BRENDA BREWER: Good day everyone, welcome to SSR2 Plenary call number 82 on 11 September 2019 at 14:00 UTC. Attending the call today is Laurin, Boban, Danko, Eric, Kaveh, Naveed, Ram, Denise, Russ and Zarko. Apologies from Norm and Kerry-Ann. Attending from ICANN Org we have Jennifer, Negar, Steve and Brenda. Technical Writer, Heather has joined. Today's meeting is being recorded. Please state your name before speaking, for the record. Russ, I'll turn the call over to you. Thank you.

RUSS HOUSLEY: Welcome. I suggest that we take item number three first, because I think it'll be short. The Doodle poll clearly shows that we're going to get more people on January 16th and 17th. So I suggest we just pick those dates. Based on a discussion on the leadership call, it became very clear that we would get at least one more person if we held the meeting in D.C. And so, I suggest that we do the two-day meeting -- January 16th and 17th -- at the ICANN office in D.C. Does that cause a problem for anyone? Jennifer, could I ask you to send a note to that effect? Just so that anybody who's not here has an opportunity to scream before we go final with that.

JENNIFER BRYCE: Hi Russ. We can certainly do that. Do you mind if we put a date on it? Like say, by end of day, Friday?

RUSS HOUSLEY: That would be more than -- do I mind -- please.

JENNIFER BRYCE: Great, thank you. That will allow us to get the travel team informed immediately. Thank you. We'll do that.

RUSS HOUSLEY: Okay, thank you. All right. So then we're going to go to the document that Jennifer sent out earlier today. Denise, are you the one who's going to walk through this?

DENISE MICHEL: I certainly can. I think I have the members of the subgroup which [inaudible] as well. The subgroup on Abuse was Norm, KC, Eric, Laurin, Kerry-Ann and Scott.

RUSS HOUSLEY: Can everyone hear Denise?

JENNIFER BRYCE: Could Denise get closer to a microphone?

ERIC OSTERWEIL: Russ, if you go back where you were and Denise, you stay there, I'll move this thing. Bear with us everyone.

RUSS HOUSLEY: Okay. Can people hear me?

DENISE MICHEL: I hear you, Russ.

RUSS HOUSLEY: All right, Denise. Over to you.

DENISE MICHEL: If you recall, this subgroup has been researching, analyzing, discussing and findings and recommendations in the area of abuse and compliance. The document that you have is an updated draft. It still needs some work, but the major findings and recommendations are there. The recommendations list at the top needs to be updated. I think we discussed on a previous call -- Laurin, I think you were leading that discussion -- we discussed the findings, where we outlined the global threats to SSR to provide context for the findings and recommendations that provides high-level information and references relating to the various attack factors and abuse: malware, digital certificate fraud, phishing, business email compromise, scams, botnets, spam, DDOS attacks.

With that overview and context, we then highlighted some important actions that ICANN has taken in the context of these threats that touches at a high-level action on the new gTLD abuse -- the threat relevance and relevant areas of the RAA, the Registrar Accreditation Agreement, the gTLD registry agreements. I think additional information needs to be provided there. Our focus there was on the

new gTLD base registry agreement, the update of that and the update of that base agreement. And then the data and advice activities by ICANN, touching on the SSAC, the Security Stability and Advisory; some particularly relevant [inaudible] have been published in the past.

The GAC, Governmental Advisory Committee, some additional information needs to be provided there. And relevant recommendations offered by the RDS review, that's the WHOIS review that just completed. And the CCT review, the competition consumer trust and consumer choice, also touches on the DAAR program and ICANN compliance.

And then that takes us down on page nine, to the recommendations that that subgroup has been working on. They fall into three general buckets, starting on page nine. The buckets involve compliance, is one. The second bucket is abuse definitions and reporting. Third bucket is policies and agreements with contracted parties. Again, some additional work needs to be done, but there's definitely enough substance here for team members to weigh in on the draft recommendations that the subgroup has put forward. Starting with the first bucket on Page nine, I'll briefly run through these. And again, the rest of the separate members should please weigh in where appropriate.

So the first recommendation is regarding compliance, and that the board and ICANN Org should fundamentally change the compliance regime by taking necessary steps to amend the party agreements, establish procedures to address systemic abuse involving contracted parties, and move its registrar and registry compliance activities to an

independent compliance office outsource to an established auditing firm.

Additional details on these recommendations are included in the bullets there. The changes to the party agreements include some recommendations for amendments related to abuse mitigation measures and obligations, focusing on ensuring that compliance office has enforcement mechanisms to treat the abuse that we've outlined -- that contract changes should be moved forward to establish procedures to address the systemic abuse. And these include moving forward with -- under the current abuse definition that was vetted by the community and have been in place for several years, had SSAC work with well-established abuse mitigation organizations outside of ICANN to define systemic abuse for ICANN's use, and [inaudible] level of abuse countermeasures for contracted parties, use this as a basis to amend contracts as soon as possible [inaudible] next renewal cycle.

RUSS HOUSLEY: Can I ask the question here? Maybe I went through this too fast -- I've only had it a little while -- but what is the difference between colloquial and legal?

LAURIN WEISSINGER: Yes. Who wrote that?

DENISE MICHEL: I think Kerry-Ann. I think that's Kerry-Ann's language.

RUSS HOUSLEY: I just don't know what it means.

ERIC OSTERWEIL: I believe the idea, if I remember correctly, is that essentially one definition is colloquial. So, what does abuse include? And then the other one is framed in appropriate legal terms so that the definition of work inside the legal document, which might be slightly different from the way we would phrase this. I think that's the only --

RUSS HOUSLEY: Actually, that to me, is a word. Because if you're talking about amending a legal agreement -- the RAA -- you better be reading one that's not colloquial.

ERIC OSTERWEIL: This is exactly the point. To add a little bit to what Laurin's saying to maybe kind of bridge the two things there -- what I got out of that was that, understanding that DNS Abuse is defined by several technical trainees. There's no clear reason why it ever should show up as legal terms, from their perspective. But we need it to. And in fact, we need to underscore that this has to be there. Because if you look at some of the provisions, like in GDPR, that was done from the reverse. It was done legally and then, "Technical people, you figure it out."

And then there's like, "What the heck?" It's the reverse here with DNS Abuse. The abuse community keeps evolving what we think abuse is,

but if we don't actually put the energy into saying this is how you effectuate legally, then some version will show up it may not map. So I think we need to have something there, concerted there, to do that mapping.

RUSS HOUSLEY: Then I think that should be a recommendation to start with.

ERIC OSTERWEIL: Okay.

DENISE MICHEL: Yes, a big question. And please raise more. As I said, I think the work needs to be done by the subgroup on this task. I'm making note that this needs to be clarified. I guess Kerry-Ann's on a call, but we'll make sure that we circle back with her. She has an opportunity to clarify that. Because the goal indeed is to make sure that clauses on systemic abuse and required counter measures included in the contract make them enforceable and very explicit, and make sure SLAs are in place that help.

RUSS HOUSLEY: All of that makes sense to me. This was the piece that I couldn't fit into that puzzle.

DENISE MICHEL: Then in the compliance area, the additional recommendation that came out of the subgroup was -- they spent a lot of time looking at ICANN's

compliance activities over the last decade, talking to compliance, getting a lot of Q&As and additional information. And where the subgroup is interested in moving compliance, is to address the inherent conflicts that we have with ICANN in compliance. Similar to financial institutions that outsource their auditing work, the subgroup is suggesting that it can move its compliance activities to a neutral third party auditor.

This would help address the inherent conflicts in ICANN, enforcing on the registrar and registry parties that it receives a large majority of its financial support. So that's the recommendation on the table -- that ICANN should establish an independent compliance office outsourced to an established auditing firm, populated with staff with significant compliance experience and understanding of both DNS Abuse mitigation and registrar and registry industries.

The suggestion is that this compliance office be empowered to react to complaints and require compliance to initiate investigations and enforce against those aiding and abetting systemic abuse. This could include step-by-step authority for the escalation of enforcement measures and implementable actions that can be used for failure to remedy in the specific timeframes. It's also recommended that compliance partner with complainants, rather than simply partner with contracted parties. So, partnering with complainants and making sure that its processes are set up to serve public interests.

It's recommended that compliance default approach should involve SLAs on enforcement reporting, clear and efficient processes and fully informed complainants, enforcement and reporting process with

maximum public disclosure. Some similar and related recommendations [inaudible] are in the RDS review recommendations and we've even included a note to make sure that we capture that as well.

And that specious complaints should be reflected in the public record as well. Separate notes that ICANN compliance has a history of keeping complainants and the public in the dark. And accommodating contact with parties, rather than public interest in [inaudible]. So unless there are questions and comments, and of course I think that [inaudible] would encourage team members to also follow up on email and clarify additional comments on the list.

The second recommendation area in abuse and definitions and reporting -- it's on page 10 -- recommending that the board and ICANN Org overhaul ICANN's approach to DNS Abuse definitions, tracking and reporting. This includes implementing community review recommendations. That's specifically the CCT review and the RDS review and other security-related actions, act now using current DNS Abuse definition and in parallel use international conventions to evolve the definition.

And finally, to create a single portal for all complaints, and make public reporting mandatory. So the subgroup is recommending that ICANN implement the CCT review and RDS review recommendations related to. abuse and security and other security-related action based on the current community-vetted abuse definitions without delay. There’s [inaudible] in there no later than 2020, which I think we should talk about some more.

RUSS HOUSLEY: [Inaudible] even come out till 2020. [CROSSTALK]

DENISE MICHEL: And again, these recommendations, we also need to add additional text to make sure these are smart goals, and we're thinking about specific activities and recommendations. The subgroup does not agree with the board and its actions to park a substantial number of CCT review recommendations and start a tabula rasa discussion about what DNS Abuse means -- that current DNS Abuse definition that ICANN has been using for the last several years, well vetted by the community, reviewed by staff every year and is, we feel, actionable. But we also think that the abuse definition needs to keep pace and evolve with cybersecurity threats.

And so we're recommending that ICANN adopt the additional term in evolving external definition of security threat -- the term that's used by the ICANN DAAR project, it's been used many times by the GAC, and is also used by operational security communities, and use this in conjunction with ICANN's current DNS Abuse definitions. We provide information citations relating to the Convention on Cybercrime. It's a reference resource for assisting with this security threat definition.

I think the group found it important to note that the expertise in security threats does not reside generally in the ICANN community. And that is similar to ICANN's reliance on external organizations like the UN and ISO to define what a nation state is, to assign ccTLDs, ICANN should recognize the external expertise in this area as well. And use the widely

acknowledged -- use cybercrime conventions to make sure that it evolves its definition [inaudible] in its work.

The final point in this area is that ICANN should establish and maintain a single complaint for all complaints that automatically directs the complaint to a relevant party. This proposal is that the system would act as an inflow, with data flowing up upstream. That it be mandatory for all gTLDs; that ccTLDs should be invited to join. This would enable ICANN to much rapidly track the data, publish yearly reports, track the complaint workflow.

LAURIN WEISSINGER: The idea is, if there is a complaint it can be put in one single place. That system will then automatically forward to the appropriate contract party. They can then deal with it like with any normal ticket system. And if they don't deal with that in a certain amount of time, it can be escalated to the next level. The complaint goes to contracted party, contracted party address the complaint and then would fill in a little spreadsheet or something like that where they would say, "Okay, we looked at this complaint. Yes, we took action." And then what action was taken. Or they can say, "Well we cannot take action." And then they might be able to choose from different reasons. An obvious one being, "Within the jurisdiction we're operating, this is not something -- sorry."

And then this like showed report goes back up so you can see some statistics on what's going on, but not necessarily old content. And what this would also do would then be that, the person who complained to

the organization, that complaint gets something back that says, "Oh, this was dealt with but only X could be done." Which also simplifies for them how to move forward.

DENISE MICHEL: And so, obviously an attractive part of this is that it will enable improved public reporting and security threat reporting, and there would be a much higher level of transparency and public access to the complaint. In addition, in the public reporting area, the subgroup has recommendations relating to DAAR. To ensure its utility, that subgroup is recommending that data gathering for DDAR should not be rate-limited; that reports should be published that identify registries and registrars that most contribute to abuse; should illustrate entities with persistently very high abuse domain registrations; published reports should provide tabular data in an accessible processible form in addition to the graphical data; the DAAR project should also have access to pricing data. And I think another thing missing here is API access. So that rounds out the second bucket of recommendations for the task group.

The third recommendation focuses on policies and agreements with contracted with parties. The subgroup is recommending that ICANN adopt new ones that may fully impact the mitigation of DNS Abuse and security threats. This includes changes to WHOIS, incentives for contracted parties for abuse mitigation, incorporating measures to mitigate DNS Abuse and security threats and agreements with contracted parties, establishing performance metrics and

institutionalizing training and certification of contracted parties and key stakeholders.

To dive into this a little bit, the subgroup has spent time looking at the changes to the WHOIS policy and the serious impediments that is caused for security investigators of abuse mitigation and the threat to DNS security stability and resiliency, and is recommending as a matter of urgency that ICANN ensure access for parties with legitimate purposes via contractual obligations and with rigorous compliance, rather than as a voluntary implementation.

I think there we'll need to add some additional language regarding how this connects with ICANN board's action and the threat policy development activity that's under way. In addition to noting the need to address rate-limiting for the DAAR project and other reporting systems, there's also recommendations to rigorously enforce the uniform centralized data zone service requirements. Noting that continuous access to these zone files are a critical part of abuse mitigation investigation and research.

The subgroup is recommending incentivizing contracted parties to mitigate abuse and security threats. There is a historical basis for this recommendation as ICANN Org, in the past, has rewarded contracted parties with fee reductions to incentivize certain business practices (elimination of the domain tasting is a good example of this). The existing contract framework enables ICANN to impose changes unilaterally and immediately.

The subgroup is recommending the following actions that ICANN should take: That contracted parties with portfolios that have less than one percent abusive domain names as identified by commercial providers and/or DAAR, receive a fee reduction. This could be a reduction from current fees or ICANN could increase the current 0.18 percent per domain name for low abuse levels.

RUSS HOUSLEY: It's $0.18, right?

DENISE MICHEL: Yes, $0.18. Recommending that registrars receive a fee reduction for each domain name registered to a verified registrant. And (3) that any RSTEP fees be waived when in connection with RSEP filings that will demonstrably mitigate DNS Abuse, and that any registry RSEP receives pre-approval if it permits an EPP field at the registry level to designate those domain names as under management of a verified registrant. So, validation verification of registrants also would have an important impact on mitigating abuse. The subgroup is suggesting specific ways to help incentivize that. This is very much the carrot approach. It has worked well in the past for ICANN. As an example, eliminating domain tasting, and we're recommending that it be used again.

Another element of this area of recommendations is incorporating measures to mitigate DNS Abuse and security threats in the agreements with contacted parties, including the registry agreements and the RAA -- agreements with the registrant. And then there are some specific suggestions from the subgroup that was included as a priority provisions

that establish thresholds of abuse, recommending 3% of registration or 30% total, whichever is higher, at which compliance inquiries are automatically triggered. And with the higher threshold, recommending 10% of all registration, at which registrars and registries are presumed to be in default of their agreements.

This approach also was underscored in the CCT review citation there and the SSR2 also recommended that. In addition, ICANN should publish a list of enforcement tools identified by ICANN Compliance as needed to combat abuse and security threats; coordinate closely with relevant non-contracted parties to identify additional gaps within ICANN's contracts and contribute to abuse and security activities; develop a list of impactful contractual updates to guide negotiations; ensure not-contracted party representatives who thought leaders on security threat mitigation are involved in all basic contract negotiations and endorse the changes.

One of the things the subgroup found was that there was a pretty large disconnect between abuse experts and cybersecurity experts, and those that were actually at the table creating the contracts. So it was felt it was important to bring those experts and representatives to the table to ensure that the contracts adequately addressed security threats and abuse. The group also recommended we make sure that ICANN's legal authorities address compliance security. And their stability in the DNS is clearly articulated in the bylaws and service level agreements. That's an area that Kerry-Ann would be able to stand upon.

And then finally the group felt there was more work to be done in institutionalizing training and certifications for contracted parties and

key stakeholders, particularly with the large growth in recent years of the number and diversity of backend registries and the hacks and security threats that plague registrars in recent years. So, recommending that there's automatic tracking of complaint numbers, probably will help with this. And treatment of complaints, we know being closest, require quarterly and yearly public reports and complainants and actions analysis and robust training and certificate for registrars and backend registries. That's it.

RUSS HOUSLEY: I know the presumed and default section of those two bullets back is exactly text out of the CCT review. So basically, what that recommendation is really saying is, please do the CCT part.

DENISE MICHEL: Right. And one of the things we may want to look at is pulling together this CCT and RDS recommendations that are relevant and were endorsed by the SSR2 team, and re-recommend them.

ERIC OSTERWEIL: One of the things that I was thinking earlier, and this really underscores, is that if we show the logic that we've used to come to the same conclusion, as opposed to just saying, "You should do the same thing." Because if we say we think you should adopt the same thing and we don't give any transparence into our thinking, it could maybe just get ignored a little easier. This is very methodical in supporting the same conclusion, and we could even tack on the end, "We note this is

completely in line with the CCT review." And I think it has more teeth that way.

RUSS HOUSLEY: So that's a way of structuring the findings. It doesn't change the recommendation?

ERIC OSTERWEIL: Correct.

RUSS HOUSLEY: All right. I just wanted to make sure understood. I'm not seeing any hands. Are there others who -- What I think I would like to do is give everybody time to digest this. I realize you only got the document today, but if you have any concerns about the direction that this team is going, let's raise them on the list before the call next week. Anyone have concerns with that?

LAURIN WEISSINGER: I will ask Jennifer to send around a Google Doc, but everyone please make sure you use the mode where you don't just edit, but where you suggest. So it's simple to track comments and changes.

JENNIFER BRYCE: Sounds good.

RUSS HOUSLEY: I'm hearing silence, which I'm taking to mean that people are liking the direction this is going.

BOBAN KRSIC: Still reading it's a lot of stuff.

RUSS HOUSLEY: Yes, of course. That's why I said by next week.

BOBAN KRSIC: Next week sounds great. Thank you. And it looks pretty good but I need more time. I am on page three [inaudible], but I think it's on a good way.

RUSS HOUSLEY: Okay. I think that brings us to any other business. Okay, I'm not hearing any, so Jennifer, could you take us through the actions and decisions?

JENNIFER BRYCE: Thank you. Just a couple of action items. First of all, for staff to send the dates. I believe it was the 16th and 17th of January -- from the Doodle Poll -- with the proposal to me in D.C. on those dates. And then, if any review team members have issues, please let us know by end of day, wherever you are in the world on Friday.

And then I see that Laurin just sent me that document that was discussed on the call, so we'll put it into a Google Doc. Please make

comments in suggest mode ahead of next week's call on Wednesday. Those are the actions that I captured. I didn't get any decisions other than the tentative D.C. meeting date. So let me know if I missed anything. Thank you.

LAURIN WEISSINGER: Just to note, this is already a Google Doc, so no conversion needed.

JENNIFER BRYCE: Excellent. One less thing to do. Thank you.

RUSS HOUSLEY: All right, thank you very much. We'll talk next week.

[END OF TRANSCRIPTION]