BRENDA BREWER: Good day, everyone. Welcome to SSR2 Review Team Plenary Number 79, on the 7th of August, 2019, at 14:00 UTC. Attending the call today is Alain, Ram, Denise, Danko, Norm, Eric, Kaveh, Russ, and Laurin. Apologies from Naveed. Attending from ICANN Org is Jennifer, Negar, Steve, and Brenda. Technical writer Heather has [joined us]. Today's call is being recorded. I'd like you to please state your name before speaking. Russ, I'll turn it over to you. Thank you.

RUSS HOUSLEY: Hi. The agenda that was sent out says that the first thing we're going to do is welcome and roll call—done. And then the next thing is, we're going to discuss the recommendations from the sub-team that's been working on compliance. I don't know who's planning to lead that discussion.

DENISE MICHEL: I'll start it off.

RUSS HOUSLEY: Okay, great. Thank you.

DENISE MICHEL: Hi, Russ. We have a group of sub-team members who have been working together on a large bucket of issues and recommendations that we grouped under abuse mitigation and compliance-related items. Those SSR2 Team members include Kerry-Ann, KC, Scott, myself, Eric,

Norm, and Laurin. Much of this text, the team members have seen before. Some of it is new. I think, hopefully working around work and vacation commitments, we'll be able to get our sub-group together on finalizing draft text to send to the team. I think we're fairly close to that.

In advance of all of the recommendation text, we wanted to outline the approach that the sub-team is taking on the key areas of focus, and highlight a couple of the new recommendations that the group is working on. I'll give you an overview—an outline of the findings and recommendations that we're working on. Norm will discuss the findings that focus on the world SSR threat—basically, the foundation for these recommendations, and you'll have that draft text in your inbox.

Then, hopefully Kerry-Ann will be on to address a recommendation relating to DNS abuse definition and incorporation of the Council of Europe's convention on cybercrime definitions. And Laurin will discuss a recommendation on establishing a single complaint portal.

To briefly review the approach that this group is taking, we have a draft text that Norm will discuss, that provides the general context and findings for these recommendations, focusing on the main threat factors. Then we have draft text that addresses the gap between what ICANN has done thus far and the threat, highlighting abusing new gTLDs, issues relating to the Registrar Accreditation Agreement and the Base Registry Agreement—noting activities and recommendations that are relevant from the SSAC, Security and Stability Advisory Committee, and also the GAC, the Governmental Advisory Committee, and other key stakeholders.

We also touch on relevant recommendations from the community reviews, including the CCT Review—Competition, Consumer Choice, and Trust Review—recommendations that are relevant to this area, and the RDS Review Team recommendations. We also touch on DAAR, the abuse data project, and of course activities that have been undertaken, and issues relating to the ICANN compliance efforts. Those are the two key areas of findings that we have in the draft text.

Then, our draft recommendations fall into three areas. The first area is compliance. The recommendation there focuses on some changes that we propose to recommend, relating to ICANN's compliance regime—empowering the compliance activities of ICANN, and changing the approach.

The second group of recommendations fall under abuse definitions and reporting—recommendations around overhauling ICANN's approach to DNS abuse definitions, tracking, and reporting. In this bucket are recommendations that the CCT Review sent to the board, that is in line with SSR2's works—recommending actions around abuse definitions that Kerry-Ann will outline for the group, establishing the complaint portal, which Laurin will review, and recommendations around improving complaint reporting and security threat reporting.

The third bucket of recommendations are under policy and agreements with contracted parties, focusing on meaningfully impacting abuse mitigation and mitigation of security threats. These include updating key policies and practices, incentivizing contracted parties to mitigate abuse and security threats, incorporating measures to mitigate abuse in agreements with contracted parties, and then institutionalizing training

and certifications for contract parties and key stakeholders to help mitigate abuse. Those are the key areas of recommendations, and with that, I'll turn it over to Norm to discuss the findings related to the SSR threat. Norm?

NORM RITCHIE: Hey. I hope people have had a chance to review the document, or at least pull it up now to have a looksee at it. That was included on the e-mail that went out for the agenda for this meeting. There it is. Thank you very much. Through our discussions, one of the things we found in our sub-team quite a bit is that we live and breathe abuse and mitigation stuff, and we just take a lot of things, probably, for granted. We just assume other people know that.

Through some of the discussions, what was missing on this is basically characterizing the state of the world right now, as far as domain name abuse goes. This is an attempt to clarify that at not too high of a level, not too low of a level—just at the right spot, but also including citations to back up the points being made.

If you scroll down, I think, to page two—that's what we're on right now on the screen—there's different types of abuse, which covers a large range of things. Too often we just use the phrase "abuse," then everyone interprets that their own way. Strictly at a higher level, it makes sense to talk that way, but when you into details, it doesn't always apply. And also, if you want a counter in your arguments, it's easy for them to throw in a detail and no one can defend it.

Breaking down the different types … With citations, you can see them there. There's malware, digital certificate frauds that the EPWG can tell us about—a well-respected group. Phishing—again, the APWG, a very well-respected group in that area. We have to add the stats and the citations in, but this is just to give you an idea of where we're heading. The business e-mail compromise has been going on for quite a while. That is an area that affects not just businesses, but also of late, it's been affecting a lot of city governments as well. They've been a target for that.

One of the areas in "What is abuse?" is [inaudible] abuse. I'd certainly say it is. Others of [you may not] agree with that. But [in these] scams, you have [inaudible] domain names, and then you have the notorious botnets. Spam is an area that some people will debate on whether that's covered in abuse or not. I don't know that it's up to us or not to determine whether it is part of abuse. I think that's up to the community to decide that. For now, we should probably include it because spam certainly is used to initiate abuse [inaudible]. Also, we need to talk about DDOS attacks as well. [inaudible] some stats on those. We have to gather them still.

RUSS HOUSLEY: So, Norm, in Kobe, we got a briefing on the DNS espionage thing. What category do you think that falls into here, or do you think it's orthogonal?

NORM RITCHIE: I think that's orthogonal to what we call DNS abuse. That was a [targeted] …

RUSS HOUSLEY: That was very targeted, that's for sure. But I was thinking that some of the business e-mail compromise things have been quite targeted as well.

NORM RITCHIE: Yeah, good point to put that in here as well. That's the attack on …

ERIC OSTERWEIL: I think that's actually in there. I think that's in the document. It's under a different section. There's something about ICANN and multifactor authentication, and pushing for the need for that, etc. So, it's in there, I believe. I'm on my phone, and I can't see where in the document, but I believe it's covered in there. I think DNS espionage is not … The 2019 candidate USG domain name concern, etc., and how the response was … Anyway, I think it's in there.

NORM RITCHIE: Okay, thank you. I think, Eric and Russ, I kind of agree with both of you. I think that it's worth mentioning here, at least to cross-reference this, if it is in another place. The purpose of this is really to highlight the problem. That lays the foundation for the recommendations, and the actions, and the further discussion that we're going to have. I think that's worthwhile.

Through some of our discussions, and some of our investigations, there's two broad areas that need addressing in order to handle the abuse problem, one being the contracts themselves. Contracts actually, in some cases, prevent people from taking action, which is not their intent. In turn, those prevent compliance from doing anything, because they actually have to follow contractual compliance. They are bound to that contract. They can't step outside of it, contracts being the Registry Contract, the Registrar Contract, and the Registrant Contract. There's three of them.

I think we need to keep the focus at that higher level, and the recommendations fall out from there. The one area where I think there has been some improvement would be in the DAAR. It's worthwhile noting that DAAR is a step in the right direction, but yet again, that seems to be limited. It's like the grasshopper jumping up and hitting the lid of the jar, where it just can't get [it's own] way right now to be really more effective. I think that covers the broad scope on that. You can read the document. Please do so, because I think this will be a fairly substantial point of discussion for the community. Comments, questions?

DENISE MICHEL: Thanks, Norm. If there are no questions, then we'll move on to the recommendation that we wanted to highlight around DNS abuse definitions, then. Kerry-Ann was going to walk through that. Kerry-Ann, has she been able to join the call?

JENNIFER BRYCE: This is Jennifer. Kerry-Ann actually sent her apologies for this call.

DENISE MICHEL: Okay. I'll walk through that, then. A draft recommendation under discussion by the sub-group is suggesting that we augment the current definition of DNS abuse that has been in place for some time, and vetted by the community. It was also highlighted in the CCT reviews report as well. The recommendation is suggesting that in addition to—to augment that DNS abuse definition—that ICANN should also use the Council of Europe's Convention on Cybercrime definitions as a reference and a resource for identifying security threats that we should recognize as threats, and that this external treaty organization recognizes as criminal acts.

The Convention on Cybercrime is, of course, very longstanding and well-used. The Convention is an active and ongoing effort—as I noted, treaty-based. What we find particularly useful about this is that it pulls in the crimes and security threats, particularly those tied to domain names. It employs a threat taxonomy that experts have developed, and it's been rigorously used. Augmenting the DNS abuse definition with the Convention's definition allows ICANN to not only rely on internationally-recognized expert work in this area, but the convention has a process whereby they, on an ongoing basis, re-evaluate, and add to, and update the security threats that are addressed in the Convention.

Much like ICANN relies on the UN's list to define what countries and territories are, relying on the internationally-recognized expertise of the UN in that area, we think a similar approach would really benefit ICANN

in relying on an external, internationally-recognized group to augment and to keep up to date ICANN's DNS abuse definitions and security threat definitions. The recommendation that we're working on would bring that into practice within ICANN.

When the sub-group has agreed on the recommendations text, this bundle will be shared with the full review team and dropped into the Google Doc. I think that's it for that recommendation. Unless there's any questions, Laurin can highlight the recommendation regarding a single complaint portal.

LAURIN WEISSINGER: Hi, everyone. I'm not hearing questions, so I'll just go ahead.

JENNIFER BRYCE: Laurin, Alain actually has his hand raised.

LAURIN WEISSINGER: Oh, I'm sorry. I'm on phone only, so I can't see.

ALAIN AINA: I want to ask clarification on two things. The first one is the last item on this thing, point three, to institutionalize training and certification for contracted parties and key stakeholders. Can you elaborate a little bit on what are you advising here, because I didn't get it correctly. I don't know if I missed part of the explanation, but can you please explain again? I'm having difficultly accepting this in the context of ICANN doing

this kind of certification for contracted parties. I would like to understand more about that.

DENISE MICHEL: Yeah, thanks for the question, Alain. The sub-group isn't done with that draft recommendation. It's still under discussion, so we don't have specifics to discuss at this point, but we'll be coming back to the list, I think, fairly shortly. Thanks.

ALAIN AINA: Hello?

RUSS HOUSLEY: We hear you.

DENISE MICHEL: Yes.

ALAIN AINA: Okay, I also have another point about the CCT Reviews recommendation. I seem to be slow these days, but maybe staff can tell me. Have all the recommendations from the CCT Review been accepted by ICANN Board?

RUSS HOUSLEY: This is Russ. That's a very long discussion. The board put them in three buckets, none of which are scheduled for implementation yet, but some

of which are being investigated. Some of them were not for Board Action, but for community action, and those were just forwarded to the community to decide whether they want to act on.

ALAIN AINA: Okay.

DENISE MICHEL: If there are no further questions, then I think, Laurin, we'll turn it over to you.

LAURIN WEISSINGER: Okay. Hi, everybody. I won't talk you through exactly what's on the page, because you can read that yourself. I'll try to give some context to this. Essentially, right now, as we know, there is no centralized system. You have to know where to go. You might report something. You don't see what's going on. Furthermore, there are interesting effects that would come from having a centralized system.

Essentially, the idea for that one is that there is a centralized system, which essentially is a website—I don't know, complaints dot ICANN dot org. You can go, and you can send abuse complaints into the centralized system. The system can automatically forward these to relevant contracted parties, and should nothing happen at, say, a registrar level, it would after some time, then go up to the next level.

Why is this important, or why did we think this is a good idea and something to recommend? Essentially, it makes it simple for people

who want to report abuse. Again, as Norm mentioned before, there are a lot of people who are not in this ecosystem, and who would struggle finding out how it works. Even if you are in this ecosystem, it's obviously much easier to do this centralized.

That's one aspect. The next aspect is that we're imagining metadata to flow up through the system, which means that if I'm a contracted party, I get forwarded this abuse complaint. I treat or deal with it as I see fit. The only thing that comes back is something along the lines where I say, "Okay, this is a spurious complaint. This is not relevant. We did not act on it because it's not appropriate." That would go back up. Or it would be, "Okay, yes, this was clearly something abusive. We shut it down." That allows the ICANN community and ICANN Org to see who is actually responding to abuse complaints, and how quickly, and in what way.

That, then, allows, a, to see what's going on—going into the direction of collecting data, having visibility on what's going on in the system, which we have elsewhere. Then, obviously that allows, if someone is hit with a lot of complaints, you can then see are they just being bad by not responding, or what are their responses?

What would not happen, according to the current recommendation, is that detailed information would be reported by the system, and the reason for that is that we feel that this would probably … A lot of contracted parties wouldn't like that, but we see less of a problem with having a very data-sparse system that still allows some insight. And then obviously if, say, one contracted party looks off, you can then always go in and see what's going on, or they can see, "Why are we so different from everybody else. Let's investigate that."

That's essentially this one. Meant to simplify how things work—meant to automate—an automated escalation, as well as some data on what's actually going on, because also clauses in the contracts right now on abuse handling are not particularly useful, as we've seen in multiple cases in the past few years. That's more or less it. Thank you.

RUSS HOUSLEY: Laurin, I'm just trying to figure out how this doesn't just become a big place where all the abuse reports get collected. Is there some vetting before they become public? I think that a whole bunch of process needs to be put around this. Maybe that requires community discussion. I don't know. It would not be good if this just became a repository of everybody's complaint.

LAURIN WEISSINGER: Hi, Russ. The idea is not for that to actually become public, simply because there is no way, without human oversight—at least not right now—to try to throw out all types of, let's call them, abusive abuse complaints. The idea is more that this is kind of an input system that then forwards it according to set rules and then waits for a set amount of time, and if nothing comes back from that party, then goes up to the next level—for example, registrar to registry.

As I said, the idea is not to make this a data behemoth. We all know that this can be also a big issue. I feel this will need at least some level of community discussion, but at the same time, it should simplify the system considerably, and would allow at least some insight into what's going on. But again, the idea is not to essentially have ICANN collect all

abuse complaints and have insight, because that would likely cause a lot of issues with contracted parties, and likely for understandable reasons, at least in some cases.

RUSS HOUSLEY: I guess you've said it twice, that this provides insight. I guess that's where I'm getting confused. Insight to whom, if it's not the community?

LAURIN WEISSINGER: It does provide insight to the community, but not to the specific content of an abuse complaint. For example, what would happen is I report a malware domain, and say, "This is abuse." This goes to the registrar. The registrar looks at it, confirms, takes action. What then throws back is saying, "Well, there was an abuse complaint, and within five days, the registrar replied, 'Yes, we confirmed. Was abuse, took action.'" That's it. But unlike now, you do at least have that very high-level overview over what's going on, plus a simplified way of reporting that in comparison to now.

RUSS HOUSLEY: No, I understood and appreciate the simplified way of reporting it. Thank you for summarizing how this is going to provide insight. Do others have questions? When does the sub-team think they will have recommendation text and then findings text?

LAURIN WEISSINGER: This is obviously my own perspective on this. We wanted to bring to the team's attention what we've been doing. We had a few, but not many questions. So, at least from my perspective, we should probably have one more call, maybe one more edit pass, before we can provide pretty final text, because there were no major changes requested or major questions, but more clarifications. We will make sure that the text reflects that.

There are already quite a lot of things in our document, like findings as well, which probably ought to just need another pass. So, at least from my perspective, we should be able to have something final very soon. Not sure who else is on the call, who is on the sub-team, apart from the ones who spoke, but yeah, that's my perspective.

DENISE MICHEL: I would agree, within just a couple weeks, I hope. Of course, we have a lot of busy volunteers, so it will be dependent on getting a final agreement on the text.

NORM RITCHIE: I would really appreciate if others could either lend support, or have questions, or something. Show me anger. Show me pain. Show me something, because this is going to be … I think it'll get a lot of attention within the community, when we do the draft report. I'd like to know where everyone stands on it. Not saying you have to do that now, but send an e-mail. Do something, please.

RUSS HOUSLEY: Norm, I think you're going in a good direction. Okay, I'm not hearing any other comments right now. Are there hands?

JENNIFER BRYCE: There are no hands.

RUSS HOUSLEY: Okay, so let's … We had an e-mail about people updating their recommendations text in the Google Doc. A bunch of people had signed up to have it done by today. Other people had signed up to have it done a week from today, and there's still a couple blank slots. Please, the penholder for each and every recommendation, make sure that you're not one of the blank spots, and fill in when you can have that done. Is there any other business we need to talk about today? Not hearing any, and assuming somebody would have spoken if there was hands. Can we review the action items?

JENNIFER BRYCE: Thanks. A couple of action items, first being that the team members should review the text that was discussed on the call today, and share feedback in one form or another to the team on the text that was discussed. And then, team members to complete their assignments based on their penholder list that was circulated to the e-mail last week. We'll recirculate for the draft recommendations text. That's all that I captured. Let me know if I missed anything. Thanks.

RUSS HOUSLEY: Sounds right to me. Okay, thank you. I think we're done, then.

UNIDENTIFIED MALE: Thank you.

JENNIFER BRYCE: Thanks, everyone.

UNIDENTIFIED FEMALE: Thank you.

JENNIFER BRYCE: Bye.

UNIDENTIFIED FEMALE: Thanks, everyone.

UNIDENTIFIED MALE: Thank you.

UNIDENTIFIED MALE: Thank you.

UNIDENTIFIED MALE: Bye.

UNIDENTIFIED MALE: Thanks, bye.

[END OF TRANSCRIPTION]