ICANN75 | AGM – GAC Discussion on DNS Abuse
Tuesday, September 20, 2022 – 10:30 to 12:00 KUL

JULIA CHARVOLEN: Hello and welcome to the ICANN75 GAC discussion on WHOIS in Data Protection Policy, including accuracy session on Tuesday 20th of September at 2:30 UTC. Please note that the session is being recorded and it's governed by the ICANN Expected Standards of Behavior. During this session, questions or comments submitted in the chat will read out if put it in the proper form.

If you're remote, please wait until you are called upon and unmute your Zoom microphone. For those of you in the GAC room, please remember to raise your hand via the Zoom room. For the benefit of our other participants, please state your name for the record and speak at a reasonable pace. You may access all available features for this session on the Zoom toolbar. With that, I will hand the floor over to the GAC chair, Manal Ismail.

MANAL ISMAIL: Thank you very much, Julia, and welcome back, everyone. We will continue our discussion on who is in data protection for the first 30 minutes of the session, and then we will start discussing GNS abuse. So without any delays, let me hand this back to our topic leads. Laureen, is it you?

LAUREEN KAPIN: It's still me. My name is Laureen Kapin, and just for the benefit of the transcript, I'm speaking in my capacity as a member of the GAC Small Group dealing with domain name, registration, data issues, and I'm also a co-chair of the Public Safety Working Group. So to put us back where we were, we were discussing key features of this proposed design, and now what I'd like to do is move on to the next slide and discuss some issues that relate to risks and concerns and some feedback from the community that was just discussed over the weekend when ICANN Org presented its design paper.

So, the first part of this discussion relates to risks and related concerns that ICANN Org itself identified in its design paper. First of all, there's uncertainty as to whether registrars will participate. The participation is voluntary, and I know we got a question about this from Brian Beckham in the chat. This system is not the result of board approved consensus policy recommendations, so it is not mandatory.

I think that is the simple answer as to the question, "Why shouldn't this be required?" I certainly think it should be encouraged, and hopefully many, many registrars will choose to participate. There's also the issue of how do we make sure that people know that it's there and a useful system for them to use.

A lack of awareness can lead to low requester usage, that's the other side of the equation. We want registrars to participate because they can deal with the request, but of course, we also want there to be requests in the system, and that's only going to happen if folks know that the system is there.

So that creates a need for a lot of outreach, education, really marketing of this system. There also are some perhaps misconceptions about guaranteed disclosures. One of the comments from the community is that, well, maybe calling this a WHOIS Disclosure System might actually help create that misunderstanding that there may be a misconception that if you make a request, you're guaranteed to get the information you seek. That isn't the case.

So I think this points to the need to manage expectations both perhaps in the name of the system and in any outreach that is conducted to educate people about its availability. There's a risk that it might not produce the information that would be most useful. Really, this whole endeavor is aimed at getting at the question, "Will this system serve the needs of the users?" At least that's one of the key questions. It's not clear whether it would produce such data. It's not clear in advance. Then finally, there's also a concern that at least as presently configured, hopefully this will change.

There's no functionality for law enforcement's requests to have the opportunity to seek to make that request confidential. Many times, law enforcement is conducting investigations that they don't want the targets to know about, and in the phase two recommendations and recommendation 12, there is the capability to request for a law enforcement request that that request be kept confidential. We would hope that any proposed system includes that functionality. So here's a little preview of some feedback from the community discussion following the presentation.

The Intellectual Property Constituency chair encouraged ICANN to rename this to instead of a disclosure system, a request system, and again, this deals with managing expectations. I want to flag the importance of logging. A lot of the information that could be generated from this system actually falls outside the communications that take place in the system. So, if we look at this diagram on the screen, you'll see that the requesters submit the request into this portal through their ICANN account, and then the registrar can access that request. After that, everything else falls outside the system.

So if there's logging to be done, for example, by the registrar about how long it takes to respond to the request, whether they grant the request or deny it, and reasons for denial, that is all done at the choice of the registrar and within the time that the registrar would deem appropriate. So again, because that's really useful information about whether the system would meet the needs of its users, that points to an opportunity to really encourage that that logging take place. Then there's one additional logging issue.

Again, because registrars may choose not to participate in the system, there's a chance that you could get a request from an entity or an individual for which no registrar is going to pick up that request because they choose not to participate. In that event, the system currently doesn't provide for logging that request. The business constituent pointed out that that in itself is useful information, and even if a request relates to a registrar that doesn't participate, that still should be logged because that's useful data. So that's the big picture overview of the current design.

In terms of timing, this can be done very quickly if the small group, the GNSO small group that's charged with taking a look at this and making suggestions for improvements or approving it as is, if that happens quickly there's this window of opportunity to provide feedback by October 10th, which would allow for possible implementation in the first quarter of 2023. So all this points to the need for the community to take a good look at this, a careful look, but then quickly provide feedback via the GNSO small group that's tasked with focusing on this proposed design.

I can take a pause there for any quick questions. I'm mindful, we also want to get to within the time remaining. The next 20 minutes, we also have accuracy which in itself is a very important topic, and then some timelines about comment periods. I did want to do a quick pause here, just if there are questions on the proposed design.

MANAL ISMAIL: Thank you very much, Laureen. I can see a question from Russia in the chat and I see UK's hand up. So please, if you would like to answer Russia's question in the chat and then I'll give the floor to UK, and then Brazil.

LAUREEN KAPIN: I'm just looking at Russia's question, "Does ICAN plan to create a certain set of rules for registrar within the operational framework of this system, or will it be completely best effort solution depending upon the registrar's decision on the obligation of the response, positive, negative response, timing, scope, explanation of the refusal to request?" My understanding, which may be flawed, but my understanding is that this is all at the election of the registrar that part of this streamlined, simplified process is, the request is directed to the registrar, and then the registrar takes it from there, and there aren't rules for what happens next. That's my understanding.

MANAL ISMAIL: Thank you very much, Laureen. Yes, I also understand that the request is logged on the system, but then any further communication or clarification between the requester and the registrar is done outside the system. Chris, is this to the same point before I give the floor to UK and Brazil?

CHRIS LEWIS-EVANS: Yes, it is.

MANAL ISMAIL: Please go ahead.

LAUREEN KAPIN: Go ahead.

CHRIS LEWIS-EVANS: Thank you, Laureen. Chris Lewis-Evans for the record. Yes, just to add to that, there is within the design paper on the response decision a recommendation for a dropdown list that the registrar should fill out, they do deny it. Again, that would be a best effort collection from the way they target paper. So there is a capability there within the system for that to be recorded. Just how mandatory that is is hard to tell from the document that we have. Thank you.

MANAL ISMAIL: Thank you very much, Chris. UK, please. Ros, go ahead.

ROSALING KENNYBIRCH: Thank you. Ros KennyBirch, UK. Just to check my understanding, could I just check some of the reasoning as to why registrars might choose not to participate in the system? Thank you very much.

LAUREEN KAPIN: You're hearing me laugh a little bit because I think the registrars actually are best positioned to answer that. I will note that requests can come to registrars directly. That's the current state of play. So any other remarks by me would just be speculative, but I will note that there is a separate path for requesters to go directly to registrars. So the rest I would say to please ask your colleagues from the Registrar Stakeholder Group because they would be much better positioned to answer that question than I.

MANAL ISMAIL: Thank you very much, Laureen. I'm sorry. I thought I heard someone trying to speak. Just bringing to the attention of everyone also, Yuko's response in the chat to Russia. So please if you would like to read it meanwhile, I'm giving the floor to UK, I'm sorry, it's Brazil. Please, go ahead.

LUCIANO MAZZA: Thank you, Manal. Luciano from Brazil. Now just to thank Laureen for the detailed explanation on the proposed system. Of course, I think anything we say right now is very preliminary, we're just, let's say, starting the discussion, this new simplified proposal. We see merit in many elements of this. We think that a simplified system might be of better service to the purposes that are there. Something that we, information that we gathered from our enforcement agents in Brazil. I think two elements were important to them.

One was that had no cost, not because it's expensive, but because the bureaucracy of paying for the services makes it not feasible. The other thing is a certain level of decentralization from the point of view of the requesters because we have decentralized would make the system very complicated. So with a similarity in the way the concept of this system is being envisaged. On the other side, I think there are certain questions that we have to make in relation to how useful the system will be compared to the reality we have today.

So let's say if the registrars are not -- if participation is voluntary, for instance, and if you don't have a system of accreditation for the requesters, in the end, the system will be not very unlike what we have today when a law enforcement agents will directly contact a registrar and try to get that information, and with a disadvantage, because nowadays, let's say a Brazilian authority make a request to a registrar in the United States, for instance, no one would be really worried about your GDPR because it does not apply to that request.

That will be a matter for the data protection law of Brazil and the data protection law of the United States. If that goes via an ICANN-centralized system, perhaps other considerations in terms of data protection will come into play. So I think in the end, what we have to see is what the added value is of having a system that's very simplified.

As I said, I think that we have to reflect upon this, we see merit in having a simplified system, but again, if that's not something that is-- if it's voluntary from the perspective of the registrars, perhaps the added value won't be that much. As I said, just a preliminary comment, we have to analyze in more detail this concept paper, and I think we have time to deepen the conversation on those topics. Thank you. Thank very much.

MANAL ISMAIL: Thank you very much, Brazil. I have Chris and Gabriel, I believe in response to Brazil's comment, and then I'm giving the floor to Canada. So please, Chris, is this to Brazil's point?

CHRIS LEWIS-EVANS: Yes, please.

MANAL ISMAIL: Please, go ahead.

CHRIS LEWIS-EVANS: Chris Lewis-Evans for the record. Well, thank you very much, Luciano, for those comments. I think some of those key benefits are really advantageous as you've mentioned that centralized point, and certainly from a bureaucracy point of view, I think that was something covered is the difficulty law enforcement and governments entities will have paying for a system and getting through that red tape, so really key points.

I think just to flag I think what I said in one of the earlier slides is really key benefit here is to move towards a complete system. Whilst it's not much more currently than what we have at the moment, there are some benefits, and if we can keep iterating onwards, I think that's what we've got to look at and what we've got to push forward for. Thank you.

MANAL ISMAIL: Thank you very much, Chris. Gabriel, on the same point?

GABRIEL ANDREWS: Yes, ma'am.

MANAL ISMAIL: Please.

GABRIEL ANDREWS: I just wanted to flag my perspective as a law enforcement officer, an internet cop, if you will. Even someone with the amount of experiences I have engaging in this ICANN space and the DNS ecosystem, even I, I can struggle to find the right points of contact for certain entities, whether they be registrars or hosting providers or what have you. So I really just wish to underscore the usefulness of having a centralized portal to initiate requests just to save on administrative time. Cops are often overworked just knowing that singles place to shop, there's value to that is my 2 cents speaking from an investigator's point of view.

MANAL ISMAIL: Thank you very much, Gabriel. I have next Canada, and sorry to keep you waiting. Please go ahead, Charles.

CHARLES NOIR: Thank you very much and good morning colleagues. That's Charles Noir for Canada. So I arrived a bit late, so you may have covered this, and apologies if you have. I'm curious about -- there's the information that entities will be requesting, and I've heard you talk a lot about the importance of logging and ensuring that we understand who and when a request is made.

I also understand that law enforcement, of course, will have hopefully the ability to keep those requests confidential. I guess my question is about who has access to, or what are we thinking about in terms of what might happen with the data that's logged or the requests is, are actors going to potentially have access to those records, say in a court case, for example, or what kind of transparency and what kind of accountability are we thinking about there in terms of access to the data about the requests themselves? Again, apologies if you did cover that. Thank you.

MANAL ISMAIL: Thank you very much, Charles. I see Chris' hand up and then I'm giving the floor to India. Chris, please go ahead.

CHRIS LEWIS-EVANS: Thank you, Manal. Chris Lewis-Evans for the record. Yes, thank you, Charles. So I think it's worth re-flagging. This is certainly one of the risks that we see is that currently there is no confidentiality for law enforcement requests. So this is something that we will be raising. So, I think it's safe to say currently, we are in very early stages, it's not clear on how the data will be kept.

Sorry, if we could go back one slide briefly. Thank you. So, sorry, just on the slider, there was a part cropped off. So in this slide, it does show that there's thought around having this logging encrypted and obviously treated under proper data protection rules. I see ICANN Org has just raised a hand as well, so Manal, maybe I can leave them to cover how they're envisioning holding the data.

MANAL ISMAIL: Thank you very much, Chris. I see Yuko's hand up, so I'm sorry, Jaideep, if we can just take Yuko, and then I'll give you the floor. Please, Yuko, go ahead. We cannot hear you if you're speaking.

YUKO YOKOYAMA: Hello.

MANAL ISMAIL: Yes, now we can.

YUKO YOKOYAMA: Hi, sorry, I'm in the room. My name is Yuko Yokoyama and I am one of the project members from WHOIS Disclosure System Design Paper ICANN Org. If I may answer Charles questions about logging. So we intend to collect data, and those data will be internally need-to-know basis in terms of who can access that data.

Nonetheless, the data will be collected and if this system was to be implemented, we will be aggregating the data and using that with a discussion with the community in half a year, one year, two-year benchmark to discuss the next step for this system or the SSAD itself. In terms of confidentiality and law enforcements access to the data itself, that is something that we have not discussed as this design paper has been just a system design, and implementation has not been decided. So that is something that we would have to discuss internally as well as with the community if the implementation were to take place. Thank you.

MANAL ISMAIL: Thank you very much, Yuko. India, please. Jaideep, thank you for your patience. Go ahead.

JAIDEEP KUMAR MISHRA: Thank you, Manal. Actually, I'd like to take forward what my Brazilian colleague mentioned, and just an observation on this disclosure system. I think one that expecting -- personally, I feel that the request requesters here, in this case, has to be effective, would essentially need to be necessarily be the law enforcement agencies. Otherwise the registrars, if you give the discretion, if you give them the sort of a choice whether to provide that information or not, is very unlikely that there is going to be there.

So instead of that, I think if we have to keep some element of voluntarily for the registrar, it may be also looked into if the registrant himself would like to volunteer to have the information available at the first instance itself being made available so that there is no such bureaucratic mechanism that one needs to go through and have an option to give that information up front.

Then we are able to focus on only those areas where a person, where a registrant has a view that he does not want this information to be made available in public domain. So for this model to be effective, first, I think it'll work basically with the alias only requesting, because then the registrar would be basically bound by, or at least, so I don't know which countries laws in that case would be applicable, because if a liaison is from say, my country or some other country and the registrar belongs to some other place, what are the chances of him being able to respond and to provide that information back to the requester?

What will be the authenticity of that requester be for a registrar to pass an information off his registrar directly to him on a voluntary basis? Second, I think the point which you also mentioned is that although I understand that all the communication between the registrar and the requesters is outside of the system, but at least if the information is flowing one way for the request that has been channelized to and fro onto the registrar, at least when that information, when that entire exercise has been completed, there could be a reverse fluid to inform at least the WHOIS Disclosure System that this particular process has been completed or concluded, rather than just leaving it completely outside the system. So just these two points. Thank you.

MANAL ISMAIL: Thank you very much, Jaideep. So I'm handing this back to you, Laureen. I already see your hand is up, and please after responding or reacting to Jaideep's comments if we can proceed just noting that we have three minutes left before we start our DNS abuse, but I understand we may run a little bit later, but please go ahead.

LAUREEN KAPIN: [00:27:06 - inaudible] timing.

MANAL ISMAIL: I'm sorry, Laureen, can you speak again? We did not get you well.

LAUREEN KAPIN: Sorry. Just responding briefly to the last comment made by our colleague from India. My understanding regarding the way for this information, even if it occurs outside the system to flow back to the system, my understanding, and that ICANN Org representative in the room can correct me or affirm what I'm saying, my understanding is that there is a way for the registrars to communicate this information so it can be logged.

It's just that the communications themselves fall outside the system, but my understanding is that there then would be a way for the registrar to convey this information back into the system so it could be logged. I think with that, perhaps we should pass the baton over to my colleague Kenneth Merrill to discuss accuracy, the understanding that we probably have to go very quickly over the accuracy issues so we could also then turn to our full program on DNS abuse.

MANAL ISMAIL: Yes, thank you, Laureen. I'm handing the floor now to Kenneth. Please, go ahead.

KENNETH MERRILL: Thank you, Manal. Great. So hello, my name is Kenneth Merrill. I'm the GAC alternate for the United States and the GAC's co representative, along with Melina Stroungi of the European Commission to the Accuracy Scoping Team. I'm going to provide a very brief overview of the work of the Accuracy Scoping Team to date. The team recently released interim report, interim final report, which was sent to the GNSO on September 2nd. An important place to start is by recalling the mission of the scoping team which is not to develop new policy but to assess whether there should be changes to current ICANN policy on registration data accuracy.

With that in mind, I'll delve into the scoping team's work. The scoping team was given four assignments. First, to outline the current contract requirements for domain name registrars regarding accuracy of domain name registration data, and how those requirements are enforced by ICANN. Assignment one tasked the scoping team with outlining how compliance reports on its enforcement of registrar accuracy obligations. The second assignment was to analyze various approaches for measuring domain name registration data accuracy. The scoping team has completed assignment one and is still working through assignment two.

The third assignment, which is yet to begin, will assess whether the current contractual obligations regarding registration data accuracy are effective. Finally, the fourth assignment will assess whether any changes should be made to the contracts to improve domain name registration data accuracy. So the GAC participants in the scoping team have provided regular updates to the GAC, and the GAC has addressed the issue of accuracy as well as the scoping team's work at ICANN72, ICANN73, and in the ICANN74 communiques, all in the issues of importance section. In the interest of time, I think it's worth noting the text at ICANN 72, 73, and 74.

It's all here on this slide, and so I'll just note most recently at ICANN74, the GAC Express concern about-- there was some concern about a proposal to pause the work of the scoping team pending a response from the European Commission regarding whether ICANN has a legitimate purpose to request contracted parties to provide access to registration data for the purposes of measuring accuracy.

Here, the GAC stress the importance of continuing the work of the scoping team, which at the time of the meeting in Hague meant completing assignment one, and for assignment two, continuing the development of a registrar survey. On top of that, the GAC also noted interest in work exploring some additional proposals such as the testing of accuracy checks in a manner that would not be dependent on access to registration data. This has been described as the use of synthetic data to test registrar accuracy checks.

Let's see. Moving forward in the interest of time here. So next slide, please. So, earlier this month, the scoping team finalized its write up on assignments one and two and delivered an interim report to the GNSO on September 2nd. So this report makes three recommendations. First, that the GNSO council requests ICANN Org to carry out a registrar survey. On this, the scoping team met on Saturday and began high level discussion of some of these survey questions.

I also want to recall our questions to the GNSO yesterday that sought clarification as to whether the scoping team might be able to commission a third party to help with survey design as the drafting of these survey questions would be important to ensure that the registrar survey generates useful data. The second recommendation was that further work proceed to explore the option of a registrar audit. This would include the use of synthetic data, perhaps with the help of a third party, to test registrar accuracy checks.

Finally, I know we're over time here, but the final recommendation was that the GNSO Council paused the scoping team's work on only those proposals requiring access to registration data, while encouraging ICANN Org's outreach to the

European Data Protection Board and its completion of data processing agreements and data protection impact assessments. Very quickly, just on next steps as I understand them, the interim report is now in the hands of the GNSO, the scoping team's instructions indicate that any recommendations stemming from the assignments will need to be approved by the GNSO Council before they are directed to the appropriate parties for action.

The GNSO Council is expected to start its consideration of the scoping team's report during its council meeting tomorrow, I believe. Although it's not expected that a decision will be made immediately. Yes, a possible decision on the recommendations could come at a later council meeting. With that, I'll pass it back to Gabe, I believe.

GABRIEL ANDREWS: Hi. Testing the audio again. I don't hear myself. Can you hear me?

MANAL ISMAIL: Yes, we can hear you, Gabe.

GABRIEL ANDREWS: Beautiful. Thank you. If we move to the next slide, please. Awesome. So I'm going to cover this very quickly. There are a set of proposed contractual changes to the base registry agreement and the registrar accreditation agreements. For the most part, these contractual provisions deal with WHOIS, and this is because the technical protocol that's behind the WHOIS requests is changing. For decades, it has been a WHOIS protocol? It's the name, and there's a new protocol that's come out of the IETF called RDAP.

The contracts are being changed to reflect this technical change. That's all well and good. However, alongside these contractual amendments for that purpose, we noticed that there is an additional contractual change that would allow ICANN'S Office of the Chief Technology Officer to use a certain category of data to improve their abuse reporting. This deserved some attention here. It's a topic that we've asked for in the past, and it seems to be happening now, and thus we wanted to call it to attention. ICANN produces monthly abuse reports called DARR, the Domain Abuse Activity Reporting.

Thus far, these reports have been able to link abusive domain names to the top level domains, but not to the registrar level. If they are allowed to use this category of data to analyze the operational stability of the DNS, that enables their DARR reporting to become more accurate, more granular to make links to the registrar level, not just the TLD level, and this helps the entire ecosystem to understand the facts of the heart of DNS abuse.

We view this as a positive development, we're very welcoming towards it, and we note that there is a deadline for comments of October 24th with a proposed timeline for potential dissemination of comment and review. That's it because we have short of time and I want to turn it over to the next folks.

MANAL ISMAIL: So.

GABRIEL ANDREWS: Or was that the last slide? Forgive me if there's no one that's ready. I see Chris's hand up, though, so let's pause.

MANAL ISMAIL: Okay. Chris, please go ahead.

CHRIS LEWIS-EVANS: Yes, thank you, Manal. Chris Lewis-Evans for the record. Gabe, yes, I just want to say that was the last slide, and Manal, I'm happy to hand over to you to move on to the DNS abuse session. Thank you.

MANAL ISMAIL: Thank you very much, everyone. Thanks to Laureen, Chris, Gabriel, and Kenneth, very intense slide deck and a good discussion. Thanks to, everyone. This concludes our discussion on WHOIS Data Protection and Accuracy. Please remain seated, we will get started with DNS abuse shortly. Just give us a minute to switch slide decks. Thank you. We're now ready to go.

Okay. Looks like we are ready to start. So, thank you, everyone. We are now starting the GAC discussion on DNS abuse. This session aims to continue GAC consideration of ICANN Org and ICANN community initiatives to prevent and mitigate DNS abuse.

We will be briefed on relevant developments and continue discussing possible efforts by the GAC to engage with the broader ICANN community to support enhanced contract provisions and possible policy development processes to better mitigate DNS abuse. We will have speakers from the GAC Public Safety Working Group, Gabriel Andrews, US Federal Bureau of Investigation, Laureen Kapin, US Federal Trade Commission and co-chair of the GAC Public Safety Working Group, Chris Lewis-Evans, UK National Crime Agency and also co-chair of GAC Public Safety Working Group, and our colleague, GAC representative of Japan, Nobuhisa Nishigata. I hope I'm getting this close to real.

NOBUHISA NISHIGATA: Actually, it's perfect. Thank you.

MANAL ISMAIL: Okay. Thank you. Ministry of Internal Affairs and Communications. So with this, I'm handing it over to our topic leads. Who will be starting?

LAUREEN KAPIN: I will be starting, Manal. This is Laureen Kapin, and I'm speaking in my capacity as one of the co-chairs of the Public Safety Working group. This is our roadmap. We'll talk a little bit about why DNS abuse is an important topic to the GAC, we'll give you some updates on community activities, we'll hear from our colleague from Japan, we'll discuss ICANN compliances recent audit of 28 registries, we'll talk about improvement of ICANN contract provisions related to DNS abuse and we want to work with the stakeholder community on these efforts, and we'll do a brief review if there's time of GAC positions to date. Next slide, please.

So, DNS abuse as folks will definitely know because it's been a topic that's been discussed over many ICANN meetings. Can we make the slide a little bigger again, Julia? That would be much appreciated. It's important to the GAC for many reasons, and we're going to hear very shortly about some studies about DNS abuse trends. There are many different existing definitions of

DNS abuse, including references to security threats. Thank you. Bless you, Julia.

Like phishing, malware and botnets, that phrasing stems from the GAC Beijing communique, I think that goes back to 2013 and is set forth in the registry contract in terms of obligations that registries have to monitor for such threats. There's also a definition that the consumer trust and consumer choice and competition review team penned as intentionally deceptive, conniving, unsolicited activities that actively make use of the DNS. For a really good reference on community work and GAC views on this topic, you can look at the 2019 GAC statement on DNS abuse, which really focuses on the fact that these illicit activities are a threat to consumers and those who are online using the internet, and a threat to the security, stability and resiliency of DNS infrastructure.

That language sits down very familiar to you because it echos the bylaws which discuss ICANN's core commitments to preserve the security, stability, and resiliency of the DNS infrastructure. In fact, the public safety working group was formed in part because of the need to focus on aspects of ICANN policies that implicate the safety of the public.

DNS abuse has been a part of our work plan from the beginning. It's reflected in our current work plan and the work plan that we're hoping actually to provide for consideration and approval by the GAC for the coming year. So the GAC isn't alone in prioritizing a focus on mitigating DNS abuse. In fact, many ICANN stakeholder groups including the contracted parties, prioritize curbing DNS abuse. There's also a recognition that current ICANN contracts have some room for improvement.

This is reflected in community discussions in board correspondence, particularly the correspondence that is referenced in the link here, the February 12th, 2020 correspondence from the board to the business constituency, and input from several review teams.

Besides the competition, consumer trust, and consumer choice review team, there's also been the SSR2, that's Security, Stability, and Resiliency review team and the WHOIS, the second WHOIS review team, and also discussed in the new gTLD subsequent procedures outcomes. So it's a topic of much concern. I'm going to pass the baton over to my colleague Gabe to discuss some recent trends in the area. Gabe, over to you.

GABRIEL ANDREWS: Yes, ma'am. If we could have next. That's it. That slide. So as we often do when new DNS abuse reporting arises, we wanted to take a moment to touch upon some recently published reports. Now, these are going to be on phishing and malware topics, and they were published by Interisle a few months ago, during and immediately after the last ICANN session.

Now, Interisle is just one of several entities who publish trend reports on DNS abuse issues, alongside other reporting from places like I just mentioned, ICANN's star reporting, and now also, the DNS Abuse Institute is publishing what will be monthly intelligence reports.

They've just started doing that as of this month. The PSWG finds all of these efforts to quantify DNS abuse to be constructive and helpful to these conversations that we have in ICANN. While these next few slides will touch upon Interisle's report, we recognize that with increasing efforts to quantify and report on DNS abuse, this is all a positive development. So the first report here focuses on phishing, which is commonly understood to mean a type of attack in which an attacker will send a message pretending to be from a legitimate entity.

This message usually tries to convince a victim to do something which might advance the criminal scheme. Something like get a victim to reveal sensitive information or to click on a dangerous link, or even to send money to an attacker-controlled account. Now, as the PSWG has previously briefed to the GAC, some of the most prevalent and damaging forms of cybercrime out there, such as ransomware and the business email compromise, both of which I've spoken to the GAC on previously, each of which are responsible for billions of dollars of loss globally each year.

These will often make use of email-based phishing as they're first means of getting the victims on their hook. So you hear phishing, but you can think this is an entryway to a lot of the really bad, dangerous stuff out there. Efforts to prevent or to mitigate DNS abuse, such as phishing, thus are going to help all of us to protect our citizens against these very harmful forms of cybercrime.

Back to this report specifically, Interisle took source data over a one-year period from various domain blacklists, places like the anti-phishing working group, open phish, phish tank, and spam house, and they analyzed them to determine what trends became apparent. They identified more than 1.1 million different phishing attacks from that year of data, and they correlated those to about 154,000 unique phishing domains.

You might be wondering how there could be 1.1 million attacks from only 850,000 domains, and that's a very good thing to wonder because in practice, bad guys might on one hand use many different domains in an attack against a single victim, or on the other hand, a bad guy might host many different victim impersonation sites on a single domain.

So while it would be really, really nice and convenient if you could simply count the number of abusive domains and trust that to represent the scale of abuse that might be occurring, the real world can often be a lot messier than that. Next slide, please. So, within ICANN DNS abuse discussions, there has been an increased focus recently on the issue of maliciously registered versus compromised domains.

That's a way of saying whether domain was used, sorry, a domain that was seen used was registered by the bad guys, or whether it was an innocent party's domain, which the bad guy might somehow have compromised. This could be very important to determine because there might be different best practices for reporting the abuse and responding to those reports depending on how the bad guy got control of the domain in question. If the domain was compromised, for example, a registrar is pretty unlikely to have much useful information about the bad guy.

Whereas if the bad guy registered the domain for their own use, the registrar is quite likely to have lots of potentially useful information, such as payment information, the IP address of the bad guy, potentially even browser cookies, all of which might be used by their abuse teams to link that abusive domain to maybe other domains also registered by the same bad guy for similar abusive purposes, and thereby maybe prevent further harm.

With that in mind, we see that in this Interisle report, they identified that 69% of the phishing domains they observed in this years' worth of data were identified as maliciously registered, meaning it's the bad guy who is registering those domains, as opposed to 31%, which were found to be potentially compromised domains.

Additionally, with those colorful pie charts there, they identify that domains that were registered in new gTLDs appear to be disproportionately used for phishing as opposed to the overall domain ecosystem at large. Next slide. All right. A month apart, Interisle also produced a report on the malware landscape for 2022. Malware is a catchall term for any software that is intentionally malicious.

So some common examples of malware categories that you might have heard before include like banking trojans, which might seek to steal bank credentials from victim computers, or ransomware, which I just mentioned. That's a category that bad guys try to deny victims access to their own data unless they pay a ransom, or keyloggers is another good example where they might try to record every keystroke of an infected machine and then use it for evil later.

The key link here is that it's codes that you probably don't want on your machine as it was written to take advantage of you in some way. For this report, Interisle, again, analyzed reporting from multiple sources, but this time focusing on threat intel providers like malware patrol, malware URLs, Spam House again, and URL house. Some of the general trends that they found were that the number of malware reports were growing year over year, but that not all reports involved domain names.

Interisle found that about 65% of the samples analyzed tended to rely upon IP addresses for communication, and only about 35% tended to rely upon domain names. When they did so, they were seen as in the previously discussed phishing report, disproportionately using that new gTLD space. Key takeaway from the Interisle malware report was noting that mitigating malware requires cooperation and determined efforts by all parties that comprise the naming and addressing and hosting ecosystems exploited by the cyber attackers.

That's just a direct code I was reading from them. This is a point that's often made by the contracted parties here in ICANN as well, and it's something that we agree with that it's indeed important to recognize that some categories of abuse will necessarily involve collaboration between those inside and outside the ICANN community, especially when it comes to hosting and email providers collaborating with registrars and registries. With that, I'm going to flip over to the next slide, and my colleague Chris Lewis-Evans.

CHRIS LEWIS-EVANS: Yes, thank you, Gabe. Chris Lewis-Evans for the record. So as Laureen mentioned at the start, the DNS abuse or mitigation of DNS abuse is of a large interest to a number of parts of the community, and there's been a fair amount of work going on within the community even in the short period since the last one. So, just to highlight some of those bits of work that have been taking place.

So, the first one is discussion paper on malicious versus compromised domains, and as we've shown there, both are important aspects when dealing with DNS abuse on those, and that hopefully will be released by the contracted parties before the end of the year. Also, the registries are working on sharing some statistics on a voluntary basis relating to how they deal with DNS abuse, so how that is evidenced and how they escalate some of those and to deal with their obligation towards monitoring security threats.

Another really useful aspect as I think we've mentioned in the previous session and being able to identify on who to go to when dealing with DNS abuse is the Registry Stakeholder Group have developed an abuse contact identifier tool under assettool.com. This provides contact information and the best place to go to when wanting to report DNS abuse.

Also, in the last ICANN meeting at Hauge, we had a presentation from the DNS Abuse Institute around their Netbeacon tool, which is a centralized reporting tool for DNS abuse that sends your abuse report to the correct point which currently is only for gTLDs, but is really good centralized point. I think, we've already mentioned the benefits for that on the WHOIS side in the previous session.

As Gabe just mentioned there, they are also starting to do monthly reports on DNS abuse trends. I think this as it gains more data, will be a really good extra source to enable us to look at what is happening and be able to look at ways of mitigating or preventing some of this abuse. Go to the next slide, please. Also, in their community, the GNSO have formed a small team beginning of this year, and it's tasked to consider what policy efforts could be considered and to what would be the most effective ways of tackling DNS abuse.

So as part of that, they sent a letter around to all of the community asking some questions around how best to affect that. The GAC provided a response which is linked here along with a number of other communities. The GNSO small team are expected to have some preliminary recommendations fairly shortly. One of those is looking to initiate a very tightly focused PDP on malicious registrations, and from that previous slide or two previous, that shows to be quite a large area of where some of this abuse comes from, but it also is more easily identified than the compromised registrations.

So, probably easier to take more effective action. Certainly, with the malicious registrations, you can take preventative action a lot easier than you can with the compromised side. So I think this will be a good step forward. Also, within the recommendations, they're looking to promote tools to simplify reporting, and certainly, sign up to the DNS Abuse Institute system is certainly a good way forward, and taking reports from them directly or integrating that into systems could be a way forward for that.

Thirdly, looking to recommend to contracted parties to consider some of the interpretations within the contracts and ICANN compliance's role in upholding those to actually how they deal with abuse and how the investigation part looks and it can be acted upon. Then with that, we go onto the next slide and pass onto Laureen. Thank you.

GABRIEL ANDREWS: Yes, this is actually me, I think.

LAUREEN KAPIN: Yes, I think it's for Gabe.

GABRIEL ANDREWS: So I'm going to cover this topic very quickly in the interest of time. One of the great community contributors out there is the Security and Stability Advisory Committee, interest full disclosure here. They were recently soliciting for law enforcement input, and I have joined as a prospective member. I will nonetheless continue to say wonderful things about them in the hopes that they might buy me a beer.

So they are a collection of engineers and security experts that focus on the technical security and integrity of the Internet's names and addresses. They have a mantra where their writing speaks for itself, and thankfully, in the interest of time, I can really focus hard on that. Go ahead and hit the next slide, please. There are two reports in particular that we wanted to call out as being of high relevance to the DNS abuse conversation.

The first was SAC114. I note that within that, there were recommendations on prior to the round, the next round of gTLDs that ICANN commission a study as to the causes and responses to, and best practices for mitigation of domain name abuse that proliferated in the first round of new gTLDs, the 2012 round, and that any such best practice is being incorporated into "enforced requirements." That's something that is relevant to ongoing discussions.

Next slide. Similarly, SAC115 created a framework for what they called an interoperable approach to addressing abuse handling in the DNS. There were a lot of really valuable contributions that exist within this document. I will note that this document first put forth the idea about a common abuse response facilitator. This was published prior to the eventual launching of the DNS Abuse Institute's Netbeacon tool, which is the closest analog to what I've seen suggested within SAC115. It's not a perfect mirror, but it is a strong step forwards.

We are, I guess, given the positive developments that we already see occurring both by DNS Abuse Institute, by community efforts of the ACID tool that Chris Lewis-Evans just spoke to, we find there's reason to be hopeful that issues such as those identified in SAC115 will continue to be worked on by the community. Go ahead and go to the next slide.

LAUREEN KAPIN: I think this is me. This is Laureen Kapin again. There was a recent presentation by SSAC to the GNSO Council with a very interesting proposal to create a cross community roadmap for mitigating DNS abuse which I think could be a very positive development. The SSAC's proposal includes these components on the slide, explore aspects of mitigating DNS abuse, and that includes proactive prevention, detection, information sharing, et cetera, and to create a consistent consensus baseline to measure results to ensure that that baseline is met and maintained over a long term.

So that would create a floor beyond which we don't want to fall in dealing with DNS abuse mitigation, and then develop and communicate a set of processes and expectations for the anti-abuse community. Then finally, to give this some specificity, to create a work plan with timeline and participants from the community to meet these goals.

So I think that this is a very interesting and useful proposal from the SSAC, and involves the entire community, which is going to be a theme of some of the efforts which we ourselves within the public safety working group would like to embark on. We'll talk a little bit more about that later on in the presentation. For now, I would like to pass baton over to my colleague from Japan, Nobu who also has some important topics to share with the GAC. Over to you, Nobu.

MANAL ISMAIL: So it looks like there's a problem with the mic.

NOBUHISA NISHIGATA: Let me.

MANAL ISMAIL: Okay, now we can hear.

NOBUHISA NISHIGATA: All right.

MANAL ISMAIL: Please, go ahead.

NOBUHISA NISHIGATA: Okay. Thank you very much, Laureen, and thank you very much for the opportunity to present today. This is Nobu from Japan, for the record. Today I will share the Japan's experience related to DNS abuse. In fact, Japan became actively engaged in this discussion since ICANN70. This primary reason is to respond the holistic or whole of the government action plan against Manga piracy in Japan. It's a huge issue, but what I'm talking today is about the contract between ICANN and the registrars, which is 100% under the ICANN's remit.

It is unfortunate to see that the registrars playing some role to allow to continue piracies, and Japan is asking for the remedy, or even your help detail would be later on to explain. Moving to the chart below, thanks to the registries stakeholder group. This chart is from the capacity building session with them. It reiterates the relationship among the parties, and I put the square to highlight-- could you click again, one click so that you can see the square, I mean for the next slide? Yes. Thank you very much.

At the square, the highlight here to show the contract between ICANN and the registries or registrars. These contracts are what I'm talking today. Recalling the discussion at the previous ICANN74, we discussed possible improvement in the enforcement of contract terms or contract between ICANN and the registries and registrars with respect to DNS abuse. This is what Japan like ICANN to go further.

Again, I'm not getting into anything about the contents. The focus of the discussion is contract between them and its enforcement. The next slide, please. Before diving into the detail, let me present a quick overview of the structure of the Manga piracies. Please know that this is much simplified for illustration but there is a bad guy at the bottom right distributing the EDR copies of Manga. It acquires a domain from the registrar on top, and it borrows servers to upload, and the illegal copies are distributed through CDNs.

These copies are provided for free, or in some cases, very small amount of money for subscription. The bad guy is making a lot of money through the advertisement, and that shows up in the piracy sites. Again, I put the shade-- could you click the deck so that we can see the shade. Thank you. I put the shade in the left to highlight what we discuss here. It is not about the Manga, not about the technologies. It is about registrar and the registrants with the bad guys. We don't blame the technologies, we benefit a lot from this tech, and it is human issue.

Human is always behind the bad use of the technology, and we as humans have to solve the problem. So next slide, please. Now, let's dive into the detail. This slide illustrates what I said in the beginning, the possible improvement of contract terms and its enforcement. I put the provision of the RAA 3.18 on top part of the contract between ICANN registrars. It says that the registrars have to provide conduct point for abuse report, including reports of illegal activities. Most of the registrars do this appropriately, properly from our observation in Japan.

The contract also says that the registrar has to take reasonable and prompt steps to investigate and respond appropriately to the report. Once the registrar receives the report, most of the registrar take actions, again, from our observation, yes, there are the handful people who patrol the internet every day to identify the bad guys and they send reports. Then, the registrant, the bad guy knows that he or she is being detected. What happens next, huh? It helps around the internet to avoid the detections.

The registrants acquire a new domain from the same registrar to continue the piracies. This is what we call domain hopping. That slide, you can see that the chart in yellow, that slide highlights two points in yellow that we should discuss further. The first one is in the left that there is no clear description in the contract what is reasonable, and the prompt steps to investigate and respond appropriately.

The text in the contract is not explicit, and this point is pointed out during the capacity building session with the Registrar Stakeholder Group, and also pointed out by the panelist yesterday in the session with the GNSO. The second point is that the bad guy, the piracy people gets a new domain from the same registrars.

The registrar should know that this second application is coming from the bad guy, it is already reported. So we heard from registrars that it is not easy for them to take down the bad guy immediately, from their perspective, but I'm telling you that the rights holder in Japan, or creators in Japan and publishers are very much frustrated by this. How the registrar makes the new contract with the reported bad guy, that's the point.

So these are the points that Japan proposed to get to dig into further. This is about the contract between ICANN and the registrars, and we do believe that there is a room for ICANN to play a role. This is the end of the presentation. We are happy to hear your comment, observation, or ideas on how we proceed the discussion further. Thank you very, very much.

MANAL ISMAIL: Thank you very much, Japan. Laureen we have here a hand up, so if we can take a couple of questions, hope it's okay. I see Trinidad and Tobago. Please, go ahead. So we have a problem with the mic here. Yes, if you can change. Maybe the first roll. This one is working.

UNKNOWN SPEAKER: We're sorry, Manal. It seems like all the energy's been directed to the next room.

KAREL DOUGLAS: Yes. It seems like there's a good --

MANAL ISMAIL: It's okay.

KAREL DOUGLAS: Musical chairs. Good morning, everybody. Karel Douglas from Trinidad and Tobago, and I apologize for the movements, and the music does sound good next door. So maybe we could wrap up in time to enjoy it. I just wanted to thank Japan for a very interesting presentation. I think he struggles two issues, the question of DNS abuse and piracy. The question is, what I have is whether or not DNS abuse includes piracy.

I say that in the context that what he seems or what appears to be the issue here is copyright issues. In law, we understand that copyright tends to be a private right, and not a regulatory rate where the ICANN institution would seek redress or the registrars would seek redress from ICANN as the case may be.

What tends to happen when it comes to piracy is that the rights holder or the owner of the right would seek to have some relief either through the law or, well, that could include the courts, the law being maybe police as the case may be, a prosecution type of action, or would seek some kind of private redress in the courts as I did indicate. That could include a notice and procedure.

So without getting too long-winded, it's whether or not this is really fit as DNS abuse or whether it's really more of a private right action where somebody who has found that their copyright is being exploited would prefer to take or should rightly take that action through the courts or through the prosecutorial approach being the police.

So I'm not too sure, I think that maybe the question he is asking, whether or not we should include piracy and these other forms of "abuse" as part of DNS abuse, which we understand from the presentation seems to be more of a technical nature, malware, phishing, and so forth. So thank you very much for your time.

MANAL ISMAIL: Thank you very much, Karel. So Japan, would you like to respond, please? Go ahead.

NOBUHISA NISHIGATA: There we go. Thank you very much for the question, and happy to answer. The first one, the definition of DNS abuse in my understanding is very vague. If you define DNS abuse in a narrow way, then the piracy is out of the definition, even though it is [01:16:26 - inaudible] activities.

So then the second point of your question, and the answer is that whether it is in the DNS abuse coverage, whether my presentation is or not, my answer is going to be yes, because the core issue is that some behavior of the registrars compared to the [01:16:50 - inaudible] provided in the contract.

Like they have to take the reasonable and et cetera, and action. Even not only the DNS abuse, but also the [01:17:02 - inaudible] activities, which is including in the copy that infringement. The third point, answering your question about the copyright or other right issues, just let me introduce some of our efforts against these bad guys. Just as I said in the beginning, it is the holistic efforts.

So I'm just taking apart, joining the forces of the whole team and the government, in other word, that we have the police people going to the [01:17:31 - inaudible] trying to catch abroad or like we have the patent office to do things and some industry part of the ministries working harder to provide the other majors or remedies or sometimes even try to change, provide a new platform rather than the piracy to enhance the margaritas outside Japan. We can discuss and only on the contract issue here, and then this is not our wish that the ICANN or the GAC or PSWG is going to expand our wing. Thank you.

MANAL ISMAIL: Thank you, Japan. I have --

LAUREEN KAPIN: That's a great step -- Oh.

MANAL ISMAIL: Sorry, Laureen. Go ahead.

LAUREEN KAPIN: Oh, do we have more questions? I was thinking that was a good segue to continuing with the presentation, but I'm happy to-

MANAL ISMAIL: Yes, we have three hands up in Zoom, and I would ask everyone to please try to keep it short so that we can finish the rest of the slides. So I have Indonesia, India, and, US. Ashwin, please. Indonesia, go ahead. Oh, if you can try another mic, Ashwin, please.

ASHWIN SASONGKO SASTROSUBROTO: Okay. Thank you. Well, not only in cyberspace, we have a problem in physical space, we also have a sound problem. Yes, I already want to get the opinion of Gabriel, it's very interesting presentations. What I want to get his opinion is whether it is possible, for example, for ICANN to define the DNS abuse in the bylaws and or accepted request for comment RFCs, which is more or less like a standard.

So we have the definition, then the definition can be adopted in local regulations, just like say from ISO and IC standards, which are then adopted in local regulations. Because it will be important if we bring a case to court since we can say that this criminal act against this regulation and so on. Thank you.

MANAL ISMAIL: Thank you Ashwin. Would you like to respond directly? Please, go ahead.

GABRIEL ANDREWS: I'll respond very briefly but directly, and this goes back to the capacity building workshop presentation I gave where I had on a slide, multiple different definitions of DNS abuse and noted that thus far in the ICANN multi-stakeholder community, there hasn't been presented to my knowledge a definition which the full community has come behind. While I can't speak for ICANN, it's my understanding that there sort of needs to be that sort of consensus that's developed within our community before we're able to get as far as what you would suggest. I think I'm going to leave it there.

MANAL ISMAIL: Thank you very much, Gabe. India, Santhosh, please, I'll appreciate keeping it brief.

THAMPY SANTHOSH: Thank you, the presentation made by the colleague from Japan and also the members from the PSWG. So the issue boils down to the malicious domain, who provides the malicious domain? Can't we have a system in place? So the colleague, Gabriel, has mentioned about that, which is part of the IGTF standard, but while filling the fields in the WHO IS, can a standard we maintain say suppose a person who enters only xyz, he has been provided a domain, so that should be stopped. So as Gabriel has mentioned about the very statistics, the point, again, boils down to the malicious domain.

So in India, under .in, that is the country code top level domain of India, we have started the e-KYC, which means Know Your Customer. So we get the information of the person who wants to register a domain. So that information we are taking it, but yes, privacy is guarantee., So that is how we are minimizing the DNS abuse. So this is a global issue, so we need to take it further so that one should know the customer who wants a domain in order to stop the e-KYC. Also, the point mentioned by the Japan colleague mentioning the improvement of RAA contract, which is a high time, it is of 2013, which has to be improved. Thank you.

MANAL ISMAIL: Thank you very much, Santhosh. I'm giving the floor next to US, please. Susan, go ahead.

SUSAN ANTHONY: Just wanted to say thank you to our colleagues for this presentation. DNS abuse is a matter of priority for the United States as it is for many governments in the GAC, and ICAN is a venue where the community can address malware, botnets, and other forms of technical DNS abuse. Drawing back to earlier in the presentation, different parts of the ICANN community seem to be moving in a positive direction towards possible solutions.

Of course, there is much work that remains to be done, but we strongly support the prospect of a policy development process by the GNSO on mitigation of DNS abuse. We found the discussion today, in addition on contract provisions, to be very useful. Perhaps at our next meeting in Cancun, we can also allow for more time for GAC discussion on this topic. Thank you.

MANAL ISMAIL: Thank you very much, US. I'm handing back the floor to topic leads, Velimira, is this really short? Please, go ahead. I'm sorry.

VELIMIRA NEMIGUENTCHEVA GRAU: Thank you. Oops. Yes, thank you, Manal. I'll try to be short. I was typing in the chat, but had one observation. I just wanted to mention that in the European Commission, we have worked also a lot in terms of what could be done, because for us, DNS abuse is also a priority. In terms of the question on definition, we have found out there're very different definition out there, and we think that while definition is indeed important for a number of reasons, it should not be the end in itself.

It seems to me that what our colleagues have presented shows well, that there are a number of points in which we could advance without necessarily having a definition, which might be a very difficult under the multi stakeholder model that we all support, but under precisely the fact that indeed it's very difficult to find what is currently such a common definition. So I think that this domination colleague, this improvement in which I understand our registry and registrars colleagues are working, and on which you would like to reflect and to see what could be our input in their reflection might be a good way forward.

Then in relation to the remark and the useful proposal of our US colleague, I have to observe however that given the final results of the different policy development processes, it would be very difficult for us to think that this is a timely and effective solution forward to this stage. We could definitely look into this cross community that was proposed by our SSAC colleagues. Thank you, Manal, and sorry for the time.

MANAL ISMAIL: Thank you very much, Velimira. So with that, yes, I think we need a longer discussion, of course, but I'm handing this over to you back, Laureen sorry. We have three minutes, so I hope we can cover the remaining slides. Very sorry to squeeze you.

LAUREEN KAPIN: Sorry about that. Yes, I will try and wrap this up and apologize that we're not having an opportunity to cover all we might have wished. I do want to thank everyone for their contributions. I think the presentation from Japan and the interventions from our GAC colleagues all underscore that there is no one definition of DNS abuse and there is no one path to resolving how we can best mitigate. I'm going to ask to go to the next slide. I will point out very briefly the crucial role that ICANN Compliance plays in this effort.

Besides responding to complaints, they also engage in audit activities to make sure that the registries and registrars are living up to their obligations under the contracts. I commend to you to take a close look at the results of the compliance audit of registries recently released. I won't have time to go over what I might have wished. Next slide, please. Next slide, please. What I want to highlight in addition to possibly targeted PDPs and more cross community discussions, there's also a role for ICANN to play and the community to play.

ICANN, of course, is a not-for-profit public benefit corporation, and their mission is to ensure the stability and secure operation of the Internet's unique identifiers, and their party to the contracts. They can negotiate and enter into these agreements, including public interest commitments, and they also have an obligation to take into account the public policy advice of governments and other public authorities committee. Next slide, please. What I really want to highlight as we close, it's midnight for me, but lunchtime for you, is that there are places in the contracts that have room for improvement.

Japan touched on it in particular, the registrar's obligation to promptly investigate and respond appropriately to any reports of abuse. The ICANN board has noted that the RAA doesn't define with any specificity what that means, but the community can come together and talk about what that means. The public safety working group intends to continue discussions and launch discussions with contracted parties, with the other stakeholder groups to find where there's common ground on these issues.

We know that we are not party to these contracts, but we all know that we can engage in constructive discussions across the community to find common ground and ideally come up with some suggestions to present to ICANN for consideration because they're party to these contracts with the contracted parties. By the way, contracted parties can do this too. So we really would love to have these discussions, and that is the message that I want to leave you with, that this is a collaborative effort that we intend to pursue.

Next slide, please. I just want to let you know that in the slides, that we didn't have a chance to go over in the depth that we would all have liked. We talk about incentives to encourage good behavior. Next slide. We also talk about possibly identifying triggers for ICANN Compliance to take action, that if abuse rises to a certain level, that ICANN Compliance would step in and intervene as part of its compliance function. I think that is where we'll likely need to wrap it up for now. Is there a next slide?

There may not be. This may be the end of the next slides. I will just let you know, summarize GAC positions. So if you want a great crib sheet on past GAC advice and input on DNS abuse, you can look at these slides at your leisure when it's not standing between you and lunchtime and see what the GAC has discussed on these issues. I really want to thank everyone for their attention, and this really underscores for us as folks who are giving presentations, that more time needs to be spent on these issues so we can continue to have these really good exchanges. So many thanks to everyone and my colleagues for their presentations.

MANAL ISMAIL: Thank you very much, Laureen. Indeed, needs more discussion, collaborative efforts, but I would like to thank you very much, Laureen, Gabe, Chris, and Nobu, very good discussion, and thanks to the other colleagues for their active participation. It's now time for a 70-minute lunch break. Please be back at 13:15

Kuala Lumpur time, 2:15 UTC for our bilateral with the ccNSO. Thank you very much, everyone.

[END OF TRANSCRIPTION]