
JENNIFER BRYCE: Okay Russ, over to you.

RUSS HOUSLEY: Thank you. Okay, welcome to the SSR2 Public Comment Webinar. Just want to start by saying, we've been working for awhile and have a document that's out for public comment. The URL is on the screen to tell you where the report can be found and where the public comment page is. The point of this presentation is to give you a feel for what's in the report, not anymore than that. The idea is for you to get a feel for what's in it and where to find the topics that are of interest, so that you can participate in the public comment.

In doing our work, we divided the working into four workstreams, the first three workstreams are mandated by the ICANN bylaws. The first one is to assess the implementation of the SSR1 implementation and make sure it had the intended impact. The second workstream is about SSR related issues within ICANN. The third one is SSR related issues within the DNS. The fourth one is an optional item within the bylaws, which is to look at future challenges.

These are the people on the review team who did all the work.

The review process is here. Basically, we've assembled the team. We've planned the review. We've conducted the review and we're at the end of that phase. The draft report is out for public comment, that will end on the fourth of March. Then the review team will convene in

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.

Cancun to process the public comments and the result will be a final report that goes to the Board for the next step.

In terms of setting the prioritization related to each of our recommendations, we conducted a survey among the review team. You can see the scatter plot of importance verses urgency that the team members came up with each of the recommendations. There is clearly two chunks but the team, as part of the process, eliminated all of the recommendations that did not tie, in one way or another, to the strategic plan for ICANN, so it's not surprising that the importance and urgency are both fairly high for all of these chunks. As a result, the ones on the lower left got labelled medium and the ones in the upper right got labeled high.

Now I'm going to very briefly walk through each of the recommendations in workstream order. The first one is an assessment of the implementation of the SSR1 recommendations. We evaluated all 28 of their recommendations and felt that 27 of them remained relevant today but they were not fully implemented so as to cause intended effect.

The first recommendation is to finish the implementation of the 27. In addition, there are seven that we felt we wanted to say more about and so those resulted in a few additional recommendations. You can look on page 23 to see that part of the recommendation in our report.

The first one we wanted to say more about is recommendation nine. We felt that ICANN Org should improve its approach to security

certifications and audits. That's a stretch beyond the original SSR1 recommendation. You can see more about that on page 23.

This one builds on SSR recommendations 12, 15 and 16 and calls for a strategy and framework and metrics and vulnerability disclosures basically issues, we're calling for best practice for handling security issues. You can learn more about that on page 24.

This one builds on SSR recommendations 20 and 22, which calls for budget transparency and budgeting SSR related to new gTLDs. We just are calling for additional clarity around the SSR budget. It's quite difficult to look at the budget now and tell whether a particular item is related to SSR or not and that's the big ask here. You can learn more about that on page 24.

Recommendation 27 from SSR1 was about risk management and we called for an improvement to the risk management framework. You can learn more about that on page 25.

Now, we're entering Workstream 2. We are calling for the creation of a position that's responsible for security and risk management within ICANN. We believe this person needs to report directly to the CEO and be focused on these security goals. We talk about that on page 27.

Within the function that would report that C Suite position is where recommendation seven falls and that's to further develop a risk management framework. Here they believe that the right answer is to follow ISO 31000 to articulate those risk management approach being taken. That is on page 28.

Again, with the organization that reports to that C Suite position, we think we need to establish a continuity of business plan, based on ISO 22301, basically calling for the establishment of a best current practice for both ICANN and for PTI operations and that that plan should be audited regularly. You can learn more about that on page 29 and 30.

Again, falling in that purview of that C Suite position, we believe that we need to deal with disaster recovery and we're calling for a plan, again that covers ICANN and PTI regarding disaster recovery, following ISO 27031. Again, we are asking that that be audited regularly. That is on page 30.

Recommendation 10 is the first one in Workstream 3. Here we're calling for improvements of the framework to define and measure registrar and registry compliance, focused on WHOIS obligations. Basically, we're looking for SLAs in the contracts. Here you can learn more about our thoughts on pages 37 and 38.

Recommendation 11. We believe that the community needs to come to a better definition of DNS Abuse, however, we're very concerned that we don't want things to stop while this definition is sorted out. Basically, we want to start the existing definition and continue community wide efforts to define the term. We have other recommendations regarding DNS Abuse, and we want those to move forward with the existing definition while this recommendation is implemented. You can hear about that on page 38.

Recommendation 12. We want to create legal and appropriate access mechanisms to WHOIS data, to resolve the access issue for external

parties such as law enforcement that are -- basically these groups are throttled today and we want to -- you can read more about that on page 39.

Recommendation 13. To improve the completeness and utility of the DAARP, which is the Domain Abuse Activity Reporting Program. We think that while things are going well there are things that can be improved. You can read about that on page 39.

Recommendation 14. To enable qualitative analysis of the relationship between payments for domain registrations and the domains that have abuse. We think that collecting, analyzing and publishing the pricing data would allow that kind of an analysis to take place. You can read more about that on page 39.

Recommendation 15. We believe that the contracts with registrars and registries should be changed to include incentives to help mitigate DNS Abuse. We talk about that on page 40.

Recommendation 16. Is closely related to the previous one. We think there should be pricing incentives for contracted parties to help mitigate DNS Abuse and security threats, such as distribution on malware. Again, we want to offer incentives to support these SSR goals in contracts. More about that on pages 40 and 41.

Recommendation 17. To create a central abuse report portal. Basically, we found that a lot of people don't know how to report abuse because there is so many different ways, depending where the domain name is registered. We recommend a single point to do that. While we recognize that this has some consequences related to denial of service,

we felt that having no easy way to report the abuse was a problem but that it would be okay to say, “No action needed.” To such a report when it’s being used as a vector of DDOS. More about that on page 41.

Recommendation 18. To ensure that ICANN compliance activities are neutral and effective. Basically, we want to audit all compliance activities against appropriate SLAs. More about that on page 41.

Recommendation 19. To update the handling of abusive naming. We want to continue activities for the definition as I said earlier but we want to measure misleading naming and when such activities should also be included in DAARP when they reach the level that you might call them abuse. More on that on page 42 and 43.

Recommendation 20. There’s currently a development of a DNS regression test suite underway. We think that the work that has been started needs to be finished pretty quickly. Page 43 for more on that.

Recommendation 21. To implement the recommendations that are SSAC 63 and 73. To establish formal procedures for key rollovers. We think that a very formal process is needed here. You can read more about that on page 45.

We’d like to see some baseline security practices documented for root server operations, including recommending some key performance indicators. Obviously, we think RSSAC should be involved in that work. More about that on page 46.

In Recommendation 23, we believe that we should increase the urgency around deploying the new root zone management system. We know

that it's under development, but we think there's some important features that are coming along in that. We've also highlighted that we think two factor authentication needs to be implemented as part of that. That's all on page 47.

Recommendation 24. We'd like to see a list of statistics and metrics around operational status of the unique identifier system created and made public. That's discussed on page 48.

Recommendation 25. Ensure that the centralized zone file data access is consistently available. Basically, we're saying implement SSAC 97. More about that on page 48 and 49.

Recommendation 26. To document, improve and test the emergency back end registry operator processes. We're aware that these have been tested twice. We think they should be tested regularly. More about that on page 50.

Recommendation 27. To update the DPS, which is related to the crypto used in DNS SEC, so that in addition to having the algorithms in the document but it talks about how to roll to future algorithms. We believe that either a roll to elliptic curve or a roll to a post quantum secured digital signature is in the future so we think that this document should be developed to accommodate that. More on that on page 53.

Recommendation 28. To develop a report on the frequency of name collisions and propose a solution. We think that needs to be done before the next round of gTLDs. That's on page 53.

Recommendation 29. To provide a focus on privacy and SSR measurements for improving those. Basically, we're asking to look at these new technologies, such as DNS over HTTPS, figure out how to measure compliance with privacy requirements when they are used.

Recommendation 30. To stay informed about academic research related to the SSR issues within ICANN and the DNS. This recommendation includes a list of conferences where peer reviewed research gets published, is related to those topics and we think when something surfaces that's useful, it should be reported out to the whole community. More about that on page 57.

Recommendation 31. Also related to DNS over HTTPS or DOH. We think it's important to have a independent study commissioned around the implications of its widespread adoption. You can read more about that on page 58.

That's the end of the recommendations but I wanted to highlight a few other things that are in the report. There's definitions, acronyms and suggestions, those are not recommendations about SSR but they're about making future reviews easier to complete, there's three of those. We explain our process and methodology. We moved the detailed findings related to the implementation of the SSR1 recommendations to an appendix to make the body of the report more focused.

We quoted the text from the ICANN bylaws and the strategic objectives. As I said earlier, we already made sure that each recommendation was focused on a strategic objective or goal, supporting which strategic objective is back there. We have some research data about DNS Abuse

trend back there as well. How the workstreams line up with the bylaws is back there as well.

That's a brief summary of what's in our draft report. Pointers to where to learn more. Please participate in the public comment. If there's any questions, I'll take them now. I see ah and from Geoff Huston.

GEOFF HUSTON:

Thanks, Russ. Certainly, is a lengthy report and it's no doubt the SSR3 Review Team did a lot of work. I have two questions. The first, are you of the opinion that the review report adequately motivates each of these recommendations within the body of the report and adequately describes the intended benefits where these recommendations to be adopted?

RUSS HOUSLEY:

Well, I don't know about -- adequate is an interesting word to pick. I think it depends who your reader is whether it does that or not. I think that there are motivations. We tried very hard to look forward to SSR3 having to evaluate the implementation of these recommendations and we tried to make sure it would be easy for them to measure whether the implementation was successful or not.

Then had the intended effect part is always the harder part, so we tried to say enough about why we wanted it done to do that. We think we met what you were saying for informed reader. If one of your comments is, please put more in there, then that seems to be then implication from you asking the question.

GEOFF HUSTON: I'll move on to the second one. One of the things that I noticed was that there was little comment about areas where the ICANN Organization, the community were doing an effective job. My question is, is such an omission from this review report, to be interpreted by the reader as comprehensive condemnation of the current setup?

RUSS HOUSLEY: No, I think it was more a coordination would make a much easier job for everyone involved and for others to see SSR3 and anyone else who chose to look, that is more how I would take it. I see Laurin, one of the review team members has his hand up, I bet he wants to add.

LAURIN WEISSINGER: On I think the first question and to some extent the second. We did discuss obviously as a review team would want to kind of go into that, the comment period and went for a time where I think the majority of the team felt, now is a good time to get some feedback, to learn what the community thinks and to still be able to deal with substantive comments. Exactly, stuff like you mentioned makes sense to be reflected.

Speaking now from my personal point of view, I do see how in quite a few cases, this needs to be made more clear, we probably do need some additional guidance, some additional explanation for the final report but again, right now is great chance to do that and to say, "There

is stuff that is missing and that really needs quite a lot of additional words.” For example, going to the second part of your question.

GEOFF HUSTON: Thank you to both of you for your answers.

RUSS HOUSLEY: I do want to build on one thing that Laurin said. We did have a fair amount of discussion about how polished the report needed to be before we sent it out for public comment. While the majority of the team felt that it was good enough at this point to understand whether the community was happy with the direction we were going, I don't think anybody thought it was okay if this version went to final. If that helps, that's where we are.

GEOFF HUSTON: That's most helpful, thank you.

JENNIFER BRYCE: Russ, there's a question in the chat from Maxim, which I'll read out, actually two out, I'll read them both at the same time. What is the reason to believe that usual, each five minutes, testing of all active registry backends by most [inaudible] of ICANN is not enough? Second question; were legal experts invited for forming recommendations to amend legal documents of registries?

RUSS HOUSLEY: I'm not sure which part of the report the first question was about. Regarding the second, no we did not have a lawyer on the team, and we did not at this point ask a lawyer to review that. At the same time, we know that there is a long process to get those agreements through a community process and then actually negotiated and implemented but I think that what have provides a direction for that. Regarding the first question, did she post a follow-up?

JENNIFER BRYCE: No follow up as of yet but Zarko has his hand raised.

RUSS HOUSLEY: Zarko, go ahead.

ZARKO KECIC: I believe I understand what Maxim is talking. Russ was talking about emergency operators not just backend operators. It should be tested all the way from escrow services, how they transfer, what are policies, procedures, how emergency back end operator is ready technically to accept the data and how fast they can go on. I believe that answer her.

RUSS HOUSLEY: Thank you for understanding the question. Yes, when we did that work, we found that it was multiple days for the emergency backend provider to come online. Laurin, you have a hand.

LAURIN WEISSINGER: Yes, it is regarding the contracts. Just to add to what Russ already said. We do have people who are on the team, we didn't look at this in that manner because this will go through a million processes as Russ said. I think what is key to us going into that direction is, if you look at the letter sent by Jamie Hedlund after the Alp names incident, which I'm sorry I can't pull out right now, it's 5:20 am where I am.

Essentially, what that letter said is, there's no provision in the contract that deal with such type of events. If you look at the contract, you see that it's correct and we do see that as an issue, particularly when it really goes to the extent we saw in that case. Obviously, this is not for us to deal with the specifics because this will go through community and a variety of relevant processes. I think there is something on contracts.

Yes, Maxim, I'm just responding to the comment as well, which is change contracts leads to issues in the real life. Yes, that is correct and that needs to be done. What we're saying is do change them, there is a gap and we're not defining how that should happen because that requires someone who knows what they're doing and also a significant amount of time because these contracts have different run times, etc.

RUSS HOUSLEY: Geoff, I see a hand.

GEOFF HUSTON: I do have a third question that's come to me as I've reading through this document thoroughly. On a number of occasions, this report effectively repeats existing SSAC recommendations to the Board and says the

Board should pay attention to these. Why are these particular cases called out? Why does the report not say what appears to be the most obvious thing? Is not the case that the review is saying, the Board isn't paying sufficient attention to its advisory committees?

If that's really what you meant to say, why didn't you say it? If you really did want to say, you should pay special attention to these particular recommendations from SSAC, are the rest of them all rubbish? Why call out just those? I'm trying hard to understand the specifics.

RUSS HOUSLEY:

There was no intent to say the others are rubbish. There was an intent to call out these as the way to solve the particular problem that is being discussed there. In some cases, for example the CCT Review called out the same recommendations related to reasons that they had in their report, we did not go through an point out every place that others had made the same recommendation but at the same time we thought if somebody else has already the work, let's point to it as opposed to write all that down in here in terms of the details. Maybe I guess we were trying to use shorthand where we could.

GEOFF HUSTON:

I'm not suggesting that, Russ. What I'm saying I suppose is, these other groups already given this advice to the Board, if this review felt it was worth repeating and I supposed I'm sort of left with the conclusion that I draw, going, the only reason you think it's worth repeating is because

it doesn't seem like it's being listened too but that's not in the report, you don't actually say that.

RUSS HOUSLEY: In some cases, things have moved but not moved fast enough. I guess what you're calling for is a distinction between those cases where the advice was given, and the needle didn't move, and advice was given, and the needle moved a little but not fast enough or far enough.

GEOFF HUSTON: I think that would be the more helpful thing because it's not the advice, it's kind of what's going on with, which is really the question for everyone, not only for the SO and AC's but for this review report and I think it will be more helpful if you added some more text about what you felt about why you felt the need to repeat them, rather than just repeating them.

RUSS HOUSLEY: That's a good question and certainly one that actually was not a discussion of the review team to date. It sounds like we're going to have an interesting discussion in Cancun.

GEOFF HUSTON: Thank you.

RUSS HOUSLEY: Please put that in the public comment.

GEOFF HUSTON: It will be there, thank you.

JENNIFER BRYCE: Russ, I'm going to read another question in the chat from Yazid it's, when stating that 27 of the previous recommendations are still relevant, I would like to understand what are the reasons and also, was there any suggestion from SSR1 on the estimated duration to implement those previous recommendations?

RUSS HOUSLEY: Yes, if you go back and look at the SSR1 report, some of them did have timelines associated, due by or due before, those kinds of things. But what we found, was with that one recommendation, that it just -- remember that SSR1 was done before the IANA transition and that one just didn't seem to still be relevant today.

JENNIFER BRYCE: Thank you. There are no other questions in the chat, and I see no hands raised at the moment.

RUSS HOUSLEY: Okay, then thank you so much for your time. I hope this has been helpful in terms of pointing you to topics that might be of interest. Thank you very much, we look forward to your public comments.

GEOFF HUSTON: Thanks all and good night, Russ.

RUSS HOULSEY: It's very early morning here.

[END OF TRANSCRIPTION]