure of the failure mechanism. There's no succession, like nobody else to take over. And that's maybe a gap that we can't predict and then an IANA role might be needed. That's going to be the next steps for the study group. Next slide, please.

And I guess we're almost done, yeah. Okay, we'll skip that because it kind of repeats what we just said. Next slide, please. Well, the bottom line was -- let me go back. Sorry, Bart. Please go back one slide. Yes, so the blue box underneath. So the finding is that what you do before the event decides whether you return to normal after

the event, which is again, another way to phrase that the preparation is key and determines the fate of what's going to happen. And you have it in you as CC, or we as ccTLDs operators are responsible and it's in our hands to do the preparation. And there's still the risk that the preparation and the recovery might fail, but that's a different risk that needs a different set of solutions or mitigations.

Anything more, Bart? Yeah. So it was Svetlana's presentation in the new session, right? That's another real world example there. Okay. The next slide, please. And I guess we're done. Next. Yeah, okay.

This is already the potential framework, which derives from the previous slides, more or less. The point is that there is no one size fits all. The study group concluded that if at all, there would have to be a tiered set of framework, a tiered framework to address the various risks and also the various scenarios based on these, the findings of the previous ones. So it's either only a standby, it could be an advisory role, or at the highest level, some of the scenarios would benefit from an active role for IANA, which is, which might be an emergency delegation or some backup to credentials or decisions about who can be an intermediate authority for a ccTLD and definitely needs a new policy. Next slide. And I think that's the final one.

And finally, do you support that direction of travel? Your final chance to say, go ahead. Okay. And I'm signaled that we need to

stop now, which is great because there's a hundred percent support. Thank you. Thank you so much. Thank you for participating in the Menti. And we are very open and interested in your feedback based on what you ranked and rated during the session. Thanks, Katrina, thanks my neighbor, Jordan. And thank you, Jodi, back to you.

JODI ANDERSON

Thank you very much. Thanks, team. If you've got any questions for the study group, please come and talk to us now. And I think there's usually a rating on the QR code for rating. Please do that if that pops up. Thank you to the teams for the updates and to the members of the study groups for their hard work over the last period. And with that, let's adjourn. Thank you.

[END OF TRANSCRIPTION]