MONTREAL – Engagement Session with the SSR2 Review Team
Sunday, November 3, 2019 – 17:00 to 18:30 EDT
ICANN66 | Montréal, Canada

RUSS HOUSLEY: Okay, good afternoon, it's kind of weird having the bulk of the audience sitting behind us, but we have a fair amount of slides here, so I'm not going to read you every word on the slides, that would just consume the entire time and that's not the point, we want to hear from you with the end. So I'll go through them, there'll be up long enough for you to read them but I will summarize what's on them, not read them to you.

So, I'm Russ Housley, I'm the chair of SSR2, the bulk of the review team's here, but not all of us. The review team is mandated by the bylaws, there are four specific reviews that are and this is basically a work in progress, and so we're here to share where we're going. The review team is made up of these people, I have to say it's a hard-working group and enjoying working with these folks most of the time.

So, this is the process that the review uses and we're in the actually doing the review part, the grey boxes are after we produce a report. The team made a strategic decision and the slide talks to that; basically, the strategic plan has been put forward for 2021 through 2025, and we have made the decision that we won't make any recommendations that don't support one of those strategic objectives. We have divided our work into four chunks that we call Work Streams. The first one is related to SSR1, the review team that

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.

came before us, our job there is to look at the implementation of their recommendations and determine whether the intended impact happened.

The second chunk is to look at the SSR security stability, stability and resilience issues within ICANN and the third one is the SSR issues within the DNS, and the fourth is to look ahead at future challenges. So we have recommendations that have come out of each of these four buckets. We originally had a fifth bucket, to look at IANA because of a post-transition, and those that look resulted in no recommendation so we don't talk about it anymore.

So the first one is Work Stream 1. The summary is that SSR1 had 28 recommendations, we looked at those and 27 of them seem still relevant today and most of those were not fully implemented. So that is leading to a recommendation that basically says, "Go ahead and finish what you started," but we realized that some of the recommendations from SSR1 were written in a way that makes them hard to measure, and so we are offering guidance that would allow SSR3 to look at that and know whether it's been achieved or not, trying to provide a measurable solution.

In addition, we found that a couple of the recommendations didn't go far enough and so we are inheriting what they did and expanding on it, saying, in addition to what SSR1 said, we think these other things should be done and there's four of those, and the first one is related to SSR1 recommendation 9 on Information Security Management Systems and Security Certification.

We believe that ICANN should establish a roadmap of industry-standard security audits and certification activities that are going to be undertaken, put milestones in place, to achieve those, and then start a continuous improvement process. So basically, we think that the auditing and certification should be done along the lines of established industry security standards, and we're not mandating a particular one but we are pointing to ones that ICANN can take a look at.

The second one is actually a build on SSR recommendations 12, 15 and 16, which have to do with strategy and framework. We think that the security issues need to be clearly, publicly and promote security best practices across all of the contracted parties. So ICANN needs to work with the community to develop and continuously update an overarching SSR strategy and a framework and then capture best practices that go with those and then establish clear measurable, trackable objectives that are implemented in practices, contracts, agreements and MOU's.

We want that to include a vulnerability disclosure process that is reported at least annually, and the third one in this bucket is the Build on SSR1 recommendation 20 and 22, which is about budget transparency and budgeting SSR related things for new gTLDs, basically, it's very difficult to figure out which items in the budget are related to SSR activities, and we think that needs to be clear and tied back to that framework that we talked about just a moment ago, so that you can tell from the budget which SSR framework activities are tied to which budget items.

And the final one in this bucket of expanded SSR1 deals with recommendation 27, which is in Risk Management, we think that it would be appropriate to centralize and strategically coordinate the Risk Management Framework, and there are actually further things we're going to recommend in this area in a future recommendation.

So the second Work Stream deals with SSR issues with ICANN, and these are the parts of the bylaws that require that this work be done, and it leads to us making four recommendations. The first one is related to establishing a C Suite Security Position; basically, we're taking the responsibilities associated with a CISO or a CSO, establish a position like that, we're not mandating a particular title, but we think it has to be a direct report to the CEO and this person should be responsible for managing all of ICANN Org's security function overseeing the interaction with security staff and other areas and provide regular ports to the community and be part of the process for dealing with security-relevant contractual negotiations.

Flowing from that one of the things that C suite position will be responsible for is Security Risk Management and so this ties back to one of the SSR11, but we believe that the international standards in this area need to be adopted and followed to make sure that we have the Risk Management process that flows into Continuity Management and also flows in to Disaster Recovery and is tied in with the ISMS that we talked about in the SSR1 recommendations.

We think this person needs to be a dedicated, responsible person for the Security Risk Management needs to report to this person and the

Risk Framework Working Group and the SSR Framework that was previously established need to be part of the work that is handled here. What flows from that is a Business Continuity Management and that needs to establish a plan for IANA, to make sure there's business continuity there and it also needs to establish a plan for ICANN Org. Again, there are well-accepted international standards in this space and we think we they should be followed.

In addition, we think an external auditor should be engaged to verify compliance with those plans, and the final recommendation in this area has to do with Disaster Recovery Planning, again, we think there needs to be Disaster Recovery Plan for PTI, in terms of the IANA functions, there needs to be one for ICANN work and, again, they are established, well respected international standards, let's follow them and in addition to that, we think you should have a practice, make sure that they work, and again audit to verify compliance.

The third Work Stream is the SSR for the DNS. This is the biggest work product section and these are the areas where we have recommendations. This is the abuse definitions and reporting has two parts to it, the short term and the longest term. The short term is basically we encourage ICANN to implement the CCT review and RDS review recommendations regarding this, and we, on the longer-term, think that the community needs to be engaged and take a look at the definitions for abuse.

If you're paying attention to what's going on around the organization that's already started, but we think that the ICANN Board should entrust the SSAC and the PSWG to work on e-crime and abuse related things, pull experts from that area and take into account the process from the conventions on cybercrime. Once this is done, we want to minimize the ambiguous language that is used today. Once we get all these definitions, and we've got a community agreement to them, let's make sure that we're all using them.

The second area is DAAR. We believe that the board and ICANN Org need to work with the gNSO, ccNSO, CCT at least to improve DAAR and incorporate more CCT data into that tracking and reporting. We need to identify entities that are persistently on the high end of the scale there, and basically, we want to publish a report that identifies those so that we're all aware of what's going on, and we think those reports need to be in a machine-readable format so that it's easy for people to use.

Contracts and Agreements. This is an area where we want to incorporate measures that are mitigating for DNS abuse and security threats. Those are terms that are already defined now, but the definitions of course, that we talked about, two slides ago, will probably alter that, which would flow into this. We want to have the SSR requirements become mandatory in contracts and baseline agreements. We want the SSR concerns and these recommendations to be part of negotiations. We want to attract the ccTLD community into adopting these mitigations and we think the board, the community and the staff need to work to advance the tracking and reporting in that part of the community as well.

Incentives. We think that it's appropriate for ICANN offer incentives with contractor parties for implementing the mitigations, related to abuse and security threats and oppose these changes unilaterally and immediately. The want to incentivize the early takedowns when problems are found, and we want to institutionalize training and certifications for all key stakeholders in this area.

Abuse Report Portal, we want a single place to do this. One way for everybody and to offer a complaint and all complaints get automatically redirected to the abuse for the relevant party to handle it and we think it should be mandatory for all gTLDs and we should encourage ccTLDs to join in.

Compliance Function. We believe that ICANN Org's compliance activities need to be neutral and effective. We want to make sure that all of the activities of this function are audited and they need to be held to a high standard. The board needs to empower the compliance office to react to complaints that require compliance to initiate an investigation or enforce a contractual obligation. Those should be defined in the SLA, and we want the compliance office to provide enforcing and reporting clear, efficient processes and fully informed complaint, measure the satisfaction and to the greatest extent possible, we want the way they work and handle things to be publicly available.

Abusive Naming, we want to build on current activities here that deal with investigating misleading naming. It's when things rise to the level where misleading naming becomes an abusive name. We want to include that in DAAR reporting and we want to develop policies to mitigate that practice. We want to measure the number that gets complaints to the portal we already talked about, and we want that information to be available to third parties to help analyze, mitigate and prevent harm from such things. There's been a lot of work, especially in IDNS regarding this and we want to take advantage of that but we also want to take a look at places where hard to spot typos, and other things are being used to mislead and so this really applies both to asking names and to IDNS.

DNS Testbed, we know that there's work underway to develop a testbed and we want that work to continue and complete, so the DNS regression testing can be done and we want to perform functional testing with different configurations and different software versions to identify SSR related problems.

DNSSEC Key Rollover, we want to establish a formal procedure for the rollover itself. We want it done with a modeling tool, using language that will specify decision points and exception legs and the full process control point. We want to do a verification of that model and make sure that it's out there for everyone to review and publicly comment on and then we want to go ahead and stage that and use it as a tabletop exercise to make sure that the whole process is well understood and all the parties that need to be are involved in informed.

Root Server Operations, we would like to see baseline security practices, best security practices developed in close cooperation with

RSSAC. This should include change management verification procedures or sanity checks, and then we'd like to see L-ROOT basically take the lead and lead by example, develop key performance indicators to measure these best practices and share with the rest of the route server operators and other relevant parties, and we'd like to L-ROOT again leading by example, to develop a vulnerability disclosure process and communicate with researchers and RSSAC whenever they can.

Root Zone Data and IANA Registries. We want to create a list of statistics and metrics for each of these databases so that we can track them and understand their availability and responsiveness. We would like to see this data put available to everyone, put on the ICANN website, perhaps under the Open Data Platform, again, key performance indicators, so that we can illustrate the baseline activity over time and we would encourage this to feedback from the people who are consuming it on an annual basis so that we can make sure they're getting the information they need.

The fourth Work Stream is about the future. We have five areas here. First one is Cryptography. PTI should update the DPS to facilitate the transition from one digital signature algorithm to another. This presently only covers key rollover with the same algorithm, but we think that we will be transitioning either from RSA to ECDSA or from RSA to some future post-quantum algorithm, depending on the time frame, we actually do it. So we need to address how to do this in that document, and then we think that there should be a consensus plan for that, as well.

Name Collisions, we need to characterize the nature and the frequency of these collisions and we know that the name collisions was an issue with the last gTLD round, so we want to make sure that that work is done before there's another one, and we think that ICANN should support an independent study of the name collisions, eventually, to adopt an account for the implementation or the non adoption or the recommendations from that study. We should like to see the whole thing published, start dates and dates and so on and we think that the NCAP should finish the work that they have started in three areas.

Privacy, the font got to get pretty small to put this all on here, but basically, we think that an organization needs to be stood up to that specializes in the privacy aspects, focuses on understanding privacy requirements and principles and facilitates law enforcement needs to WHOIS information, make sure it's worked with the community and that's basically the role. There are lots of aspects to it to make sure that PII is protected and this is, of course, an area where laws and regulations are evolving.

So we need to make sure that those specialists are tracking it, keeping us up to date, highlighting where other work needs to be tackled. We think that doing that more proactively and following instead of a fire drill, when due stuff shows up was the right way to go about it and we need to cut out the periodic audits to make sure that's all happening.

We think that it'd be beneficial to the whole community to take a look at peer-reviewed research. We list some of the forums where that kind of research is being published. Naming Systems and DNS often come up in these venues and then when there is something there that's actionable, that should be brought forward to the rest of the community with an action report.

And DNS over HTTPS or DoH enables applications, vendors to choose a resolution infrastructure, regardless of how the system is configured that it's running on. This allows vendors to, on an application by application basis, override the choices that administrators or users have made in terms of which DNS resolution infrastructure will be used, and can also selectively enforce the DNSSEC. So we think that we should have a commission investigation into the adoption of this, with particular attention to regarding the resilience impact that this might have on the DNS ecosystem and the security concerns that that protocol enhancement brings. This is our most recent work and so I added a point here that one is still under active discussion within the review team, but at the same time, I wanted to share it.

Wrap up; so in addition to these recommendations, we're putting forward a few suggestions. I did not want to walk through them because they are not SSR related, what they are, is sharing some experience from going through this review process and their suggestions that will make it easier for not only future review teams in the SSR space but all specific review teams. So we are going to put those together kind of has a lessons learned and they're suggestions, not recommendations, so as to not mix the two.

And thank you and I think we have plenty of time for questions, which I'm pleased about. That was a whole lot of drinking from the firehose there. What we have done with the slides is the bullets that I use to summarize them are there and then right behind each is a hidden slide that has the full draft text associated with that recommendation. So if there was one of those that really piqued your interest and you want to see more about it, the full text is there in the slides when you download them. So, if there are any questions, please come to a microphone.

MASON COLE: Hi, my name is Mason Cole, I'm with the Business Constituency. I'm interested in the incentives that you outline for helping contracted parties deal with abuse. Could you talk a bit more about some of the fine level detail maybe that went into that recommendation?

KC CLAFFY: So we'd like to hear suggestions of the details on how you think it should be implemented or others. I can outline some of the potential details that are under discussion, but we'd really like to hear reactions and thoughts from people in this room. So the background for this is that there have been occasions over the last several years where ICANN staff has unilaterally changed the fee structure to incentivize particular actions; domain tasting is one of the more famous ones and so, we're recommending that this be done for DNS abuse and security threats as well.

So one suggestion is that the contracted parties with portfolios that have less than a specific percentage of abuse in their portfolio for example, 1% as identified by commercial providers, and or the DAAR statistics receive a fee reduction. So it could be a reduction from current fees or ICANN potentially could increase current per domain transaction fees and provide a registrar that meets a low abuse threshold with the discount.

We're also discussing that registrars receive a fee reduction for each domain name registered to a verified registrar to another incentive, up to an appropriate threshold and are also discussing our RSSAC fee reductions, where the RSSAC involves verified registrant and other activities to help mitigate DNS abuse.

In addition, we're discussing that ICANN Org should incentivize the mitigation of abuse and security threats, by refunding fees it collects from registrar's and registries on domains that are identified as abusive or security threats, and are taken down within an appropriate period after registration. So those are actively under discussion and would be great to get additional input on that and other things.

KERRY-ANN BARRETT: This is Kerry-Ann, one of the things that we're discussing why the full text is not there is that we want to ensure that safeguards are built into such an incentive program because you don't want to be abused as well. So one of the things that the team has been debating is how much information or suggestions should we give because, at the end of the day, it has to have a full assessment and evaluated to make sure that the incentive program is not one that will create more harm than they go that were intended. So it's really to see what the community thinks about such a scheme and if it could work, how to ensure that we balance it for the sake of the public interest.

MASON COLE: Well, I'm no longer with a contracted party, I used to be with contracted parties and I recall that when I was with a registry, that beyond the cost of labor, our ICANN fees were the most significant expense we had as a business. So I would think it would be attractive to use ICANN fees as an incentive to help keep your namespace clean, both on the registrar-side and on the registry side. So I think actually, I think that's a very good idea, I would encourage consideration of that. So are these going to be brought up at the DNS abuse session on Wednesday?

KC CLAFFY: We haven't actually thought of it, weren't planning on it. Is that something that you think would be useful?

MASON COLE: I do, yeah, I think the more robust conversation we can have about abuse, the better.

KC CLAFFY: Yeah great.

MASON COLE: Okay. Thank you.

DREW BAGLEY: Drew Bagley from the CCT Review Team. I just wanted to applaud all of you on your efforts and your hard work. I think your recommendations really look like very effective recommendations from the vantage point that I saw through the work on the CCT Review Team looking at some of the overlapping issues.

And so the original recommendations you put forth really look fantastic, but additionally, the complimentary recommendations you put forth, I think really have the opportunity to improve upon the CCT Review Team recommendations and it looks like there's consistency amongst the two review teams, and following an approach to both incentivize good behavior, as well as create mechanisms in place to take away excuses to do nothing about bad behavior.

And so from the dialogue we've had over the years in the community, we've obviously seen excuses first gravitate around definitions of abuse and complaints, there's no definition and so there's now consistency amongst the community as a whole looking at consensus from several years with regard to security-oriented DNS abuse, and now amongst two review teams in a row, and now we're seeing that even from the contractor party, so I think that's terrific to really see that and then see that you guys are also addressing the complaints about there not being, you know, a means for high care compliance to do something.

So I think this is very consistent with what we saw through our own research and I think the recommendations look great, I really hope that the rest of the community reacts positively as well, because you know, what as Mason was suggesting, you know, we all know this is a cost to the contracted party, so if we can provide incentives such as financial incentives, to do good things, I really think that should take off, so I applaud you for your efforts and thank you so much for the hard work.

RUSS HOUSLEY: I guess in short, we are trying to be good stewards of the namespace.

KC CLAFFY: And while you're here, Drew, any news on the majority of the CCT review recommendations that the Board paused?

DREW BAGLEY: So there's no real update other than the Board has now released, as I'm sure you all saw, the Draft Implementation Plan, and then had a public comment period for that. We've been actively engaging with the Board throughout the past year since we first put out our final report a year ago and then since the first Board Resolutions came out in March.

And so one of the things that we've consistently pointed out to the Board, and continue to point out, is that for the recommendations where the Board has posited that there needs to first be a definition of abuse before implementing them we've pointed out that we already created and supplied that definition and that we didn't make that definition up and said we based off of a decade's worth of community work and community consensus. So our hope is that particularly after this public comment period we'll see some movement on that but there's no update on that.

Wendy Seltzer: Thank you, Wendy Seltzer here, and I have two comments, distinct parts of the work one is following up on the discussion of abuse. I want to share the caution from my work with the Chilling Effects Clearinghouse that abuse reporting can be abusive also and that ICANN has in the past carefully stayed away from the content regulation side of monitoring for abuse, and I think it's very important that we do that here too, and that the incentives should not be to monitor what goes on behind a domain name or the ways that they're being used but looks only at the names themselves and that we rely on other mechanisms outside of ICANN to continue the fight against abuse that happens through content.

And then my second comment was in the last bullet you had on investigation into DoH and I think that that's a very good area of investigation for the protection of security and then user privacy, and so from the end-user person perspective I think that there's a lot that's positive in the potential of DoH to encrypt the DNS queries and provide protection against the inline snoops who might be seeking to see that as it's otherwise going in plain text and so while it's true that some implementations could take control away from the end user, better implementations would give more control to the end user, allowing the end user or the enterprise managing the end users computer to direct the DNS traffic in a way that is both secure from snooping and under control of the user or the users organization. So I think looking at that technology and the ways that users can improve their security could be a helpful perspective.

RUSS HOUSLEY: We agree and on the review team, we've been talking about two different implementation approaches we've already seen in the wild. One that’s kind of helpful in one that's kind of not, and are concerned that we get more data about which direction actually gets used.

SUSAN KAWAGUCHI: Hi, I'm Susan Kawaguchi, thank you for all the hard work. Obviously, the recommendations have taken a lot of thought and a lot of review, and I'm also a member of the RDS Review Team, which you know, we finalized our report a few months ago. One of the things we found, which I think you've recognized also, probably more in-depth was that the need for those metrics and to really be able to understand what is going on.

There were several, you know, somewhat recent policies that had dealt with the WHOIS that no metrics were being collected, no one had any idea if the intended consequence of the recommendation from previous either PDPs or review teams, had at once implemented had actually had the result that we were looking for originally.

So we need those metrics. We need some sort of analysis done, the review and the reporting to make sure that, you know, we could decide as a community, “Oh, wait, this isn't what we intended,” but if you don't have the metrics to know if it's actually doing something, then it's very hard to review things. So that is one of our recommendations is to include, make sure all that data is collected somebody's looking at it reviewed and analyzed. So I appreciate that we're all on the same vein on that one too.

UNKNOWN SPEAKER: Yeah, yeah, we spent a lot of time talking about the need to have data and when it's not even always clear exactly what you're going to need it for, but taking conscientious measurements and ensuring that regardless of who's taking them specifically and for what reasons that they are preserved in they're available so that longitudinal analyses down the road can benefit from the fact that conscientious measurements were taken in the past. So yeah, that was one of the big themes that I think we've kicked around on the team a lot. Sounds like we're on the same page there.

RUSS HOUSLEY: I'm not seeing anyone else head towards the microphone. I'm kind of surprised we're wrapping so quickly. Going once, going twice. Okay enjoy the week.

[END OF TRANSCRIPTION]