
ICANN70 | Virtual Community Forum – GAC Discussion on DNS Abuse Mitigation (1 of 3)
Tuesday, March 23, 2021 - 09:00 to 10:00 EST

JULIA CHARVOLEN: Good morning, good afternoon and good evening. Welcome to this ICANN70 GAC session on Tuesday, 23rd of March. Recognizing that these are public sessions and other members of the ICANN community may be in attendance, the GAC leadership encourage all of you GAC representatives to type your name and affiliation in the participation chat pod to keep accurate attendance records. If you would like to ask a question or make a comment please type in the chat, the feature is located at the bottom of your Zoom window, by starting and ending your sentence with a <QUESTION> or <COMMENT> as indicated in the chat.

Interpretation for GAC sessions include all 6 U.N. languages and Portuguese. Participants may select the language they wish to speak or listen to by clicking on the interpretation icon located on the Zoom toolbar. If you wish to speak, please raise your hand. Once the session facilitator calls upon you, unmute yourself and take the floor. Remember to state your language you will speak, in case you will be speaking a language other than English. Speak clearly and at a reasonable pace to allow for accurate

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

interpretation, and please make sure to mute all other devices whether speaking.

Finally, this session, like all other ICANN activities, is governed by the ICANN Expected Standards of Behavior. In the case of a disruption during the session, our Technical Support Team will mute all participants. The session is being recorded, and all materials will be available on the ICANN70 meetings page. With that, I would like to turn it over to the GAC chair, Manal Ismail. Manal, over to you.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Julia, and good morning, good afternoon, and good evening everyone. Welcome to the first of two sessions on DNS abuse mitigation scheduled at 9:00 Cancun time for an hour. The GAC will consider recent ICANN developments, including the conclusion of the SSR2 review and that of the subsequent procedures PDP to determine next steps in ensuring appropriate measures are taken to prevent and mitigate DNS abuse in gTLD, to include consideration of complete proposals through contract of provisions where we will receive a presentation from our Japanese colleagues. With this, allow me to hand over to our topic leads today. We have Laureen Kapin, US

Federal Trade Commission and co-chair of the GAC Public Safety Working Group, and Chris Lewis-Evans, UK National Crime Agency and co-chair of the GAC Public Safety Working Group, and Gabriel Andrews, US Federal Bureau of Investigation. Without any further ado, allow me to hand over to Laureen. I expect you will be starting?

LAUREEN KAPIN: Actually, Chris and Gabe will be starting; I will be ending.

MANAL ISMAIL, GAC CHAIR: Okay, I thought the names listed in the order of presentation, sorry.

LAUREEN KAPIN: No worries, we tricked everyone.

MANAL ISMAIL, GAC CHAIR: Over to you, Chris.

CHRIS LEWIS-EVANS: Thank you, Manal, and hello everyone, good afternoon, good morning, good evening. As Manal has kindly detailed there, we're

going to cover a number of items today in the first of our DNS abuse sessions. We have an hour but as always, a lot to cover. We will take questions after the first section on SSR2 but mindful to get onto the DNS abuse section, we will try ask keep that limited and if necessary, I believe we have a [indiscernible] update session after this so may carry DNS abuse questions over into that section.

So the SSR2 review has taken place and I think it has some key messages in there covering DNS abuse which is why we wanted to really put these two sessions together. So as always, we like to highlight some of the key sessions within the DNS abuse that are occurring during ICANN70, listed there. As I say, we have a second session on DNS abuse with you on Wednesday, so tomorrow, and during that we will also be covering an area that I know we have had a large amount of interest from the GAC, and I think specifically Russia have asked a number of times about an update on that so I think that is a key deliverable that we have been pushed for. And as part of the ICANN 69, I think the PSWG were tasked with coming up with concrete proposals, which hopefully we will get to before the end of this session. And I will hand it over to Gabriel Andrews to cover some of the SSR2 recommendations and how they impact Public Safety and DNS abuse.

GABRIEL ANDREWS: Next slide, please. So starting from a high level, this is going to be a review of recommendations that were put forth by the second security stability and resiliency team, which we shorthand as SSR2 and their final report. For background, because of ICANN's bylaws which require that at least every five years a review is conducted of their execution, their commitment to that SSR2, stability, reliability, resilience, security and intraoperability of the Internet systems that ICANN administers, this report is that review. The SSR2 included [indiscernible] Kerry-Ann and her colleagues and her colleagues have made themselves available here today to answer questions. And we will turn to them after I give a summary, with the most direct impact on our ongoing DNS abuse conversations.

This report is both thorough and detailed and while worth noting full consensus was achieved on all of their 63 recommendations, this will be a high-level overview only, again, focusing on the DNS abuse recommendations. So I won't be speaking to every point on every slide, and I have paraphrased liberally from the SSR2 report in the interest of brevity.

The SSR2 team first noted in the recommendation, one, that their

prior team of SSR1 had put forth recommendations of their own and all remained relevant and none fully implemented. Attributed to that the recommendations themselves may not have been specifically measurable and recommend a review of all the SSR1 implementations and throughout their report further stressed measurability in each of the recommendations they put forward in the SSR2 report, measurability a consistent theme. Recommendation 2 is quite notable in that it seeks the creation of a corporate level, otherwise known as a c suite within ICANN. This would suggest combining roles and responsibilities which currently exist within both ICANN's office of the chief technology officer and within the chief information officer. Recommendations 3-7 proceed to give specific obligations that this new role would be responsible for. Those obligations would include security, stability, resiliency, budget transparency, risk management processes, meeting industry standards. Vulnerability disclosure programs and risk management, including business continuity and disaster recovery.

Recommendations 8-15 have the most relevant impact on our ongoing community discussions on DNS abuse. Some of these worth noting, numbers 8 and 14 in particular also likely to be the most contentious within the broader ICANN community. In

drafting number 8, one of the contentious ones, the SSR2 report identified past instances in which ICANN community guidance was later not incorporated within the contracts produced at the closed door sessions between the ICANN and contracted parties. SSR2 cited an example of this in a 2009 memorandum that was entitled mitigating malicious conduct.

They wrote: Unfortunately, there was a gap between the measures outlined in the memorandum and what emerged from the closed negotiations between ICANN org and the registries. SSR2 proposes in recommendation 8 that ICANN org commissions abuse and security experts to represent the interests of non-contracted entities in its future negotiations with the contracted parties with the goal of improving security, stability, and resiliency of the DNS for its users, businesses, and governments. Anything touching on contracts we expect would be somewhat contentious, but I think an important recommendation to consider.

SSR2 report on this page 34 noted that during April 2018 dialogue with the SSR2 review team, ICANN's contractual compliance -- contractual compliance asserted that the current contract do not authorize ICANN org to require registries to suspend or delete

potentially abusive domain names and thus ineffective in allowing them to pursue those in engaging in systemic DNS abuse. Because recommendation 9 turns to contractual compliance, asking the Board to direct ICANN to strictly enforce contracted parties adherence to the contractual security, stability and resiliency obligations to monitor and enforce registration data accuracy, to have external audits conducted against ICANN org's compliance team to ensure meeting their mission and finally, to task the team with publishing regular reports that will list the tools the team feels they don't have but which might be useful in order for them to address their mission of addressing threats in the DNS, including any tools that would require changes to the contracts.

Those of us who have engaged in previous ICANN meetings in recent, last couple of years, may have noticed that community conversations on DNS abuse have become somewhat derailed on occasion over contention about what it actually means and thus we see in this recommendation 10 there is a recommendation for ICANN to provide clarity on the definitions of abuse-related terms. And then to have ICANN org put those terms on a centralized web page that ICANN org would create and maintain and to clearly denote which abuse categories ICANN org sees within its

[indiscernible] or those it sees outside its -- and [reading] [refer to slide] and then to make a consistent use of these terms in all of ICANN's published documents whether the contracts, review team implementation plans or other such activities and to have all of those uses to reference the Web page that was created for this purpose.

Now, I think this is a noble effort and having a clear set upon list of terms that we all use the same way would perhaps really help us avoid the instances of speaking past each other in these DNS abuse conversations.

I will skip 11 and focus more on 12, quite relevant to the anti-abuse discussions. Twelve includes four provisions that seek to improve DNS abuse reporting. Functionally these are seeking improvements to DAAR, domain abuse activity reporting. And 12.1 would task ICANN org with creating a DNS abuse analysis team, which has no conflicts of interest with this. And these would be tasked with overhauling the DNS abuse reporting and prioritizing that the data be actionable, that there is data validation, transparency of the reporting and independent reproducibility of any analyses conducted. Then to improve contracts with those commercial services that provide the data

that goes into DAAR to allow that to be shared for non-commercial use, this is something that doesn't currently exist with many of the contracts for these data feeds and there is good reason for this, the data is itself commercially valuable, so there is nuance that could go into the contract negotiations to allow the data to be shared, to allow independent security researchers to conduct their own research analyses and suggests that ICANN publish the contracts publicly and terminate any contracts that don't enable data sharing.

It goes on to have ICANN publish reports that identify the registries and registrars whose domains most contribute to abuse. Different than any prior to DAAR reporting. This would give us better insight to those that have more than their fair share of abuse activity. I would say there are needs to have that granular level of review and ICANN should publish reports that identify registrars and registries in response -- this is something I have seen, registrars and registries put forth themselves that they would like to publicize the efforts they are taking, somewhat aligns with other conversations.

It is clearly important to have a shared set of facts when we speak about what is actually happening in terms of DNS abuse, so these

suggestions are thus very important to consider. I anticipate that the Public Safety Working Group will offer some comments which may support these recommendations or in some cases go even further when it comes to improving the abuse reporting.

Next slide, please. Recommendation 13, will seek to have ICANN org create a centralized DNS abuse complaint portal. This portal would automatically direct all abuse reports to the relevant parties. Meaning if you are a complainant and bringing a complaint of abuse, you don't have to do the research on your own to know which registrar or registry is associated with a domain. You can submit complaint of abuse and the portal would route it. [reading] use of this referral system would be made mandatory for all gTLDs and voluntary for ccTLDs. It noted this recommendation would reasonably be expected to take several years to be implemented after approval.

This is the last of the deep dive into the recommendations here. Noting along with recommendation 8, these recommendations 14 and 15 likely going to be the most contentious within the community. Fourteen calls for the creation of a temp spec for what they call evidence based security improvements, this is a temp spec that will be recommended to require contracted

parties keep their percentage of abusive demands below a certain threshold and to have ICANN track that and notify the contracted parties if the domains' portfolio have been identified as abusive. To put contracted parties on notice if they exceed the established threshold, to put a clock on those contract the parties to improve or face consequences, and finally, to offer financial incentives for achieving a very low percentage of abusive domains within their portfolios. Thus 14 while likely to be contentious, it nonetheless contains a recommendation for financial incentives for registrar or registry to do an especially good job in their anti abuse efforts without specifying how those results achieved and while I think there will be a lot of contention in these provisions and caution us to tread lightly, I think there is still room to find constructive areas of collaboration.

Recommendation 15 would be to launch an effort to create evidence based security improvements, and that is something proposed that would follow the temp spec and be tasked with defining counter measures for different types of abuse, time frames for contracted party actions, contractual compliance actions in the case of policy violations and so forth. This would insist that ICANN terminate contracts in the case of quote, pattern and practice, end quote, of harboring abuse. Two big asks, 14 and

15, and calling them out for awareness.

Now, that is the end of the deep dive into recommendations with specific DNS abuse applicability, but in the interest of completeness, worth noting recommendations 16-24 engineering and standards focused and while we don't see these as having direct such safety implications, they aim to improve the stability of the DNS and the GAC benefit from future comments put forward by the SSAC, security and stability advisory committee.

This is my last slide here, and the final comment we wanted to highlight there are already both some comments put forth by the registry stakeholder group and pir, seeks to [indiscernible] abuse and security experts in those contract negotiations, they have also objected to 14, seeking to create the temp spec. That said, the registry stakeholder group did have a rather nuanced position on a lot of these put forward.

As we conclude, I would like now to turn to our colleague, Kerry-Ann and invite her and her colleagues to comment as SSR2 authors to either clarify the intent behind any of the recommendations that I covered here or perhaps to highlight any

other recommendations that I may have only lightly touched upon or glossed over that they feel are worthy of specific GAC consideration. I invite her now to take the mic and assist.

KERRY-ANN BARRETT: Thank you so much. This is Kerry-Ann Barrett, for the record, thank you for such a comprehensive overview. I will hand it over to Russ Housley as the chair of SSR2 just to probably bring to bear some of the more -- in addition to the ones you have highlighted which did outline much of our discussions as a team, I will hand it over to Russ first to take the floor. Thank you.

RUSS HOUSLEY: Hi, can you hear me? This is Russ Housley, okay. So one of the things that summary did not include was overlap between the SSR2 recommendations and those of previous review teams. We highlighted in our findings where that overlap takes place but we purposely included the things that overlap because we thought it was making a stronger statement. If more than one review team thought that a particular thing ought to move forward, that instead of just saying well, they said it, we don't need to say it, we felt it was better to say this is important to say from a CCT perspective and from an SSR2 perspective was a stronger

statement than just not saying anything. So for that reason, we do include things that were said by previous review teams, basically to encourage that those are really, really important things from more than one perspective.

But I think maybe we can answer questions from the GAC community. There are four of us who are implementation shepherds, myself, Kerry, Laurin, and KC, and we are on the call.

KERRY-ANN BARRETT: Thank you, Russ, I will probably hand it back over to Andrew. I think it will be useful if members have questions and any area that provide clarification at this stage. Another aspect we could probably give in terms of our logic, in doing the review, the team took a lot of time thinking about institutionalizing the recommendations, very long-term haul, not just fixing short term gaps but thinking about what are some of the institutional things put in place that would allow long term benefit of the stability and security of the Internet. And I will hand it over to Andrew and to the GAC members for questions.

GABRIEL ANDREWS: I am not entirely sure how to be aware of which questions are in the queue, if anyone. May I ask for support staff's assistance for identifying and responding to questions.

CHRIS LEWIS-EVANS: Yes, thank you, Gabe, for that overview. Manal, should I hand it over to you for the queue?

MANAL ISMAIL, GAC CHAIR: As you wish, I already see Kavouss' hand up. Let's give him the floor, and happy to have you moderate the queue if you wish, Chris.

CHRIS LEWIS-EVANS: Kavouss, over to you.

IRAN: First of all, thank you very much for the very useful presentation which in fact I did not expect to be so useful. And thanks for all the work you have done. I have some questions in the role of clarification. Many of the recommendations are intended to help to mitigate or resolve, to some extent, the problem of DNS abuse.

Something that I have not seen, perhaps I have not read the recommendation, the time frame for the implementation of this recommendation. And the second is the implementation itself but most importantly is to oversight the implementation to identify whether they are going in the right direction as it was intended. And possibly, I say possibly, have some sort of kpi for the implementation.

So it is a very long process depending on the time of implementation and depending the way that this implementation oversight, whether we need to come back for the sort of trial and effort to review that, perhaps having some rules for the revisions if we don't want totally to change that, and in what area we go back to the community to ask additional views on that. I'm sorry, the questions were very, very general. Some answers may have already been given in the SSR2, but I would be very happy if some answer would be given to the question, in particular for the implementation aspects. Thank you.

GABRIEL ANDREWS: All right, I will quickly state that the lack of focus in this presentation and review on implementation I will take responsible for, because the SSR2 report actually I felt did a very

good job of calling out for any recommendation they put forward exactly when it could be considered implemented, and I thought that was very helpful but I will invite the other authors, shepherds to further answer your question, Kavouss.

RUSS HOUSLEY:

Hi, this is Russ. So the next -- the current step we're in is the report has been delivered to the Board. The Board asking for public comment. They will then review the report in light of the public comments they receive and decide which recommendations will be implemented, and then ICANN staff will put together an implementation plan for the ones that the board has approved for implementation.

The shepherds from the review team, the four of us on this call, are available to the Board and the staff throughout that process to make sure that any miscommunication or lack of tightness in the language is resolved. But we tried very hard to provide in the report an indication of, one, what successful implementation looked like without saying exactly do this, do that, do this other thing, because we wanted the community and the staff to have some say in how those things that are laid out in these recommendations are achieved. I hope that was helpful and

answered your question.

KERRY-ANN BARRETT: And Kavouss, another thing that the recommendations did, at each recommendation where it touches on another recommendation or related, we took careful time to ensure that all related recommendations we tried to cross reference them so at least there is some mapping of which ones would impact the other or which are related and could be implemented together, another way to ensure what measuring success looks like for the position we want it to be generally is done.

GABRIEL ANDREWS: Thank you. Chris, how are we on time?

CHRIS LEWIS-EVANS: We have a question from Nigel Hickson from the UK first, if that's okay. And Russ or Kerry Ann, this may be one for us. It says good afternoon, and thanks, could I ask and apologize if missed, if the SSR2 team will host a webinar this week to the whole community on these important recommendations? And I know and Fabien linked in the chat there was a webinar prior to ICANN70, I just wonder, Russ, whether you will hold another either during or after

ICANN70.

RUSS HOUSLEY: We thought doing one in advance would help people prepare their public comments and responses. And so we are not planning to make a presentation this week. If it is useful, we can make sure that you have the slides from the previous one.

CHRIS LEWIS-EVANS: Thank you, Russ, I think Fabien has shared those in the chat. So Jorge has asked a question: [reading] how do the SSR2 recommendations relate to the CCT rt recommendations and has consistently been looked after?

KERRY-ANN BARRETT: For that question, I would probably ask Casey, if you are available to take that question?

KC CLAFFY: Yes, KC, a member of the SSR2 team. Yes, in general, I think Russ sort of answered this earlier, we felt that all of our -- not all to the extent that recommendations touched on the CCT recommendations, they were consistent with the CCT

recommendations. In some cases we spelled that out but not all, so the overlap was intended to reinforce the recommendations of other teams where it existed. Does that answer the question?

CHRIS LEWIS-EVANS: Yes, I think it does. Thank you very much, KC. So Gabe, I would say we have one or two minutes, if it was a quick question.

GABRIEL ANDREWS: So I note as a law enforcement officer, I have hard time evaluating the recommendation number 2 that sought to create an executive level position within ICANN for security obligations, and that is something I note is important, but I don't fully understand necessarily the reason behind it and the justification, and I wonder if the shepherds can speak to that to identify why they felt that was so important and any potential downstream effects.

KERRY-ANN BARRETT: I want to give Laurin an opportunity.

LAURIN BENEDIKT: So to do this quickly, there are two broad reasons behind it. Number one is that this would bring security and security

concerns to kind of the highest level where we think for an area, organization like ICANN org is where it belongs, right? That is key thing for ICANN to look at and to deal with.

The second part is that if you look at the kind of literature, best practices and so on and so on for security management, a lot to be said about having security separate from other functions because you want to have that standard on its own so that you don't have the people who do whatever is needed, who implement, to also audit and look over the shoulders of those same people, so it makes sense to have two buckets, to implement and one to kind of look at it, has overview, giving it importance and also independence within the organization.

KERRY-ANN BARRETT:

And one of the things we looked at is the strategic placement of that position, recognizing that as like as we implement some of the recommendations that we have from all the various communities, to recognize the strategic advice, overview was necessary and encapsulate it into a position of whatever form it may be called, we thought it necessary to make that cut out to establish that as a strategic level, not just at mid-level management.

GABRIEL ANDREWS: Kavouss was asking if we could flip back to slide 6, to show the recommendations being spoken to. Yes. Thank you. And thank you for the answers.

CHRIS LEWIS-EVANS: And Nigel, I see you posted a question in the chat, maybe we can come to that after the DNS abuse presentation, because I think that will lead quite nicely into that, if that's okay. And with that, I would now like to pass over to a presentation on how some of our GAC colleagues, DNS abuse, how it has affected them. So if I could see pass it over to Shinya Tahata for the Japanese presentation on DNS abuse, thank you.

SHINYA TAHATA: Good morning, good afternoon, good evening, everyone. First of all, I would like to express my appreciation to the GAC chair, GAC leadership and Public Safety Working Group co-chairs to giving me this opportunity to speak. In this presentation, I would like to propose a project that can be considered to strengthening enforcement such as audits and as a section of DNS abuse.

DNS abuse is also a serious problem in Japan. For example,

please see page 1, the graph here shows around 5,000 URLs are reported to have been used by a phishing website every month. This website deceives users into believing that they are well known online shopping or banking sites and cause a lot of economic damage. In order to reduce the number of [indiscernible] it is important for registrars and registries to take action such as disclosure of registration data and suspension within the scope of ICANN contracts. We believe that we should [indiscernible] on registrars and registries to comply with agreements. This would be the best and most appropriate way to deal with abuse of domain names.

So ICANN contracts incur provisions that registries and registrars shall take appropriate measures against abuse. For example the registry agreements include that provision that requires registrars to include in registration agreements a provision prohibiting illegal activities. It also provides consequences for such activities, including suspension of the domain names. First of all, the agreements require registrars to investigate and respond appropriately to any reports of abuse. Also stipulates that should publish a point of contact for third parties wishing to report abuse. We believe having each comply with each agreement would be the best and most appropriate way to deal

with abuse domain names.

However, in fact there are some cases where registries and registrars and privacy and providers are showing invalid addresses as a dedicated abuse point of contact and don't respond to reports of abuse. At the present we know that ICANN audits the operations of registries and registrars. We think it is important to facilitate this, we can discuss more effective ways of doing audits such as confirming compliance of each provision of a contract.

Ideally, registries and registrars should investigate and appropriately take actions in order to guarantee that the operations of registrars and registries are in compliance with ICANN contracts. Japan would like to propose that GAC begin discussions of finding appropriate measures to strengthen enforcement, such as audits in this session. For example, we can discuss several ideas to improve the legal -- such as increasing the number of selected registries and registrars, implementing audits every year, and adding abuse other than DNS security abuse. That is all for today's presentation. Thank you very much for your time.

CHRIS LEWIS-EVANS: Thank you very much for that presentation, I think that was very interesting to see how you are seeing some of the DNS abuse and I think you highlighted, the raa, thank you very much for the input. Kavouss, I see you have your hand up. Do you have a question for this presentation?

IRAN: Yes, a comment, first of all. Thank you to my Japanese colleague. I think having audits an important issue, fully support that. There are two different types, internal and external. Internal inside the ICANN and outside, someone totally impartial and neutral, and I in general support the idea of audits. How we could do that, that is something to be discussed but we should put it in our work program to see creation of audit in ICANN and then talking about internal audit and then external and the report of the audit at least every year we should have the report, if not at every ICANN meeting. Thank you.

CHRIS LEWIS-EVANS: Thank you very much, Kavouss. And I see comments but just being mindful of time, I know we have a number of other slides on DNS abuse. So if we could cover those first and then get to further

questions after that. Can we go on to the first of the DNS abuse slides, please. Slide 16. Thank you.

So the first slide more informational around background work going on, DNS abuse throughout the community within ICANN. I think most of GAC colleagues will be aware of the amount of work that has been going on recently and the scale of that work across the whole community and I think it's worthwhile highlighting some of that GAC work going on with our other stakeholder groups and other members within the ICANN community. So some key ones here for me on the latest work, so I think on the DNS abuse framework side, I think they're now over 50 signatories and also [indiscernible] has started a DNS abuse institute, I believe less than a month old. So it will be interesting to see how that comes along and what recommendations that institute can make into the contracted parties.

We have also had a good session already this week with the DNS abuse Working Groups, both from a registrar level and a registry level, and they're really looking to engage with the community to gain an understanding of how DNS abuse affects each of the different stakeholders and what then can be done from a registry and registrar level from there.

Next slide, please. So as I mentioned at the beginning of the session, during ICANN69 we were asked as the PSWG to develop concrete proposals regarding DNS abuse for the GAC to consider and look at taking forwards. We considered quite a number of areas as you can imagine, and from a Public Safety point of view, I think it's really key we focus on the impact the DNS abuse causes and really try to understand and be able to articulate correctly the significance of DNS abuse onto the users of the Internet broadly and to make that sort of known within the ICANN environment.

One of the major ways upon which DNS abuse affects those users is through cyber crime, and realistically probably there are one or two of the sort of normal DNS abuse definitions that really affect users and people would understand. And from that the serious nature, one of those areas that we identified was phishing emails as having a high impact on the users. Also important is getting time reaction. I think recently we have seen a slowdown in some of the action that has been taken forward, certainly from a law enforcement perspective, and I think it is key that we understand the causes of that and how we can be more proactive in the measures we can take when we do detect DNS abuse or abuse of the DNS.

One of the other areas that I think we have talked about quite a lot and had really good conversations with the registrars and registries and other parties is fostering better information sharing mechanisms, something that I think has really taken on board across the landscape and we will be looking forward. I think we have mentioned it a couple of times, and it was good to see it also in the SSR2 review that Gabe has gone through that that sort of involved streamlining and standardizing abuse reporting and to really make that better known, I think it has come up a number of times in our communiqus about ensuring that our law enforcement colleagues in all different countries represented in the GAC aware of not only how to access data but how to share information with registries and registrars to report abuse.

And then finally, I think one of the things that I note is key to Laureen's side is educating end users and I think it is really important for them to understand not only what DNS abuse is or how it impacts them but also how to deal with it and how to stop themselves from becoming a victim of cybercrime. So with that, I want to pass it over to Laureen for the next slide, over to you, Laureen, thank you.

LAUREEN KAPIN:

Thank you, Chris, and I am very grateful to my colleague from Japan, because a lot of the issues that he identified are precisely some of the issues that we are working on at the Public Safety Working Group level as well, and I know time is short so I will be going over these briefly to allow a few minutes at the ends for questions and we also will and pick up whatever we have left over at our meeting later today. We certainly want to try to work with other stakeholder groups to identify specific issues where we have common grounds and agreement and discuss opportunities, we have to deal with these, including possible policy development efforts and some things already suggested by review teams including the CCT and SSR2 teams and also discussions with the contracted parties are ways to incentivize good behavior that seeks to take a proactive approach to dealing with DNS abuse. Trusted notifier programs and some registrars and registries already operate these programs so that could actually serve as a model and best practice. We would like to see closure on the discussion of DNS abuse definitions, because we think actually there are quite a bit of work that has already been done and the contracts themselves, these are already consensus policy positions defined in our existing contracts for new gTLDs, already have definitions that encompass DNS abuse and security

threats.

And then also, and this I think is what my colleague from Japan also identified, the existing contracts do have provisions that should be robustly enforced, and these could be clarified because some gaps have been identified. Also the reporting that our colleagues from ICANN org do as part of the DAAR reporting system, that is very, very useful and could be even more useful if it included information regarding registrars and actions taken by registries in response to threats. And also, we have the great example of our ccTLDs, in fact we had references yesterday as an example to dot EU and dot UK, with active, proactive practices in their approach to combating DNS abuse. So we want to continue these efforts, particularly also getting more data on DNS abuse to make sure that our tools and current mechanisms still relevant.

I think I am going to hold onboard discussion of the next slides and save those, so you have a little bit of a trailer. Those will discuss specific improvements to contract provisions and also DNS abuse definitions that are already the result of the current policy work. And we can discuss those in our Public Safety Working Group updates later on today. We have a few more minutes for any questions, and I did want to allow for that.

MANAL ISMAIL, GAC CHAIR: Sorry to interrupt, Laureen. We already have a few questions in the chat. If I can help out reading them.

LAUREEN KAPIN: Perfect, thank you.

MANAL ISMAIL, GAC CHAIR: One from Morocco, asking one of the proposed recommendations refers to the possibility or authority given to the ICANN organization to terminate contracts in the event of repeated conduct and abuse protection practices by any contracting party. For the case of registrars, what is the legal basis for this recommendation? Also, are there any measures to respect the rights of the clients of a registrar in case of termination of contract? Would you like me to go through all the questions before you take them?

LAUREEN KAPIN: I think that question relates to the SSR2 recommendation, so I would pass that onto any of my SSR2 colleagues who are best positioned to answer that.

GABRIEL ANDREWS: Specifically, I think that might refer to 15, [indiscernible]

KERRY-ANN BARRETT: Not sure who is on the call from SSR2, but in terms of the rationale for that, the idea was not an automatic termination but more to explore the possibility of this, recognizing it would have to be contractual obligations whenever that opens back up and as Andrew pointed out, the outcome would be to -- the feasibility of that, the lawyer of us in the group, thinking about what are the contractual ways we could address this, the legal part would be to be a part of the contractual obligations whenever that is reopened.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Kerry-Ann. And there is a question from CTU, the [indiscernible] asking, it's often mentioned that there is as yet for community wide definition the DNS abuse. How much of a challenge has this been in developing the recommendations and having them accepted?

LAUREEN KAPIN: I'm sorry. Kerry, Ann, please go ahead.

KERRY-ANN BARRETT: For us it was pretty difficult over the years that we were doing the review. One of the things we did was CTU was try to map it across ICANN's website but one recommendation we gave is actually consolidate this to try and have some singular place these definitions could be found.

LAURIN BENEDIKT: Which is it is really difficult to work on something without having agreement on what you are actually talking about. So this is still even though this has been going on for many years in terms of discussion, a key factor where we need to kind of find some form of agreement on what we are talking about, and I think one of the ways in which we try to deal with this is to essentially say we need clear key performance indicators, so it ensures things put into numbers and clear language, so we know (no audio).

GABRIEL ANDREWS: We just lost audio.

MANAL ISMAIL, GAC CHAIR: So --

LAUREEN KAPIN: Manal, I know we're getting short on time, and I defer to you. I do have a brief answer, or I can hold it until the Public Safety Working Group session.

MANAL ISMAIL, GAC CHAIR: If it is really brief, go ahead, Laureen.

LAUREEN KAPIN: Can you just go to slide 22? What I will say briefly, we do think that there are already existing definitions that exist, and I will discuss these in more detail, but the CCT review team did discuss the existing consensus definitions in its final report, and then the ICANN contracts give us very specific language as well. And taken together, I think this forms a very good foundation for how to move forward on what the community has already identified as DNS abuse definitions, and we can absolutely discuss this more in

the Public Safety Working Group update session later today.
Thank you so much, Manal.

MANAL ISMAIL, GAC CHAIR: Thank you very much, Laureen and just closing with a comment from European Commission that was also in the chat, saying: I would like to comment on the impressive work of the SSR2 team in putting together a very clear and operational report on the crucial issue of mitigating DNS abuse, very positive in both [indiscernible] including contractual enforcement and longer term measures I would agree that discussing the implementation of the SSR2 recommendations is of essence and the community would need to be fully involved in this collective effort.

Apologies to our interpreters if I was reading quickly, just for the sake of time. We are five minutes past the hour, so just to thank you very much, Chris, Gabriel, Laureen, Shinya, and also shepherds from the SSR2, Laurin, Kerry Ann -- and thank you for a very thorough analysis and deep dive on SSR2 recommendations as well as recent developments within DNS abuse and also next steps and a concrete proposal for improvement from our Japanese colleagues.

So with this, it is time for a 25 minute break. Please be back in the GAC Zoom room at 10:30 Cancun time, 1530 UTC, where we will receive a 30 minute update from the Public Safety Working Group and then start our discussion again on subsequent procedures. Thank you very much, everyone.

[END OF TRANSCRIPT]