ICANN77 | PF – GNSO: BC Membership Meeting
Tuesday, June 13 2023 – 10:45 to 12:15 DCA

BRENDA BREWER: Hello, and welcome to Business Constituency Membership Session at ICANN 77 on 13 June, 2023. My name is Brenda Brewer, and I am the remote participation manager for this session. Please note, this session is being recorded and is governed by the ICANN expected standards of behavior.

During this session, questions or comments submitted in chat will only be read aloud if put in the proper form, as noted in the chat. I will read questions and comments aloud during the time set by the chair of this session. If you would like to ask a question or make a comment verbally, please raise your hand in Zoom. When called upon, kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly at a reasonable pace. Mute your microphone when you are done speaking. To view the real-time transcription, click on the closed caption button on the toolbar. To ensure transparency of participation in ICANN's multi-stakeholder model, we ask that you sign in using your full name, for example, a first name and last name or surname. You may be removed from this session if you do not sign in using your full name. And with that, I will hand the floor over to BC Chair Mason Cole.

MASON COLE: Thank you, Brenda. Good morning, everyone. Mason Cole here, chair of the BC. It's a pleasure to see everybody here in Washington, DC, and to

be together again. Welcome to the BC meeting. We have a pretty full agenda on the screen, as you can see. I want to remind you, as Brenda just did, please log into the Zoom meeting room so that we can manage the queue appropriately. I'll take cues from Zoom just for the sake of expediency.

So Brenda has put the agenda up on the screen. Thank you very much, Brenda. Are there any additions or updates to the agenda as you see it? All right, very good. All right, we have a busy day, and thankfully, we have 90 minutes today. So we have a little bit of extra breathing room. We have a couple of guests, which we're going to hear from first, and then we'll move on to our regular agenda. But first, item number one on the agenda is taking a moment to remember a couple of members of the ICANN family who we recently lost.

Pam Little, who you may know, is a longtime participant in ICANN processes. She's a longtime participant in ICANN processes, recently passed away, as did Cherie Stubbs, who was longtime secretariat for the Registry Stakeholder Group. And both these women were tremendous contributors to ICANN work. So I'd like you to join me in a moment of silence as we remember them. Thank you very much.

All right, we have a couple of guests with us today. First on the agenda, we have Ching and Ed from WhoIsAPI. You might remember they joined us in a recent BC meeting to present some research that they conducted on DNS abuse. They've come back with some updated data for us, and they've got 15 minutes on the agenda. Gentlemen, are you ready? The floor is yours. Thank you.

ED GIBBS: Thank you. My name is Ed Gibbs. I'm with WhoIsXMLAPI, and we're going to be talking about some of the research, like you said, that we've recently conducted. And to kind of show you and peer into exactly what that looks like as far as some of the badness goes on the surface web. So next slide.

Worked for some major companies, Symantec, Riverbed, Cisco, a few others. Started out in development, and current board member of PICDO, as well as a few other companies. And helped write a few books on cybersecurity. Next.

Pretty much the agenda. I'm going to try to stick to this. Within 15 minutes, it's going to be a little difficult, but I'm going to move fast. If you've seen the Cancun presentation, this is kind of a rehash of that, but with some updated figures. So next.

So what we're seeing is rather disturbing, of course. We look at things like, if you heard the term pig butchering, this is an up and coming issue. These are often, how do you put it, organized crime groups, syndicates that are almost enslaving people to scam for pennies on the dollar. And they don't make a lot of money at this, or the people behind it, but except the bosses in management and things like that. We're seeing a substantial increase in that, as well as CSAM material.

The CSAMs, what we also see is a migration from the root TLD to subdomains and host names. Because they know they can hide very easily underneath that. And chances are, you're not going to block Azure or AWS or anything like that. But typically, migrating to the left, they have a little bit more anonymity and can organize there.

So the pig butchering farms, these are, like I said, groups, organized crime. They typically register domains in bulk. We recently saw one with 10,000 domains registered in one day. And when we started to uncover that and peel it back, I reached out to some friends at Homeland Security, FBI, and things and said, does this look familiar? And they said, yes, don't touch it. You don't want to draw attention to it, so I'm not going to highlight it here. But the domains are out there. And we were able to use some of the algorithms that we helped develop through some data scientists that we have that was able to isolate what these domains were and the countries they were registered in and even identify the crime group behind it, which we don't want to mention here.

But like I said, they're commonly masquerading behind these. They appear as casinos, banks. Crypto recovery is a big one popping up to scam people. We recently encountered situations where people have lost $100,000, $200,000 in a single day. You know, imagine your life savings gone, your business account drained. And so the people behind this they simply don't have any regard for people or anything, they're there for one reason, and that is to get your money.

And we're seeing a lot of this every day. I can't tell you how many times we go in and we see thousands of bulk registered domains. And when we do a scan of them, most of them aren't active yet. And when we look at the security tools and products that are out there, they're only picking up a portion of it. And I threw the tagline out there, 15% of the time it works 100% of the time. And that's about what we're seeing. 15% of the domains that are registered in bulk are blocked. They're detected, but they're not detecting all of them. They're missing a lot.

And so we're able to see that and we're working with some of the large tech companies to provide that information to them.

The other issue we're seeing is a lot of the older domains, the scammers and phishing people and things like that, they're smarter and they're learning. And what they're seeing is these older domains have a higher value because they have a reputation behind them. And they can leverage that reputation to evade a lot of the security products, go through what we call newly registered domain detection.

If you look at the creation date and you're going to base a domain off of that, that's fine. But these older domains, if you look at the creation date, it goes back two years, five years, seven years which raises the question, how far back do you have to look in order to say this is not a domain that you want to do business with? Certainly you can look at all the attributes of it, but are you really going to make a decision based off of that if you have a high reputation score?

So some of the abusive domains, when we did some further research, we pulled all the DNS record, resource records, and basically built an algorithm to compute exactly what the profile of these domains look like. A lot of them don't have MX records or some of the other records you see up there. 99% of them don't have subdomains or anything. They're just thrown out. It's garbage, just pure garbage. But they're there for a reason sometimes, the majority of the time they're there. And if they can get one or two or three of them to work for a short amount of time, they're effective. So, next slide.

When the banks started announcing financial instability in March 2023, we saw through our analysis 3,900 subdomains. These are new

subdomains that were created with bank names in them. So like I said, they're getting smarter, they're moving to the left. You take Silicon Valley Bank, they had 21 of the 117 domain names that we saw. 51 of 816 had Credit Suisse and Signature Bank. And then other key words that we used, these seed values, bank collapse, bank alert, recover, a big keyword there, recover, because everybody's interested in recovering their money. Particularly in the crypto. And these fraudsters are popping up saying we'll recover your crypto wallet and things. Of course, they can't. But people don't know that. So, it's very effective. And so, we're seeing a lot of that. And privacy shields remain to protect their identity. Privacy shields are good, but they serve a purpose. And it's really hard sometimes to figure out exactly who's behind it without court orders.

These trends tend to reflect in DNS. And hence, the term DNS abuse. We can spot those trends. And we started writing some newer updated algorithms to base it on current trends in the world and highlight that in DNS. So, next slide.

When we look at some of these rat platforms, phishing, scamming, whatever you want to call it, we can see how many were taken down. We're starting to learn when websites are seized or domains, we can spot those and figure out exactly what the relationship is to those.

One of the more interesting algorithms we wrote recently was to go deep into these domains and really start to look at the information and cross-reference it using things like reverse WHOIS and different tools, and go horizontally across and figure out what other domains did they register by creation date, by name servers and different things and

figure out the association. And whether it's using tools available to us to figure out exactly—uncover the domains that they don't want us to know about. So, we're able to do that as well. Next slide.

The tech market releases coincide, a lot of times with iPhones, Google, Facebook, Apple, whatever the market releases are. We can see those connected domains pop up everywhere. And they come out fast. And very often, though, they show up in bulk registration. And so, a lot of those, like I said, really, they may never go active for some time.

The problem that we have is when do they go active. We can only do so many DNS resolutions without being blocked ourselves. You're looking at millions and millions of DNS calls a day to keep up with this. But the intent is really the security organizations that are out there are kind of keeping an eye on that and blocking it. And do a very good job for the most part. But like I said, they're not blocking all of them. It's impossible to detect them all. Next slide.

Fashion is also a big one. We see a lot of these now. Of course when you do keyword searches, see values like Armani, Cartier, Gucci and things, those are easy. It's when these move to the left or they start obscuring the names. You have a hard time trying to keep up with it. And it takes a lot of resources on the back end. And so, we're able to find a lot of those strings.

So, domains names that you would never think of, they're getting really creative on what these are. So 2,504 domains between January and March, that's a lot of domains that were bulk registered. Next slide.

This will be my last one. So, this is a kind of a peer into the cluster of these bulk registrations, what they look like. You know, some of these may look like nothing. You know, the trick is to hide it behind something that you can't see. Or you visibly see, but you don't know what's behind it. And the worst of this is on your mobile phone because there's no mouse to roll it over and say, okay, well, this is a bad link. You know, a lot of times—we recently had a case personally where being from a small town, we got a text message and it was from a local bank. It appeared to be from a local bank. And they were just broadcasting this to everybody they could in this area code and assuming you would hit it. Now, because they were targeting mobile phones, if you hit it from a desktop browser, nothing came up. But if you hit it from iPhone, Android, whatever, the domain would appear. They asked you to log in, what's your account number. It was the craziest thing in the world, how much information they were asking for. But some of these domains are behind that. And so, I was able to pull that up. So, again, that's my last slide. Brenda, I think we're going to cut it here and move on.

MASON COLE: Ed, thank you very much for that presentation. Very informative, and it feeds into our kind of ongoing concern about DNS abuse, which is maybe the main policy issue that the BC has been working on now for the past year or two. So, let me open the floor briefly for questions for Ed or Ching. Mark.

MARK DATYSGELD: Thank you very much. I am chair of the small team on DNS abuse on the GNSO Council. You mentioned bulk registration several times. This was

a subject that came back, back and forth between us and the contracted parties, and we were trying to find some common ground to work on that subject. But we never quite made it. The official answer that the Council is giving back to them is that currently we do not have enough evidence to start policy-based action around bulk registrations because it is this area that it appears at least from all the conversations we had that we don't have enough evidence, and the contracted parties do not have enough evidence. So, we do not know how to proceed exactly. So, could you discuss, at least in general terms, what would be good procedures for us to start finding those leads, what would be good ideas for us to head in the direction of closing in on these bulk registrations? Because the time would be about now, let's say.

ED GIBBS: It's very difficult. It's complicated because bulk registration does serve a legitimate purpose, right, that you would want to continue a business practice of because how do you distinguish between what's good and bad? It would take, like I said, an incredible amount of resources to do that. The vetting process would slow down that process substantially. But I really don't see a way around it.

You could rely on the upstream seller to vet it, but is that part of their core business? And at what information are you going to vet? You know, do you require a business license or proof of some form of intent? It's very difficult. And like I said, it's really going to complicate the process. You may not get same-day registration anymore, to where you have to verify documents and reach out and continue to look at what is the purpose of these domains and can that be automated, which is highly

unlikely. The more you automate, the more it's going to be abused or likelihood it could be abused.

So I'm not sure I have the answer to be able to figure that one out. I've thought about it, but really, where we are in this stage is, we know something needs to be done. But what is that answer and how do we effectively implement it?

MASON COLE: Thank you, Mark, for the question. Alex.

ALEX DEACON: Hi, everyone. And just following up on that, the question that I had is, would you be able to share roughly how you determine that a registration has been done in bulk? Is there an algorithm or some way that you've determined that these are bulk registrations versus other ones? I think that would be helpful.

ED GIBBS: We start looking for patterns. Without giving away the secret sauce, is being able to go into what the linguistics and semantics of those names are, then correlating who is registered at the time of the registration, the country and look for commonality between a lot of that. So it's cycled, recycled, recycled again, and refined. And we're able to group them within a sequence. So it takes roughly about eight hours of compute time among a cluster to be able to do that. So it's quite intense, and we're getting ready to update the algorithm. Right now,

we've got 16 computers in that cluster. We're going to upgrade it to about 32 to be able to dig deeper.

MASON COLE: Thank you, Alex. Other questions for Ed?

UNIDENTIFIED SPEAKER: [inaudible] here, Meta. Great presentation, Ed. I just had a quick question. You talked about domain aging. I was wondering if you've seen any trends in terms of that move to the left and domain aging in regards to DNS abuse. Just any kind of trends and correlations, like how long are they aging before the abuse starts, especially as it relates to subdomains?

ED GIBBS: So the aging process is becoming more and more popular. Secondary registrars continue to promote and sell them because they already know the keywords. They know their validity and how many hits they're going to get. And so they become a high value. And so the people acquiring those have very much interest in figuring out exactly how they can leverage it to weaponize it.

What we see, though, also is a correlation between the domain names that have a high reputation appearing in the subdomain records. So you can almost guarantee that anything that appears as a domain name can also appear as the subdomain. We're seeing a lot of that. And it takes an incredible amount of resources to go. Right now, we're averaging about three billion rows of DNS records that we have to go through and figure

out the correlation. So an incredible amount of resources being used to go into the depth of this and the abuse behind it. So, but there is a correlation, absolutely.

STEVE DELBIANCO: A quick follow-up. The beginning of what you said implied that some registrars realized the high value of proven strings and that they're selling those. Does that mean that they're suggestively selling them to potential registrants where I type in a domain name but, oh, no, registrar comes back with a lot of variants of that that I can get? And if you had evidence of registrars providing suggestions of names that feed into this process, that would be the most valuable screenshot you'll have shown me today.

ED GIBBS: I'll get that to you. There is evidence of that, absolutely. You know, when we look at some of the common platforms that are out there to register, without mentioning names, they do suggest what those names are. And there's a reason why they're suggesting those. So for them, the more value that they can offer behind that, of course, the more expensive it is. But if you can find a domain name that's expired or soon to be expired, and it has a high ranking, that would be potentially more profit for them.

CHING CHIA: So, very quickly, add on the conversation here. Some of the customers and partners that we talked to, they found that not only—and potentially kind of a registrar involved in the process. Also, the

secondary market player could be the places that the CNC and the operator to pick the domains from. Because the domain has been proven or has been registered for quite some times. And also, there's some other kind of traffic has been flowed in and out from the name. So, there will be considered from the cyber security point of view, a safer name than those newly registered names. So, those are also the sources. Yeah. Thanks.

MASON COLE: All right, folks, last question, and then I'm going to cut the queue, because we need to move forward with our agenda. Go ahead, please.

PAOLO ROQUE: Thank you. My name is Paulo Roque. I'm the president of the Brazilian Software Association. It's an association in Brazil with about 2,000 companies with revenues close to $20 billion. And employing more than 232,000 direct employees. We are very concerned about this DNS abuse. And we would suggest a stronger measure of knowing your customer when you accept someone to register a domain.

In Brazil, I also run a certification authority. We have to do all this know your customer procedure. We have to do biometric match. We have to check documentation. And I think we should apply the same thing in the domain world. Because now is a wild west and it's very complicated.

We understand that this start with the freedom in mind. But then the bad guys came in. And we will support any initiative in this direction. This is our main concern. Thank you.

MASON COLE: Thank you very much. That's very encouraging. All right. Oh, Mark, make it tiny, please.

MARK DATYSGELD: Very brief follow-up. So, that is in the recommendations of the GNSO Council for follow-up work on DNS abuse. Know your customer practices. And we will be exploring this over the next few years.

MASON COLE: Thank you, Mark. All right, ladies and gentlemen. Looks like the queue is clear and we need to cut it right there. So, item number three on our agenda. you may recall that we, the BC and the IPC have collaborated to fund a study by the DNS Research Federation, specifically as it relates to ccTLD practices and DNS abuse. And this is meant to inform our work on the NIS2 directive in the European Union.

Emily Taylor and Alex Deacon are here from the DNS Research Federation to give us an update on their research findings. And I know that many of us on the excom and others are really eager to hear what they found. So, Emily, may I turn the floor over to you?

EMILY TAYLOR: Thank you very much, Mason, and also thank you to the members of the BC and IPC for funding this study. I'm joined today, as you said, by Alex Deacon, our Senior Research Fellow, and also Nathan Alan, who's our Director of Engineering, and will sort of share out the presentation. So, if you go to the next slide, please, Brenda.

I'm going to just very quickly, very quickly describe who we are because we're a new organization, and then the background to the project, which you've just sketched out. And then I'll turn over to Alex to describe our sources and methods, and then Nathan will take you through some of our results. And then we will try and understand why the phenomenon that we were seeing, or what possible explanations there could be, and then look forward to questions after that. I'm sorry, next slide.

So, the DNS Research Federation is a new not-for-profit in the UK. It's founded by Oxford Information Labs, and we've got several members of our team here today in the audience. We're around all week as well, so we'd be very happy to talk to any of you.

Our mission is to advance the understanding of the domain name system's impact on cybersecurity policy and technical standards. Because as we were making the decision to create this entity, we realized that although in the ICANN community and in technical standards bodies, there is really vibrant engagement and a lot of activity, that world is somewhat misunderstood or not understood by the social science community and policy makers who are doing the cybers and regulating in many times.

So, we achieve our mission through education and research, through access to data, and we've used our data platform, the DAP.live, the DNS analytics platform, in creating this study. But it's an extremely versatile platform that we've created by open sourcing the 20 years of software libraries created by Mark, by Lucien and by Nathan here, and making

them available to the open source community for the purposes of this project.

And our last element of the mission, not so relevant for this space, but, of course, our experience of technology is very much determined by technical standards. There's an awful lot going on in that community relating to naming and addressing, and we wanted to break down some of the barriers to participation and make it easier to understand what is going on there. So, next slide, please.

The background to this study, as you said, Mason, is the finalization of NIS 2. That is a directive under the European Union law, and so, as many of you will know, it has to then transpose into the law of each member state. So, the next 18 months, finishing in around October next year, we'll see that sort of core element transposed into the national law of the 27 European Union member states.

So for this community, the article relating to WHOIS provisions has been a source of great interest because it is creating that sort of matching legal obligation to go with the GDPR that obliges registries and registrars to provide that WHOIS data, to continue to collect it and make it available.

And there are also additional data verification procedures which have to reflect best practices used within the industry. That's taken directly from one of the recitals, and nobody really knows what is meant by that, which will, I'm sure, become a term of art as time moves on.

So, these communities, the BC and IPC, wanted to learn more about the EU ccTLDs, those country codes who seem to have... You know, because

they have policy independence, they can do their own thing, and they've also all been living in the data protection environment for many years. And so we wanted to find out how their abuse rates compared with the rest of the world.

We also wanted to think about how those abuse rates relate to their market share, and also the impact of demonstrated effective practices which CENTR documented in a study, an excellent study that was published last November, and it's great to see the authors of that study, Polina and Peter, in the room today. So, we wanted to sort of bring those two data sets together and see how they interacted with each other, and then consider any other factors that might be relevant. So, next slide, please.

I'm now going to hand over to Alex Deacon, who'll take us through the sources and methods.

ALEX DEACON: Thanks, Emily. So, again, my name is Alex Deacon. In terms of sources and methods, we leveraged several data feeds within the data analytics, the DNS analytics platform, dap.live. The first being gTLD zone files, where we could actually see the domain names for the ccTLDs, and also we used Domaintools data to understand how many registered domain names existed for each ccTLD.

Currently, within the dap, we have several abuse-centric feeds that give us an idea of which of these domain names may appear on block lists for phishing, for example. We use OpenPhish in the APWG lists. For

malware, we use the abuse.ch URL house. And for spam, we use Spamhaus. So, those are the current feeds we have available in the dap.

And then we also went out and we had a look at, again, the ccTLD registration numbers, the pricing, and the population of the country related to the ccTLD, just to kind of put everything within perspective.

And then the CENTR study was actually quite helpful in terms of laying out the habits of data accuracy and processing and the like. We also used the European Commission's study on abuse, and Emily will talk more about this later.

So, what did we measure and how did we define abuse? For this study, we measured, as I mentioned above, just phishing, malware, and spam from those feeds that we had available to us. And the way we counted abuse was to count the distinct or unique domain names found on each abuse list.

This is important because we wanted to understand the rate of abuse for each ccTLD. So, we had to ensure we were comparing apples to apples and oranges to oranges. And so, we used this distinct, unique domain name methodology, which, by the way, is used by the DNS Abuse Institute, and we believe also the DAAR, although that's less clear to me, at least. And we counted the unique domains that we found on each of those lists for the year 2022, January 1st to December 31st.

And the numbers that, and the findings that Emily will present next, I think, is, or maybe it's Nathan. It's Nathan. I'm sorry. We'll be focused just on the year 2022. I think that was it. Next slide, please.

NATHAN ALAN: Yeah, thank you. So, yes, I'm Nathan Alan. It's nice to be with you all. So, the results of the findings that we had, the way that we were able to do that is to create some abuse rates, and the rates were calculated based on, as Alex mentioned, all of the reports across all of the different data feeds that we have, and that gave us an abuse total for a TLD.

We then wanted to find the abuse rates, and we took that total and divided it by the total number of registrations for that TLD. We then averaged all of those per TLD to try and find some kind of global standard, and then we put that into context so we could see how different TLD types, such as EU ccTLDs or the other ccTLDs that we had data for, the legacy gTLDs and the new gTLDs, how they ranked and how they fared. If we could go next slide, please.

So, as we can see, if we plot this in the graph, we can see that the EU ccTLDs are by far the lowest in terms of abuse across the whole market. And if we look at market share, if we can go to the next slide, please, we can see the breakdown of registrations by each TLD, and we can see that the EU's ccTLDs have 15% of the market share, and you can see the others, the new gTLDs have around eight, the other ccTLDs, about 22, and the legacy gTLDs. And by legacy, we mean com, net, org, those kind of TLDs.

And then if we move to the next slide, we can see how that actually breaks down in terms of abuse. So, the EU ccTLDs only have 3% of the overall abuse that we were able to capture, which, if you were to compare that in terms of market share, is significantly lower than you might expect if it was a level playing field.

So, that kind of summarizes the results that we were able to gather, how we were able to gather it, and how we were able to rank abuse rates for each given TLD. Thank you.

EMILY TAYLOR: The next slide, please. And when we dig down and look at those EU ccTLDs, which were our object of interest for this study, we can see that there is somewhat of a long tail, but actually, if you look at the numbers in the y-axis, you're actually dealing with fractions of 1%. So, these are really, really low levels of abuse. But as Ed's demonstrated in your excellent presentation, by measuring it as a percentage of the total overall domains, I hope that that doesn't minimize the impact of each of these abuse incidents, which is, of course, great.

But what we're seeing is that they're quite homogenous as a group. They're clustered in a very low level, which really makes it an interesting observation. Next slide, please.

So, as I said, one of our major points of comparison was the CENTR study. And so, we wanted to know what are the correlations between what we know the ccTLDs are doing about data and the low levels of abuse that we're seeing. So, if you go to the next slide, please.

What we found from the CENTR report is that about half of the TLDs in their group, which was the European Union ccTLDs, undertake automated syntax validation on the registration of domain names. Just a really simple move. You can just make sure that things aren't just garbage going on the way in. That although you may not really know for sure who exactly the registrant is, if their data fits the format that you

would expect for that field, then it can at least not be rejected. You know, so that simple measure, which is undertaken in about half of the ccTLDs in CENTR study, seems to be very doable and have potential enormous impact.

But also what was curious from the CENTR study, and makes sense when you know the ccTLD environment, is that they do all sorts of different things. So actually there's a very rich source of good practices or effective practices within that group. There isn't a single size that fits all. They're all doing different things that they calculate to be suited to their environment.

Only 20% undertake systematic identity verification. So a minority, but a significant minority. And it may well be that if you came back and revisited this in years to come, that that would go up. I think that probably there are some underlying trends that are changing within all of the environments.

So the most common move that we saw was ad hoc steps or that CENTR observed, so that when they have a reasonable suspicion about something, they go and follow it up and do something about it. And that was, so 14 of the 20 something ccTLDs in their study did this. And that was the most common.

But there are certain challenges to implementing automated identity checking because even within the European Union where there is huge harmonization of laws and practices, there is no pan-European identification system. And so within the ccTLD, you might have an effective way of checking your own citizens. But a lot of these ccTLDs also take global registration. So they are like micro gTLDs in that sense.

So they have all of the same challenges of checking international registration data. Next slide, please.

This is an unreadable chart that just shows how all of the different practices are all over the map effectively. And that's just taken from my reading of the CENTR study and putting it into a graph. Next slide, please.

So what do we learn from all this? So what? What we see is that there are very low rates of abuse here. So there's something interesting about this group of ccTLDs. But what we can't say is that they're all doing one thing that makes them different. And we can see a correlation between care and due diligence on data. We can't say for sure that there's a causation and there may be other factors that help us to explain why the European ccTLDs are so different.

These are very mature. And the domestic markets, these are very, very typically very, very wealthy, mature nations that have mature cybersecurity institutions, probably quite a lot of back and forth between the relevant law enforcement, public safety and local stakeholder groups that care about this. You know, in a way, the CCs are sitting in the middle of their community, much like ICANN does, and trying to satisfy a diverse range of stakeholders who all want them to do different things.

But there are also other factors like they have been living in data protection land for 20 plus years. And although the GDPR was a massive shock to the world outside of the European Union, actually those data protection principles didn't change very much from what the 1995 directive had.

And within this group, there's also a predominance of non-profits. And so the motivation primarily is to serve the community, to do a good job. They tend not to be diversified businesses, although not all. And as I've said, they have close links to local stakeholders.

But there are other quality markers. The renewal rates are really, really high. I think there's an average of 84% or something like that in that group. That tends to show that the people are really using and valuing their names. And that there is a much higher rate from other CENTR studies shows that there's a much higher rate of sort of developed web content. So these tend not to be junk domains.

Pricing and market penetration. Actually, I was expecting the data to tell a different story there. I was expecting that low price would mean high abuse and that ccTLDs with lots and lots of checks and balances would show low market penetration. And that just didn't come out at all. And so that's a really interesting, confounding finding for me personally, having been around this area for quite a while. So next slide, please.

Then finally, I wanted a bit of a shout out for the other ccTLDs. Because if you look at the y-axis on the—so we've been talking about the EU group on the left-hand side. So we're looking at hundredths of a percent at the lowest rate, okay? Look at Australia, look at Brazil, look at UK and Tanzania, Thailand. These are in the thousandths of a percent.

So we've created a dashboard to go with this on the DAP, which lets you kind of play around with the data and have a look at it. And actually, I think, and I'm really grateful as well to Peter from CENTR who read an early draft of this, and he said, how about you change the order of things

so that the best registries turn out as number one rather than number 577, which is what I've done. And I think that was a very good tip. Thank you for that.

So number one, two and three are outside the European Union. So my suggestion to these groups and those people who are interested in understanding what works in the TLD management is have a look at those as well, because they will be doing something interesting as well on data. So next slide, please.

So excellence, as Aristotle may or may not have said, is something that is not a one-off, is actually a habit. And I think that my takeaway from looking at this with Nathan and with Alex is actually it's a combination of factors. It's not just what you do, it's who you are and how you are that creates that excellence over a long period.

You know, I know that within our groups and within ICANN generally, we do like to focus on what's wrong and we need to, but it's also, I think, sometimes quite interesting and novel to look at good examples and say, well, what are they doing? You know, there was one football manager who said we had a bit of a rubbish team, but we looked at what winning teams were doing and we tried to copy them. And I think that this is what the NIS is encouraging us to do. And I hope that this study in a small way helps to start that trail of investigation. So thank you very much and look forward to your questions and comments.

MASON COLE: Emily, Alex, Nathan, thank you very much. Outstanding presentation and good research that I know we're going to value and use. So let me open the queue, if I may. Are you happy to take questions? Steve.

STEVE DELBIANCO: Thanks, appreciate your work. Just like Graeme Bunton's DNS Abuse Institute, the element that you count is a domain that has been used. And I understand that it may or may not be indicative of the quantity of spam and phishing that occurred with that domain, driving traffic to it or using it to fool people when they see it. And is it impossible or just too expensive to actually measure the activity? Probably. And then have you done any validation to know that just counting the number of domains that are used is in relation to, is it relevant to the quantity of abuse affecting the citizens who view that? Thank you.

EMILY TAYLOR: I'm going to turn that over to Alex because I don't know if you've seen or members of the community have seen, he's just done an outstanding blog for us, which looks at that very question. So yes, indeed, we did consider that issue and you're absolutely right. There are different and valid ways of counting abuse that come out with different results, but I'm going to hand you over to Alex who can speak much more to that point.

ALEX DEACON: Yeah, thanks, Steve. I think, well, we'll post a link to that blog. I think you'll be interested in that. I mean, the reason why we chose to measure abuse the way we did for this study is, as I mentioned too, when you do

the rates, you have to compare apples to apples, but it turns out there's lots of ways to measure abuse, as we know, and how you measure it really depends on, the victim of abuse, if you will.

So for the most part in the cybersecurity research world, they measure what they call phishing attacks, which is a more accurate measure of the impact of abuse on users. And I think the trends over the last two years is that those attacks have been going up.

When you count the unique or distinct domains that are used to perpetrate those attacks, it may be and often is the case that those rates are going down. So there's really no connection between the two. You can't make any assumptions either way. Abuse rates on users may be going up, does not mean that, well, sorry, abuse rates that are going down for unique domains used to attack users, if they're going down, it doesn't mean that abuse is going down in general. And so we'll send that link around and I think you'll find it interesting.

NATHAN ALAN: Can I just follow up just very briefly, just to mention that we look to all of the different avenues that we had in terms of reporting. And as Emily mentioned, we have a dashboard on the platform that shows a lot of the charts and slides that we have, but also a breakdown of all of the different abuse rates and levels for each TLD. You can drill down into more detail and see a more detailed overview of what's actually happening as well. So that's also available.

EMILY TAYLOR: And just a final thing. So sorry, but it was such an excellent question. I just wanted to reflect on what Ed was saying in his presentation, because we are also seeing that move to the left and that a lot of the, as things get tightened up at the top level domain level, we should expect more of that. And it really does point to a governance gap at the hosting level, at the third level domain providers, because that's really what's a major difference and it really comes through in Alex's blogs and he goes into that more detail.

MASON COLE: All right, thank you. And Steve, thank you for the question. Marie is next in the queue. Before I call on Marie, Emily and Ed, I just want to confirm, would it be all right if your presentations were made available to the BC? We'd like to circulate that. If you could send those either to me or Brenda, we'll make sure they get around. Okay, thank you. Brenda has them. Sure, okay. Marie, then Margie.

MARIE PATTULLO: Thank you. Obviously, firstly, thank you so much. I would like to ask a slightly different question, if I may. That is, when you looked at the different forms of validation, did you find a correlation between the drop in abuse rates with different forms of validation? Where I'm going to here is that, as you know, we'll talk about NIS2 at another point, but when we're working with member states—I should explain I'm based in Brussels—when we're trying to explain to them why we would like certain, to use your terminology, KYC, and there are some that are complex and there are some that are not so complex. Now, naturally, we're never going to get to zero, but we can disrupt. And the same with

anything, if you disrupt this channel, then at least we can move them into fewer channels, which we've got more chance of actually addressing.

Now, if I look at something like DK Hostmaster, they've been superb with reducing their rates, in particular in certain aspects like intellectual property problems. Because they brought in a number of validation methods. And it's a clear correlation.

So do we have anything that, when we are working with member states at European level, we can say, guys, see this? Proof, this works. And naturally, there is always that aspect when we're talking ccTLD, that this is your country's reputation. And the member states do seem to understand that the reputational value, which of course is extremely valid. So do we have anything around that? Thank you.

EMILY TAYLOR: We have incomplete data. I'll just get it out there. We mapped in that unreadable map I put up there. It showed all of the different measures that different ccTLDs were taking. And you're right, .dk was mentioned by several people as an example of a registry that is really doing a lot of different measures. And sure enough, it's got one of the lowest aspects of abuse. But it's not the lowest. And there are other registries that do a similar amount of stuff to .dk that are kind of in the middle. But you're also going, you're looking at an incredibly low base.

So if I was saying, what, we do actually abuse score, we risk score. One of the things that we would, one of our outputs was we produce a risk score for each of the TLDs. Each of the European ccTLDs comes as a low

risk because they're all in their different ways, they are doing things effectively. So the correlation didn't come out as strongly as I was anticipating. If I was going to make my imagined list of the top ones, it would be the ones with the most measures, but it doesn't come out like that.

So that makes me wonder whether in fact taking simpler steps like validating data on the way in, such a simple step could be a real game changer. And that the steps over and above, yes, they may make a difference. And, but there isn't that simple straight line correlation. So Cyprus has the lowest level of abuse in that whole data set, not Denmark. Denmark's not far off. And we're dealing with fractions of 1% here among all of them.

MASON COLE: Thank you, Marie. Margie.

MARGIE MILAM: Could you go back to the slide that had the 20% up? Yeah, there. Only 20% undertake systemic identity verification. Do you have examples of what that means, the systemic identity verification? Because I think when we were interested in the study, we were looking at it just to see like, what are common elements that would be useful to increase verification of registrants?

EMILY TAYLOR: So thank you very much for that, Margie. That was taken from the CENTR study and actually Polina and Peter are here. So they might be

able to add more detail. But my understanding of that was that it's about where do the checks take place in the system? So are you checking things on the way in at registration? So everybody, every individual or company goes through a range of checks and then you get your delegation? Or do you just let it run through the process and then if something causes a problem later on, you go and have a look at it and maybe delete it and maybe check it? And so that's how I understood systematic identity verification, that it's something that is part of the registration process. Everybody goes through it. But it may be that—yeah, they're nodding. So I think we're on the right track. Thank you.

MASON COLE: All right, thanks, Margie, for the question. One more question and then we need to cut the queue because we need to move on with our agenda, if we may. Go ahead, please.

NAT COHEN: Thank you for the presentation. As from the perspective of a domain name investor, when I looked at the country codes, the correlation that jumped out at me is just the difficulty in registering a domain in those country codes and also the difficulty, as Ed alluded to, of registering in bulk. Some of those registrars, it's very hard to do it or it's manual or it takes a lot of time. So if you want to register thousands of names or hundreds of names, you're just not going to do it in those country codes. Thank you.

EMILY TAYLOR: Yeah, I think that this is part of the dilemma for any TLD manager. It's like, how do you get just the right amount of verification and checks and make sure that your data quality isn't outrageous while also not turning away all your customers? It is something worth reflecting on that the level of growth among the European ccTLDs is lower than the average global growth. So that maybe tells us something about some friction.

I was expecting that to come through much more strongly in the market penetration test that we did because I thought coming to it with that assumption, which I thought, well, more checks equals less domains and rubbish market penetration. That just didn't come through in the data at all. SOme of the registries that have the highest level of checks have really, really decent market penetration up among the highest in that group. So it's a more complicated figure and picture than I was anticipating. But thank you very much for that comment.

MASON COLE: Thanks, Nat. Okay, Emily, Alex, Nathan, thank you very much. Outstanding presentation. We appreciate the data very much. So thank you.

EMILY TAYLOR: There will be a dashboard when we finalize the report, there's going to be a dashboard that we will make available that will allow a bit more drill down if you're interested in the detail.

MASON COLE: All right, thank you. Very good. Also, on the subject of DNS abuse, before we forget, there is later today an update from the Contracting Party House and ICANN on the proposed contract amendments that they're making to address DNS abuse. I believe the time is 1:45. I don't know, it's marquee one, two, and three. So if you're inclined, you should attend that session because it'll be very informative.

All right, okay, so the queue is clear. We're going to move on with the agenda if we may. Steve, let me turn the floor over to you for the policy calendar review.

STEVE DELBIANCO: Thanks, Mason. I'll go through this quickly because we're going to run out of time. We only have this room until 12:15. So the first thing I want to do is acknowledge the work of Tola and Lawrence on drafting our comment on the NomCom number two review. Our comments focused carefully on the handful of technical bylaws amendments that all made sense, but we differed with the recommendations in a couple of important areas.

And we used this as an opportunity to reiterate the BC's belief that the NomCom should not be naming eight of the 15 voting seats, but rather say six of the 15 voting seats, and that those two voting seats should go to the GNSO, one each to the Contracted and the non-Contracted Party House that would more appropriately balance the fact that over 98% of the revenue from ICANN comes from gTLDs and probably 95% of the work at ICANN is on the GNSO area.

If we were to do that, it also solves the dilemma we have in a Non-Contracted Party House of trying to arrive at a consensus candidate for board seat 14. Can you imagine if the CSG and NCSG each had a board member and so did the registries and registrars? These would be individuals that are keenly aware of the gTLD space, the work that it brings. So we'll continue to press on that through the holistic review. I'm not optimistic, but let's be transparent and aggressive about it. Thanks again, Tola and Lawrence on that.

For the open public comments, we have several. None of them close this week, so we have some time, but the IDN EPDP has released its initial report and I want to thank Ching Chiao sitting over here to my left for drafting our comment. We circulated it a couple of weeks ago and then they extended the comment period. So I'll be filing it on the 19th. This would be a great opportunity to see if anyone has any comments on that draft. Ching, why don't you go ahead, please?

CHING CHIAO: Thank you, Steve. Actually, not a comment, but actually an observation from yesterday's new gTLD status update is that we would like to file the comment. We were hoping to do this by the end of last month, but this being extended and now this issue, the IDN EPDP, according to ICANN Org yesterday, is actually becoming a critical path other than the closed generic item. So this somehow is interesting development that this is going to be, the PDP is going to be closed, phase two, it's going to be closed at November, 2025. So it's going to kind of become the roadblock for the overall AGP development. So I'd like to just to bring up these things here.

STEVE DELBIANCO: Is that because of controversies or complexity associated with the IDNs? Why is it taking so long?

CHING CHIAO: That's a good question. The complexity is definitely there, but myself in my own personal capacity, I'm not seeing a roadblock. I'm seeing more complication on the closed generic string issue. This could be dealt with, but not as that length of time that I actually expected, just to make it clear, yeah.

STEVE DELBIANCO: Are there any other comments or questions for Ching on the BC's draft comment on IDN? Ching, thank you again for contributing in that significant way. Zak Muscovitch then stepped up to the plate and volunteered on a comment that closes in a couple of weeks. It's on the ISPCP constituency charter amendments.

They're amending their charter in many ways to conform with the good practices that came out of Work Stream 2. And it's an extensive revision, but it looks familiar. A lot of the revisions in there look similar to the BC. Zak, we circulated your comment for member review, and I wanted to see whether you wanted to walk us through what you found.

ZAK MUSCOVITCH: Sure, thank you very much, Steve. As Steve mentioned, it's a best practice for constituencies to update their charter now and then. This particular one hadn't been updated since 2009. The BC's, by

comparison, has been updated as recently as 2017. And so we're in fairly good shape, but at some point in time, we'll probably want to update ours as well.

And this particular one serves as a fairly good example of an updated one, in my view. I'm not particularly familiar with ISPCP, but so if you have colleagues or friends that are in it, it's worth perhaps canvassing any issues that they're aware of that need to be addressed in this.

And although what attracted me to this comment in the first place, I was told that it could be done in one sentence, I did nevertheless try to come up with some kind of criticism. So please take a look at that and share your thoughts. Thank you.

STEVE DELBIANCO: Thank you, Zak. And your criticism was advising them to change some of the wording they had in what they would ensure. To say that they would aspire. I think it was a great piece of advice. I hope they take it. Thank you, Zak. Any comments or questions on that work? We'll be filing that on the 26th of June.

We also have an open comment period on the PTI and IANA governance proposal. These are a handful of bylaws amendments for the technical identifiers organization. And they are mostly about aligning the timing for the op plan, budget, and strat plan. I do not believe we will have much to say about it. I want to thank Rajiv from Google for volunteering to draft the BC Common. He understands this topic very well. But they are very administrative amendments. And you'll have a chance to review that prior to submitting it on the 5th of July.

And then earlier this week, actually later this afternoon, we'll have an opportunity to listen to the contract parties talk us through the changes that are being made for registry and registrar agreements to account for DNS abuse. It is probably worth me showing, if I can, a screen or two on what that might look like. Let me see if I can bring it up. Because the changes themselves are worth the BC to understand. Let's see. Nope, not trivial here.

All right, so the abuse mitigation that you see here, the first one up is the registry agreement. It's probably more interesting to look at the registrars. So what we see here is that the registrars in blue are the changes. So they have to maintain an abuse contact to get reports of DNS abuse. They added that word and/or conspicuously and readily accessible form. The key though is right here.

For the purposes of this agreement, a DNS abuse, what it means, and there's a list of explicit definitions with a reference to another place to get the deal. That is not as extensive a list as we might have wished. Although I do not believe we will be successful at lobbying for an extension of what that list includes at this point in the negotiation. Their negotiation began with ICANN Org. It's a bilateral negotiation between the contract parties and ICANN in which we encourage ICANN Org to represent the interests of us and the other users and registrants of the internet. They don't necessarily concede to do that, but we will insert ourselves into that equation. We have tried to look for a more expansive definition, but this is the definition they locked into as a precondition for their negotiation. I don't think it's going to change.

With that in place, when they have actionable evidence, and this is the new obligation, when a registrar has actionable evidence that a registered name sponsored by them is being used for DNS abuse as defined, they have to promptly take appropriate mitigation actions that are reasonably necessary to stop or otherwise disrupt.

That is all brand new language. It's an obligation not just to collect and report, but to actually take action. I don't know, maybe we ought not to let the perfect be the enemy of the good, but let's at least explore. And Margie Milam has volunteered on the BC side to take a look at what we might say about this language. Because that's really all that's on the table, are the words. Later, presumably, we'll work hard to get ICANN Compliance to step up and ensure that it's actually happening, right, to track it and enforce. But at this point, I think all we can comment on are the words. Margie, did you want to say anything about the registry or registrar work that you volunteered to help us with?

MARGIE MILAM: I have had a chance to look at the amendments. It certainly is a step forward, and I want to acknowledge that the contracted parties have done a great job of trying to address this issue. As you guys know, the BC's been talking about this for many years, and it's great to see some action here.

When I look at the language, I see areas where there can be improvement, and I think that's where I'd like to focus the comments as we develop them for submission. For example, what certain things mean, I think is going to be very important, in particular, actionable

evidence. That's one that kinda jumps out at me as an area that I think needs clarification.

Because in my observation, ICANN Compliance tends not to enforce where they don't really understand what it means. And we've heard that from ICANN Compliance in the past. So I would suggest that defining what actionable evidence means is probably going to be something that we could focus on.

Another is, if you take a look at 3.18.2, it says domain name that it is being used. So you have to have actionable evidence that it is being used for DNS abuse. And this is an area where I think we are already seeing problems, even in the current voluntary program that registries and registrars are engaged in right now.

Because what typically happens in the cybersecurity space is that when, and you guys, I'm sure, see this as well, when there's a malicious domain name that's being recognized, oftentimes the hosting provider may take it down. But that doesn't mean that the domain name isn't still able to be used for abuse in the future. And at any moment, the registry or registrar, when you send that notice, content might not be live at that particular moment. Yet we may present evidence that the abuse had taken place in the recent past, which is why it was actually suspended by the hosting provider. We want to avoid the whack-a-mole problem. And so that's an area in particular where I would say we'd probably want to focus on is being used, has been used. Because that way, it gives a little bit more freedom to be able to submit the information and then get the domain name actioned on.

The other thing that I think this misses is the abuse at scale issue. And this is something that the presentations we heard from both of the presenters today haven't pointed out, the scale issue. And if you remember years ago—it's probably, what, four years ago when the CCT recommendations were approved by the board, there was actually a CCT review team recommendation that related specifically of recommendation 15 to systemic abuse. And the recommendation to the ICANN board at that time was that ICANN should negotiate the RAA amendments and amendments with the registries to deal with systemic abuse.

And so that's completely absent from these negotiations. And I think that there should be an explanation for why the CCT review team recommendations haven't been addressed yet. So these are the kinds of things that jump out at me. But certainly, it's a step forward, and I don't want to diminish the fact that it is a step forward, and we appreciate that the registries and registrars have done this. And so as we work on the comments, those are the kinds of things that I would focus on.

And then the other area is the web form concept. Because we see a lot of problems with the web forms in the current state. Oftentimes, registries will have very—not registries, registries or registrars, but probably registrars, have very limited abilities of providing information to support your request. They might limit the number of characters, they might not like a PDF attached to the request, that sort of thing. And that's actually the kind of thing you need to be able to provide the actionable evidence to have the domain name abuse acted on.

So I want to be cautious that we don't end up in a situation where the web form makes it more difficult to actually prove the DNS abuse to be able to have the takedown acted on, so the domain name acted on. So those are the kinds of things that jump out at me right now, and I'll keep looking at it to come up with recommendations for the Business Constituency.

If we can look at the registry amendments, those, I think, are even more interesting, and I just wanted to point out a few things that I saw in the registry agreement.

Okay, this one is pretty wishy-washy. It says, where a registry operator reasonably determines, based on actionable evidence, that a domain name is being used, the registry operator must do two things, take appropriate mitigation action, so we don't know what that means, although it does say that are reasonably necessary, but it says that a minimum shall include a referral to the registrar. So they can satisfy their obligation by referring it to a registrar, or they can take additional action.

And so if we're thinking that this is going to be an obligation that requires a registry operator to do something, the minimum thing, right, we're talking about the minimum, is they refer it out to the registrar. Well, that's not, in my view, really taking action on DNS abuse, and I was expecting a similar obligation to what we saw in the RAA.

So I think that's another area where we'd want to focus our comments on, because it doesn't seem to me that it's really putting an obligation that's going to be enforceable from ICANN Compliance in a way that we would like to see as a business constituency.

STEVE DELBIANCO: Beautiful, thank you, Margie. We have a queue right now. We have Crystal and then Mark, and I would just suggest that not only today, but in our CSG CPH gathering on Thursday, we take the opportunity to acknowledge and thank the good faith effort that we've seen. Let them know we'll have a couple of ideas and suggestions to make it even more effective. And that's not going to be a surprise to anyone in the contract party house, but I do want to surprise them by acknowledging and thanking them for the effort. Crystal first, and then Mark.

CRYSTAL ONDO: And full disclosure, I was part of the negotiating team for registrars on this. I just want to just high level what Steve started saying at the beginning, this is not perfect. It will not ever be perfect. This has to pass 90% of registrars. 90% of registrars have to say yes to what will be in the contract.

I think your questions are totally valid. I do recommend everyone read the accompanying advisory. Jamie went to great lengths to explain what actionable evidence means to him. There's a lot of examples in there as well. So have a read of that. But I just do want to temper the BC in terms of whatever you ask for, whether it's provided or not, eventually 90% of registrars have to say yes. And that is a very high bar. And I think we need to recognize that we can't ask for unicorns and puppies. It's just not going to pass 90%. And that's unfortunately where we stand. So just keep that in mind as you're phrasing terms and I think coming in at least acknowledging that this is more than registrars have to do now. Registrars now, send me an abuse report. I can send you an

auto response. Thank you. And that's the only requirement in the current RAA. So this is a huge step that registrars are willing to take. And I think trying to undercut it would be a huge disadvantage to the entire community.

STEVE DELBIANCO: Mark.

MARK DATYSGELD: I would like a unicorn, perhaps not from this particular process, but in general. So how should the BC react to this? I would say warmly, very warmly, especially towards the registrars that they delivered the thing we asked. This cannot be overstated. We asked for this and they delivered this. And this is a potential way forward for other things in the future, for future ways of improving the DNS and improving this community. So let's be very clear about, this is pretty much what we asked. This is pretty much what they delivered.

The registry is trickier. Maybe there's more to be said about that, but no matter what we do, let's keep the tone very, very, very warm and very open. Let's talk to our CSG colleagues to as well join us in this effort of saying, hey, this is a good thing, because not necessarily the entire community will be seeing it that way. There will be people who will never, regardless of the amount of good that this will do, will say, oh, but this is subverting the multi-stakeholder process and other things that I have heard circling around.

So we have to defend this. We have to gather around this and show that this is a good way of doing the thing that we are here to do, which is

protecting businesses and customers and actually making the internet better. So whatever we do and say, let's keep that position very clear. We are very supportive, very warm, and we have a few comments.

STEVE DELBIANCO: Can I assume that, Crystal and Mark, that you would join Margie on the drafting team for these comments?

CRYSTAL ONDO: I probably shouldn't, just because I am doing it on the other—

MARK DATYSGELD: I don't know how much COI I have on this.

STEVE DELBIANCO: Who else can join and help with this, help Margie and I on these comments? It'd be a great opportunity. You can obviously see that it's a relatively small, bite-sized portion of content. You don't have to read very much, and anything we say is to be very finely tuned. All right, I'll be badgering you about that later. Margie, why don't we wrap up on this one and move along?

MARGIE MILAM: Yeah, there's one other point. The amendments only apply to the base agreement, so it doesn't apply to the legacy TLDs, and I don't understand the rationale behind that. Maybe, yeah, Crystal?

CRYSTAL ONDO: Verisign, they have agreed to incorporate this into their agreement, so it will apply to legacy TLDs as well.

STEVE DELBIANCO: That's in the Verisign LOI. Okay, thank you very much. Let me move on to the next item, which is the draft framework. This is not a public comment that's [inaudible], but it's a draft—Go ahead, Paolo.

PAOLO: Sorry, quick question. The draft of the new obligation is very good. Is there any penalty if the registrar or registry doesn't comply with that?

STEVE DELBIANCO: Thank you. ICANN Compliance can warn a contract party that they're in violation of any provision of their agreement or consensus policy. If they don't cure that over a certain period of time, they can move to that next level of enforcement of defining that they found a breach, and a breach may or may not turn into being disaccredited as a registrar. It rarely, if ever, happens, and often it doesn't happen because Compliance will tell us we don't have the language that's specific enough to be able to hold them to an obligation.

So this whole point that Crystal and all of us have talked about is to give language in here that ICANN Compliance can say, oh yeah, this is, I can enforce this. I can hold people in breach. I can take away their accreditation. Okay? Great.

So the other comment is the closed generic gTLDs. Now the BC has been very clear about this. We believed that we would be concerned if there

was consumer deception and competition fraud if a single competitor ran a generic TLD in a market that that competitor worked in and if they ran it in such a way that consumers would be deceived if they went to second level in the main .TLD, like eco.hotels, but it turns out it only shows the hotels or features the hotels that the owner of the .hotels generic closed TLD wants to be there.

So if one wants to run a closed generic TLD where they are a competitor in that industry, the BC wanted to see appropriate consumer protection and competition safeguards. These may or may not be preemptive safeguards. They might emerge post delegation based on the behavior that's there. But this whole project looked at whether there could be preemptive safeguards for closed generics. I have read this over. It is wildly complicated. It is running a gauntlet to get your application through if you're a single entity choosing to run a generic word and using it for your own purposes. And your application sort of gets flagged for further review. You go through a whole lot of tests of how explicitly you declared your intentions. You have to meet a public interest test for the process. It's not likely we'll see a lot of closed generics in the next round if the framework emerges, anything like this.

I was shocked to learn this morning that it's almost a two year long, 96-week process for the closed generics to finish their work, 96 weeks on something for which a dozen TLDs might qualify. So this is vintage ICANN overkill. And I think that we should do our best to see if we can accelerate it. We are not all that active on that. Tim, do you have anything you want to add on closed generics?

TIM SMITH: Hi. No, nothing to add on that, Steve.

STEVE DELBIANCO: It's not an official public comment. So I will have to coordinate—that's my role—with you to get a comment filed. And I don't think we just want to beat them up for taking too long and making it too complicated. We have to offer constructive suggestions. I don't think we have anything on NIS2. Marie, looking at you. Okay. Thank you. So I'll turn it over to councilors right now. I know we're running short on time. Tell me how to advance.

MARIE PATTULLO: Thank you. I'll keep this quick. For those of you who don't know us, your councilors are me and Mark, who's over there. I know we are short on time. We have a meeting tomorrow. It's public. Please come. 30 minutes of that will be what we're calling a town hall. There are two ways of looking at that. Either you come to the microphone and ask us questions or you come to the microphone and shout at us. Both of those are valid.

Within our bit of the council, we are directed by you. Mark and I don't make it up as we go along most of the time. So if you do want us to do something, not do something, comment on something, let us know. Please let us know. There are a couple of things that we'll see if you read through the policy calendar. We don't need to go into now, but we have an unofficial kind of meeting on Thursday about something we discussed at the last public meeting, the so-called SOI, the statement of interest.

Very simply, where we are on that, there is an exemption, has always been an exemption. When you fill in an SOI, when you want to be involved in a work stream at ICANN, you say, are you here on behalf of someone? Yes. Who is it? Not telling you because I'm a lawyer and I'm not allowed to. It's always been there.

But for reasons that none of us are quite sure why, suddenly it became a thing that we're trying to capture everything and we're going to be in every working group. Anyway, having proven by figures that this basically never happens, and if it did ever happen, it would be a minuscule part of never happening, what we're looking to do is turning up a little bit more. Are you here on behalf of someone else? Yes. Are you going to tell me who? No. Why not? Because I'm a lawyer and I can't. What kind of a client is it? Somebody in the stripey carpet industry, something to that level.

Now, we understand from the conversations we've had, both within the group and with friends and colleagues throughout the community, that just about everybody's happy with that. So that should be Okay.

But the link to the document is at the end of the policy calendar that Steve sent around. That's about the only active thing. If you do have an issue, please let me know before Thursday.

And before I hand it over to Mark, there is one other thing I'd like to say, is that we, Mark and I, have made it one of our little things to do, to go around and prove that, firstly, the BC is not big, evil corporate America, that we do have one-man bands out of Brazil that were actually quite nice. With the help of people like Paul as well, we've proved that we are allowed to talk to the NCSG without hating each other.

I realize that might sound childish, but it's something that's actually quite hard sometimes, and we are very determined to keep that going. And that's why I, on a personal level, would like to say, yay, that Lawrence is coming in as our next councilor, because if anyone thinks it's white corporate America... And you guys are going to be a dream team, and I'm so glad I'm handing it over to you. Thanks.

MARK DATYSGELD: I'll add briefly to... First of all, Lawrence! Second, SubPro, we have a bit of an update in terms of timeline. I won't go too deeply into it. They say 2025. It looks a little bit... That word. Fill in. Like, it needs to be sped up, and ways need to be found to speed that up, and the EPDP team is actually willing to do it. The bottleneck is in ICANN Org.

So the real question here is, how do we manage this moving forward in a way that we help the EPDP team move faster, while also pressuring Org to allow them to move faster? That's the game we're going to have to play the next two years, according to them, but I'm very hopeful that we can expedite that. So that would be the headline here. And back to Steve.

STEVE DELBIANCO: Any questions for our councilors? And remember that you can actually walk up to where they're sitting in Council and tap them on the shoulder, instant message or Skype them, or email. So communicate with our councilors, please. Any questions? Okay, fantastic. I'll turn it over to Tim Smith for CSG.

TIM SMITH: Thanks, Steve. Very quickly, CSG has been working with NCSG on Board seat 14. We haven't been making much progress, but we did agree to have a face-to-face meeting later this week on Thursday morning. And I think both parties believe that we need to spend more time together, understand common interests. So that's a starting point in this process. And we'll let you know how we make out on Thursday and keep working on Board Seat 14.

Beyond that, I guess the only other issue which we haven't discussed within CSG is this request for participation in the IANA Naming Function Review. So that's something that we'll be addressing, perhaps not in our Thursday meeting, but certainly before the deadline of June 30th.

And other than that, there is a CSG meeting on June 14th, which is tomorrow, I think. And then the CPH and CSG meeting, which we've already discussed a little bit, which is taking place on Thursday afternoon. And that's really everything for me.

MASON COLE: Thank you, Tim. Thank you, Steve. We are a bit over time, Brenda, sorry. I know that we're... I know. I know, we're going to push it just a bit. We're going to go to Lawrence and then I think we can adjourn after that. Caroline, I think Lawrence is going to provide details on the reception. And by the way, everyone please give Caroline a hand because she has worked very hard on this reception. Caroline, thank you for all your hard work. It's going to be a great event. So thank you. Lawrence, quickly, please.

LAWRENCE OLAWALE ROBERTS: So just riding on that, our outreach event is later this evening, 6:00 PM, at Yardbird. And I have also circulated to members, basically, the body of what I'm supposed to present. Since we're out of time, just to say a big thank you, not only to Caroline, Chris Mondini was here a few minutes ago, thanking the ICANN team, Naela, Chris Mondini, Joe and Andre, not only for helping to support, we had to go through multiple meetings and they're also picking a portion of our bill. So see you later this evening. Thank you.

MASON COLE: Thank you, Lawrence. And I'd also like to say that Tripti Sinha, the ICANN chair, will be a guest at our reception tonight. So I hope everybody can come and say hello. There'll be a couple of board members also in attendance. So Yardbird at 6:00 tonight.

Okay. We ran through that agenda really, really fast. So sorry, even though we had 90 minutes today. So any other business quickly before we adjourn? All right. Thanks, everybody. BC's adjourned.

[END OF TRANSCRIPTION]