JENNIFER BRYCE: Good morning, everybody. Welcome to the SSR2 meeting face-to-face in Los Angeles day two. Today is the 26th of January. My name is Jennifer Bryce, ICANN Organization. Let's go around the table to my left.

NEGAR FARZINNIA: Negar Farzinnia, ICANN Org.

NORM RITCHIE: Norm Ritchie.

DENISE MICHEL: Denise Michel.

BOBAN KRSIC: Boban Krsic.

MATOGORO JABHERA: Matogoro Jabhera.

RAMKRISHNA PARIYAR: Ramkrishna.

ALAIN AINA: Alain Aina.

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.

LAURIN WEISSINGER: Laurin Weissinger.

KC CLAFFY: KC Claffy.

ERIC OSTERWEIL: Eric Osterweil.

RUSS HOUSLEY: Russ Housley.

JENNIFER BRYCE: Thanks, everyone. At this time, we have no remote participants and no observers. Brenda Brewer from ICANN Organization is online. And with that, please remember to state your name into the microphone before you speak for the recording. I'll pass it over to Russ. Thank you.

RUSS HOUSLEY: Good morning. Welcome back. I wanted to start with a reminder that when each of us joined the review team, we put a statement of interest in. Please take a look at that and make sure that it's still current, you haven't changed employers or have new conflicts or anything like that. Just to make sure that all of that is up-to-date. If you need to update it, please give it to Jennifer or Negar.

This morning we're going to focus on DNS SSR. We're going to start off with a brainstorming session that Eric is going to lead. He sent a list of topics that we're going to brainstorm about and determine whether those are the right big buckets and we want those big buckets to not have a lot of overlap. Then, we'll break up into groups to discuss each one of those topics and see which things we ought to study, what information we need to do that, who we need it from, which team member is going to get the information to put it all together.

So, right before we broke up yesterday afternoon, Eric went through the current list, which is just to start the brainstorming from, and I hope that planted some seeds for you think about overnight. So, at this point, I'm going to turn it over to Eric.

ERIC OSTERWEIL: Thanks, Russ. Okay, you're pulling it up. So, we're waiting for the … Awesome. Cool. So, Jennifer just brought up the list on the Adobe Connect screen.

So, I guess what I'd like to do is I'd like to go down the list one at a time really quickly and see if we can get on the same page about what this list should have in it and should not have in it. Once we come up with a candidate list, I'd like to cycle through a handful of breakout sessions on it.

What I'd like to do is, looking at the clock, it looks like it's 9:06. So, I'd like to spend no more than 20 minutes on this first round, talking about what the right starting point is for the list of topics that we'll brainstorm here. This is a good time for people to take a good look at what's up there – there we go. For everyone to take a good look at what's up there. And I'll go one at a time through them, unless anybody wants to jump in with a starting point objection or acceptance. I see Denise.

DENISE MICHEL: Neither. Just an elaboration to remind people how we came up with these categories of ICANN SSR, DNS SSR, and the future. Those are the three that we're working on. As we discussed yesterday, ICANN SSR is … ICANN has full or majority responsibility for the activity DNS SSR, the big buckets. Please correct me if I'm misstating any of this. That contains things that ICANN has a partnership role in or it significantly impacts and is connected to activities that are within ICANN's remit and then future is [inaudible] title [inaudible].

ERIC OSTERWEIL: Thanks, Denise. Does anyone have any thoughts or comments before we move forward? Seeing no indication … I'm not monitoring the Connect room, so if there's a hand in there—

MATOGORO JABHERA: It would be on top of that [inaudible] of the fact that we are going also through this. It could also be good to see on the previous exhausted [list] that was prepared on the DNS SSR, if I remember from the Madrid, that has come up to this point. So, that we will all be aware on where we started, as Denise said, and on the current list we have. Thank you.

ERIC OSTERWEIL: So, do we have that list? That was a long time ago and I'm not sure. I see Jennifer nodding.

JENNIFER BRYCE: Yeah. So, there was a list that was initially developed I think back in Madrid and then I know that … I think KC and Eric, you guys did some iteration of another document as well maybe around October in Barcelona. Is that correct? Anyway, I'll put up the initial.

ERIC OSTERWEIL: Okay, Jennifer is searching. She's found it. We're taking a second and ingesting. Okay. Yeah. I definitely remember the SSR2 work stream topics Google Doc that you just – one of the ones you just posted, Jennifer. Thank you. That one, in looking at it, does contain some things that did not make it into the current draft of the Word document that you just put up a second ago on the screen.

My two cents is that we're here face-to-face. This is sort of precious time for high throughput. So, I propose that these things that are on the current ones being shown which is the old document, SSR2 work stream topics we did some time ago. Take a look at those real quick and those that resonate with any of you, I think keep them in mind. Then I'd like to go back to the more recent document and let's keep these things in our mind and we can use those in stickies or make categories if there's no category for them or something like that. So, thanks, Mr. Matogoro, for bringing our attention to that.

So, back to the high-level buckets. Again, these are just starting points. So, in the event that we want to change them, this is the right time to do it. I'm going to bound this conversation for 20 minutes from now, so at 9:32 we'll be done and we'll move on to the next thing.

But going down the list, I'll just read them out. Hopefully, you all are looking at the document or whatever works best for you. This is a good time for us to decide if we're going to go forward. This doesn't have to take 20 minutes. If there's silent acceptance, I'll take that.

So, root KSK rollover. In there, I suspect there are a number of issues to the extent to which we think it's a relevant topic for the DNS SSR, so I'm not asking us to blow them out now. Does anybody think that that's not a good topic to include in the DNS SSR work stream? Alain, are you … I see you pawing the mic.

ALAIN AINA: I guess I was activating my mind so that I can … So, I think that we should look at the root KSK management function IANA [inaudible] as a whole, not only look at the KSK rollover which is one of the activities inside the key management. So, we should look at that key management [inaudible], and inside then we can [inaudible] to the key KSK rollover.

ERIC OSTERWEIL: Okay. I have Boban, then Norm, then I have Russ.

BOBAN KRSIC: Alain, just for clarification, do you mean with that that we take only work on the key management itself [inaudible] or what do you mean with [as a whole]?

ALAIN AINA: Okay. What I mean is if you look at the root zone [DNSSEC] has a component that [inaudible] zone signed key managed by [inaudible] at the root zone maintainer and the KSK managed by the root zone [inaudible]. Okay.

Then, for us, what we are covering here is the KSK part which is the [inaudible] what IANA does. With that system, [inaudible] KSK management, the whole system has rollover responsibility, key ceremony, etc., key generation up to [the key rollover].

So, for me, the key rollover is just one [inaudible] activity inside that key management system so that [inaudible].

NORM RITCHIE: I just want to agree with Alain. I find that a bit too granular and it's really about root zone management and operations [inaudible] – administration, sorry.

ERIC OSTERWEIL: Okay. Thanks, Norm.

ALAIN AINA: If you look at [inaudible], for example, [inaudible] speak for itself. We have a root KSK rollover, then we have root KSK [cryptography]. So, if we measure the two together, we are talking about the KSK management.

ERIC OSTERWEIL: Okay. Russ?

RUSS HOUSLEY: From a similar perspective, I think that keeping the root KSK rollover and then the discussion of root KSK cryptography separate doesn't make sense. They kind of go together.

ERIC OSTERWEIL: Okay, great. So, Jennifer, is that document something that I can edit or is that – okay. Let me just pull that up and edit the right thing. Great input, everyone. Thank you.

Okay. So, I'm in the document now. I'm going to make a change that I think encompasses what everyone just said, so let's try this.

[MATOGORO JABHERA]: I have a comment. This activity we are doing, I think it may be good if we can associate each of these activities to the [role and] responsibility of ICANN in [this] DNS. So, for example, root KSK, we just described. Okay. We link this to the KSK management function of ICANN. If we [inaudible] we should be able to also [inaudible] to which roll [inaudible], operational role of ICANN in DNS, [inaudible] of ICANN. We tried to categorize each of these topics.

ERIC OSTERWEIL: Okay, yeah. I think I understand what you're saying. I think I totally agree. So, what I'll do is I'll real quick right now, I'll try and modify this topic and fold it in with the one that [inaudible] out below and do it in a way where I won't [inaudible]. That is something maybe we can do in the breakout session. Does that make sense? How's that? So, DNS root crypto is very broad. There's the [ZSK] and the KSK, like you just said. There's a lot of management functions. There's changing the keys. There's crypto [inaudible], so we should probably do stickies for that. That's great input. Anyone else have any thoughts? Okay, cool. Roaring success.

So, next one. And we can always jump back. So, I'm going to go forward briskly, but we can always back up if I've blown past something. Alternate root deployment and coexistence. So, what I had intended by this was not that ICANN has any purview over alternate roots but that the presence of alternate roots impact aspects of unique identifier system or the DNS root itself by the presence of potential ambiguity and separate management functions.

So, I thought it was worth us talking about whether that was something that traces back and see if it relates to anything we would make a recommendation on. Does anybody have any thoughts on that?

UNIDENTIFIED FEMALE: Yeah. Do you see an overlap with the future bucket of issues, future threats?

ERIC OSTERWEIL: I think, based on the presence of alternate roots today, there's probably a clear and present aspect and probably also a future aspect. My personal opinion is that it would be both, but I'm open to suggestions or thoughts. Okay. So, we can come back to it if we want, but it sounds like silence acceptance.

So, the next one – some of these may … Well—

UNIDENTIFIED FEMALE: Does it obviously go with the responsibility [inaudible]? Like root zone management, that one?

UNIDENTIFIED MALE: I will [inaudible]. No. [inaudible] the root server. The root server. The root zone itself. Because when you have [alternate], you are impacting both root server and the root [inaudible] itself and [inaudible] space. So, [inaudible] to one role inside ICANN. But then we need to [inaudible] how we deal with it, because [inaudible] ICANN business. It could be. Yeah, we could say it because what can ICANN do to prevent people for running an [alternate] root? This is for discussion.

ERIC OSTERWEIL: Yeah. That’s exactly right. This is for discussion because we may get to the point where, as we look at it, we decide it’s completely something we shouldn’t bother with, but if we don’t talk about it first, I think we miss a chance [inaudible]. For example, maybe it’s as simple as there needs to be a canonical list of known other roots and they need to be monitored and explained or something like that. I don’t know.

DENISE MICHEL: I think that would be a good comment, Eric. I guess it’s good … I would think it’s good to remind ourselves that simply because we’re committing to conduct research and analysis in these areas doesn’t necessarily mean that the outcome will be a specific recommendation. After looking into it and discussing it, we may find that this is not something we’re going to recommend action in. Any of these. I’m not talking specifically about that, but …

ERIC OSTERWEIL: It is a journey. Alright, cool. So, the next one is root zone SSR measurement reports. So, what I had in mind about this was that in the past there have been SSR reports issues and they had some aspects of them that included measurements. I don’t know if there are still quarterly or yearly SSR reports published, but in any event, I think it would be worth us discussing whether this is the kind of thing that should happen, whether there are some things that should be measured about the root zone, some aspects of SSR that can be published periodically, whether that’s for longitudinal analysis down the road or status monitoring of how things are going. I think we should investigate whether measurement and [inaudible] changes observation of the root is something that is an SSR topic that should be ongoing. Again, this is a discussion point, so if anybody objects, that totally [inaudible]. But any thoughts?

Okay. To that end, same thing for TLDs. So, some sort of set of measurements periodically reported and archived longitudinally of SSR measures for the TLD space as well, as the root.

In my own mind, I think probably measurement and then analysis probably separately as well. I think probably transparency would be like "here are the measurements and then here's some analysis on top of it" building it sort of from a transparent perspective. But I think that's down in the sticky area. I just want to call it out as something we should brainstorm.

KC CLAFFY: I don't know what an SSR measurement is because SSR is not a unit of measurement. [inaudible] doesn't.

ERIC OSTERWEIL: Denise?

DENISE MICHEL: Yeah. I think I agree. Part of this exercise will be providing some parameters and definitions about what is within this bucket that we're describing. Probably a likely place to start is called out security obligations in the gTLD, for example, registry contracts. I think there's some obvious things we can look at and then have a discussion about whether there are other specific things that feed into SSR on TLDs.

ERIC OSTERWEIL: Cool.

DENISE MICHEL: And then the CCT report also did a ton of stuff in this area that I think there's a very hazy line between SSR and CCT in [inaudible].

ERIC OSTERWEIL: Cool. I sense we're in [inaudible] agreement. So, these are obviously not in a great order because we'll come back to something in a second. Then, namespace abuse. This one, I put it in there knowing full well how broad and general that statement is and it was because I didn't want to go down on my own without the team doing the brainstorming of dissecting that into various pieces of things that are important that, in some cases, may seem like they run too far afield to be relevant to SSR but that we may find systemic relationships to things that are within ICANN's purview. I thought this would be a great starting bucket to get people's thoughts around what are the things that we care about.

My personal opinion is that coming up with things that matter should start with known problems and the known problems I think, broadly, a lot of them fit under what I would call namespace abuse. So, that's why I put that here. I'm certainly open to input. Russ, go ahead.

RUSS HOUSLEY: Can you explain the difference between that and IANA number abuse or is IANA number a subset of namespace?

ERIC OSTERWEIL: That is a really good point. I think you're right. I think I'd rather fold IANA number abuse into namespace abuse, and if we get unhappy with calling IANA numbers a namespace, then we can break it back up. So, that's a really good point. Okay.

DENISE MICHEL: Norm, there will be overlap or connections with some of the elements of ICANN SSR [inaudible] as well. But I think there's an ample number of things to explore in this area that aren't currently in, say, the registry-registrar contracts. [inaudible].

ERIC OSTERWEIL: Great. Okay. So, the next thing is the jump back I was talking about. IANA registry SSR measurement reports. This one I put in I thought for more completeness than anything else. I'm not sure exactly what that means. I have a better sense of what root and TLD SSR measurement reports might suggest that we brainstorm. But considering the IANA registries and their importance, I think it's important to figure out whether there's anything in there that we should look into as needing measurement reports about those, because they're critical and I think potentially often forgotten. Okay. This is going swimmingly.

Okay. Then, change control for the root zone. Actually, I'm missing something else that KC added. I'll put that in after we do change control root zone. But change control for the root zone. So, this is the function by which the root zone has changed, and in general, more generally or differently than the DNSSEC crypto we were talking about above. Does anybody think this is worthy of more discussion, should be kicked out, have any concerns with anything?

DENISE MICHEL: Can you just elaborate a little bit more about some of the things that would fall in under this element that you would consider drafting?

ERIC OSTERWEIL: So, what are the processes that are involved when there's a change to the root zone that needs to happen or is being requested or needs to be backed out and are those processes robust? Are they being followed? Are they being audited, monitored? Do we know what's going on there? Is it just something that affects the SSR of the DNS and should we look at whether we should investigate it? It's a very broad fishing expedition, but that was the inspiration behind it. Does that make sense?

DENISE MICHEL: Are you going to put all of these under a category of root zone management, this change control and KSK and crypto?

ERIC OSTERWEIL: We could. Should we do that? Okay. What else would go in there?

NORM RITCHIE: As you're doing that, you added DNS [flag] day which is going to be … That's a very specific event that's occurring shortly. Is there a broader category that you're concerned about there?

KC CLAFFY: I guess it would be [such] events, but I'm really not sure about this one, if this should be on here. I mean, it's the kind of thing … Oh, somebody should do something, but who? Well, except they tried to make changed to improve the security and the stability of the DNS, so it depends how broadly you want to interpret the mission.

NORM RITCHIE: I think the [inaudible] old telecommunications days, it was called inter-operability and DNS is a great example of that. [inaudible] telecommunications [inaudible] work the same globally and DNS is the same as interoperability of different implementations.

ERIC OSTERWEIL: And I think that maybe when we get into—

MATOGORO JABHERA: Based on my understanding that these are the broad topics that we have identified and depending on my experience on this kind of perspective is that we identified the topics, we assess within the ICANN, according to the ICANN remit. I would also recommend that we identify some of the entities, organizations, or stakeholders that are being or might be affected in case change happens in one of these topics, because as you remember, when we started, we said we need to reach a point to where we have a kind of smart recommendation and in order to achieve that, [inaudible] of assessing the technical side within ICANN but also we need to go to a next step of seeing is there any other feedback that we could also receive from other stakeholders who are being affected by each of these areas that we have identified?

In that way, the assessment that we are doing or the review that we are doing will lead us to a conclusion or to a recommendation that even if a different entity or someone else has been given on the same topic will reach to a point where we come up with the same conclusion or recommendation. So, it's very important.

I had also the same observation from the other topics that we've already covered that, from the academia point of view, when we're doing this on the methodology part, we are assessing within the ICANN, but it is also important to capture some of the feedback from the other stakeholders who might be affected in case any change of these is happening within the ICANN or other area that we have covered. So, that was kind of my observation that when we are going through on each of these topics, it's best that we have a clarity on what we need to achieve.

For example, if we're saying on the top-level domain is a measurement report, what do we need to achieve out of this? And what approaches should we use? Are we going to review some of the documents that we have? Are we going to see the actual implementation with the ICANN? Are we going to assess the impact or any other outcome that might happen or feedback from the stakeholders who might be affected? For example, [inaudible] top-level domain could be on the [inaudible] and others.

So, we need to have [inaudible] on that strategy so that when we are coming up with a recommendation we find that we captured all directions that we think is important to be captured. Thank you.

ERIC OSTERWEIL: Yeah. I think that's great input. My hope is that when we get into the breakout sessions and we start actually decomposing these and dissecting them that that's what we'll hopefully all keep in mind, because you're exactly right. What we need to do is, once we get into these things, figure out how to make them actually specific, smart, etc. And whether we need to see implementations or not, we'll probably get to as we look into each of these things.

Okay. So, that is the whole list. If anyone has other things that they think are missing from this list or you want to back up and revisit any of them or yank them out, this would be a good time. We're just past the 20-minute event horizon that I put forward, so we're right on time for my made-up agenda. Norm, go ahead.

NORM RITCHIE: Are you going to try to pare this down some or is this going to be … Are you still looking for additions or are you looking for possible deletions?

ERIC OSTERWEIL: Either or both.

NORM RITCHIE: Yeah. I'm not sure software interoperability is part of this, but that's my own opinion. I think it might be on the fringe of being in scope or not.

ERIC OSTERWEIL: Just a clarifying question. Is that something that … So, you think it's not worth having it as a brainstorming bucket? Because one thing that can happen is we can brainstorm and find that it's exactly the case and throw things [inaudible], too. I'm not proposing that we enshrine these things at the end of this section right here. I was more saying we can look at them more closely and see, unless we have a sense right now it's not worth our collective time because we are … This is precious time, so I don't want to waste it on things if we know that this probably is a dry well.

BOBAN KRSIC: I'm trying to remember the part [inaudible]. There was also something. He drafted the report about two or three pages. Do we have [inaudible] here as a topic or the team management? I can't remember. It was last year or two years before.

ERIC OSTERWEIL: Yeah. Geoff drafted something that it's hard to tell what the intersection of this is because Geoff, my view of it, was doing a bottom-up summary and this is much more top-down. My sense is that the top-down gives us a better view starting from a problem and dissecting into what the relevant pieces are and the bottom-up I think can sometimes be a little more narrow in scope. You know for sure what's inside the purview of ICANN and you don't necessarily see the systemic things that are impacted by it. So, I think this will probably dovetail into all those areas, like nameserver, deployment, etc., and so forth. But I think this is starting more from there are problems, let's look at those problems, and see if they're relevant.

So, I think they will marry together but it's not here right now. It's like I expect that when we're done with the brainstorming we'll see all those things represented. Is that okay?

BOBAN KRSIC: Yeah. Do we have that report that he drafted?

UNIDENTIFIED MALE: Yes. Jennifer put the link in the chat. I was just skimming through it. One of the things that's in there is a coordination with the IETF over special use registry names and I know that's a political hot potato, but [inaudible] that is a sub thing under the namespace abuse because it's a special relationship, but I know that some people feel it's a form of abuse.

ERIC OSTERWEIL: That's a good call. Yeah. Okay.

UNIDENTIFIED MALE: I think we may want to add something specifically on the root server system, including the L root because we know that ICANN [developed] L root, so maybe we have to look at the root server system, including the L root. Or maybe go for the L root and then talk about the root server system or look at the root server system, then go to the L root which is the one ICANN [manages].

ERIC OSTERWEIL: Okay. So, I've added root server system and used the example L root as a good starting point. That's good. Thank you.

Alright, cool. I'm all for continuing this discussion. I don't want to cut anyone short, but I think if we reached the point of highest value, then now would be a good time to start talking about breaking out. Does anyone want to say anything before we do that?

RUSS HOUSLEY: Just from a logistics perspective, we have this TLD SSR measurements and IANA registry SSR measurements. If we were to combine those two, we'd have six groups. We found that six was a good number yesterday, if we had broke into three groups and assigned two buckets each. So, if we merged those two, we could do the same. I'm not saying we have to use the same groups of people, but that number worked well yesterday.

ERIC OSTERWEIL: I have made that change. Okay. So now, mostly it fits on the page. We have root zone management and we have a bunch of exemplars underneath there. The current starting point only are DNS root crypto, change control for the root zone, root zone SSR measurement reports – actually, maybe I should move that one down. I'll put that one out in the SSR measurements. And root server systems, [inaudible] root. So, that would nominally be one sub-team or breakout.

Then, we have alternate root deployment and coexistence. Then we have SSR measurements. Then we have namespace abuse. Then we have software interop.

So, how does that sound to people? Any thoughts? Yeah. I put that under root zone management. Is that not a good idea? It's hard to know if that should be under root zone management because root server system is not managed by one organization, so maybe it should break out.

NORM RITCHIE: Sorry. I was just looking at something to just tweak something on this discussion. One of the things we are not considering is unauthorized changes to DNS for any identifier. Is that what [inaudible] name abuse? Namespace abuse I guess would cover that. I'm thinking of [inaudible] a registrar's user's account changes the DNS [inaudible] covers namespace abuse, right? Not the root, just the namespace.

ERIC OSTERWEIL: Yeah. My opinion would be it would be namespace abuse. We can even change these names if we get somewhere else with them. So yeah, I'd put it there.

So now, the tricky part is my sense is, based on the diverse expertise we have in the room that a lot of these breakout groups will draw a lot of us at the same time. In other words, it will be hard to do these all in parallel because a lot of us will probably want to be in more than one breakout at a time and hopping back and forth is going to be difficult.

So, I'm going to propose that of the six we have here, we do them three at a time. Then, that way, people can hop back and forth but you don't have to hop back and forth between six things at the same time. You can do it between three. Does anybody have any thoughts about that as a management process for the breakout? I think we could take them in the unordered order that's there. We could do root zone, root server system, and alternate root deployment coexistence at the same time as the first set of three. How does that sound to everyone?

Yeah. So, I'm proposing that we have three boards I see sitting up here that we basically congregate around those three boards. We name each board one of those categories. We put a whole bunch of stickies at each. Then, people will each go to whatever group you want with a pad of stickies and write down the things that you think are relevant to that topic and put it on the board there and discuss. And you can float back and forth between groups. How does that sound as a starting point? Okay. Let's give it a shot and let's try it for …

So, let's do an experiment. Let's see how we do without leaders, so we give maximum flexibility. And if it looks like it's evolved into brawling and melee, then we'll reconvene and put leaders in place to referee the matches. But I'll propose that … Let's do a round on the first three. I'll go around and I'll name each group, like which one is doing what, and let's try that for 45 minutes or we'll call back if there's a problem. But in 45 minutes, let's all come back and see how we did and then we can figure out a go-forward plan from there. How does that sound?

Okay. So, what that means is it's 9:45 now. At 10:30, consider the group is done. Feel free to float back and forth. Put stickies on the board. Don't worry about putting up a sticky. If someone says, "That's already up there," and you feel like it's not, put it up there. More is better than not enough. And then what we'll do is when we get done with the breakout group, we'll try and de-normalize things or we'll try and normalize things down, so that we have consistence of what people think. And feel free to discuss. Alright. See you all in 45 minutes.

Okay. I'm going to call us back since it looks like we've converged. Maybe what I'll do is I'll go around. I won't be able to use the mic, but I'll just read out the things that are on the board before we go to the next round and see if people have reactions to that.

UNIDENTIFIED MALE: [off mic] so root server system, L root. So, L root operations, SSR, best practice. L root technical leadership. Lead by example. Happy to handle all root traffic. System [inaudible]. Management processes. RSSAC [inaudible]. RSSAC roles and responsibilities. [inaudible]. L root management strategy. Root server system evolution. Root server system DDoS protection. Recovery and resiliency. Continuity. DDoS handling. Root zone [inaudible] client can get it from [inaudible] and no is correct. Visibility by supporting a root ops report.

ERIC OSTERWEIL: Okay, it looks like we're done with the stickies. Maybe I'll do the same thing I did last time. I'll read it to you all and then we can stick it in the document and go from there. Any comments or questions before I do that?

Okay, I'll ask everyone to bring the Google Doc up for themselves. Do people need a break? Okay. I've got a request for a break. So, how about 15 minutes, back at 10:55?

JENNIFER BRYCE: Okay. Welcome back, everybody. The recording is un-paused, so please remember to state your name for the record and I will hand it over to Eric.

ERIC OSTERWEIL: Thank you, Jennifer. Okay. So, now I think what we'll do – and I'm open to any suggestions, if you would prefer something else. But I think what we'll do is we'll go down the categories and the list that we brainstormed and we'll consider each of the points there and either … We'll assume by default we're keeping them, but we can certainly discuss taking them out or changing them. But the extent to which we keep them, I think what we need to do is decompose these things into things that match the S.M.A.R.T. goal that we set for ourselves. They should be measurable, etc.

So, I'm going to go forward, unless anyone has any comments or questions. Seeing none.

JENNIER BRYCE: Sorry. I did forget to mention Noorul has joined us, so he is online as well. Hi, Noorul.

ERIC OSTERWEIL: Hi, Noorul. Okay. So, the first section was root zone management and the first bullet in there was data sharing, data release. So, like I said, we can modify this list. We can take things out, change them, whatever, but starting with the presumption that something up there is going to be kept, data sharing and data release, we need to now talk about how would we turn that into something measurable, attractable, a recommendation of some kind. And Russ says what information we need to do it.

So, I can go ahead and just assume the speaking role for this unless the author wants to jump in. But data sharing and data release. So, it's very general for root zone management. I think what we need to do is start off with what data that we want to share and release, maybe justify a little bit why and talk about how we would measure whether that's been accomplished after we may have recommended it.

BOBAN KRSIC: Maybe just a question to that end. Is there actually any data available about the root zone management itself? Alain, you are the [inaudible]. The question is, at the moment, any data available regarding the root zone management process itself? Maybe because the idea is [inaudible] data sharing and [inaudible] mind? Okay. Do we have actual any data that is provided by ICANN or …?

ALAIN AINA: IANA provides some studies on [inaudible] query for about the root zone [inaudible] on that.

ERIC OSTERWEIL: So, can I ask either of you to annotate that, whatever you have in mind for that or we can nix it? Again, I think at this point, I'm going to start pushing people to step forward if you have a perspective on this. I'll take the pen on some things for sure. But can you write something real quick in the Google doc to sort of enshrine that? Being specific. So, what data and how would we measure whether if we recommend that, it's been accomplished? Denise, go ahead.

DENISE MICHEL: Yeah, thank you. I think a while ago when there were attacks on the root servers, I think that prompted some discussion within this group and I'm wondering if data sharing regarding attacks breaches might also be appropriate as a sub-category here. Just a question.

ERIC OSTERWEIL: I think it could be. If we as an SSR team think it's important to have … So, Alain, I think you and Boban were talking about statistics of normal traffic, and Denise, you're talking about incidents like DDoS and relevant statistics that are probably different kinds of statistics. Does anybody object to making a recommendation that these be produced as public reports after … Well, of course [inaudible] might have to say quarterly or something like that. But then the DDoS statistics after maybe an incident?

KC CLAFFY: You mean for the root, each root? [inaudible] root zone, root ops? RSSAC has done this whole governance thing [inaudible] several documents about measuring of [inaudible] itself. So, I just want to make sure that if we do a recommendation in the space, it's aware of the current trajectory of RSSAC has published this thing about governance which I think involves measurement, but I have to go back and check. And their own proposal for measurements that should come out of the roots. And I assume some of them are doing some of that, although I haven't checked lately.

DENISE MICHEL: Thanks, KC. Instead of jumping to I think recommendations or – I think an appropriate step here is the question: what data sharing and data release is available regarding the root, regarding security instances for each of the root servers to make sure we understand this space? That's how I'm thinking about this. That coincides with Alain's, Boban's [inaudible] about this.

KC CLAFFY: There was no presentation on that in October that you recall?

ERIC OSTERWEIL: No, there wasn't. I'm trying to transcribe real-time so that we can hopefully at least have a starting point. I'm saying it's now turned into what data sharing and release is currently available, [inaudible] DDoS measurement stats. And I'll add something about, again, this is not measurable right now, so I'm going to add something in that would make it measurable and I would like people to look at what I'm typing and tell me where it's gone askew or [inaudible].

Okay. So, I put something in. Can people read it and tell me if you think that's a good place to start?

But you just said that there's some people that are archiving or they're doing it. So, root ops … I mean, if I were, for example, a management function in an organization like ICANN and I was aware that someone was doing these stats and my job was to [type] them and serve them, I could just simply say to those people, "I need you to provide it to me, blah-blah-blah," and I'm going to put it in a database with a PHP frontend or something.

NORM RITCHIE: Yeah. ICANN now has the big [inaudible] open data initiative where they're sharing and they tend to share more data regarding various things within ICANN and IANA. So we might want to check there and see if that's actually covered already. Meaning, I think we need an update from the last 15 months because things have changed.

ERIC OSTERWEIL: How does that look? Get an update from [inaudible]. Okay. So, maybe I'll try and come up with a sort of strategy as we're going forward. So, what this basically says is there's a priming statement, do some recognizance and then there's a proposal, something that would be smart, I think. If people want to object or correct something, that's great. Then, the follow-up is an outstanding action. We should get a briefing on [ODI]. They should inform for that. How does that look as generally going forward? I'll do that with the other bullet points that we keep.

Okay. Again, I want to continue to beat on the fact that these things are up there. Just because they're up there doesn't mean they have to stay. We can certainly discuss it. I hope nobody feels proprietary. If it's something that you put up there with no attribution, [inaudible] off, so I think we should all feel like if you see something up there that doesn't make sense, let's yank it down. This is not the list that's perfect.

Okay. So, the next one is elliptic curve crypto. There's lots of ways we could address this. Is it something that we want to discuss that elliptic curve crypto in the root zone management should happen, we should evaluate some aspect of it, we should investigate whether it makes sense. What do people feel like we should do with this one?

NORM RITCHIE: So, looking at this elliptic curve crypto KSK roll frequency and process and root KSK operational really hang around the same topics. You have to roll the root to change the algorithm. You have to … But you can roll it and keep the same algorithm. There's a lot of things that are synergistic there, so I think we should … Anything we do, we ought to combine those.

UNIDENTIFIED MALE: I agree. And to build on what Russ said and to make sure we agree on it, I think when we look at the KSK operations, we should avoid as much as possible going into detail and [inaudible], for example, those who are talking about the [inaudible] algorithm. So, what do we have to do? It's not really [inaudible]. We have to look at the root KSK operation, follow [inaudible] practices and have [inaudible]. For us, maybe we look at the procedures. We look at how it has been done. But it's not for us to prescribe that. We have to do [ECC] and when or not. So, I think we have to—

ERIC OSTERWEIL: Okay. Not to be argumentative or anything, but just … One thing we could do, potentially – and I'm not saying I know what the sort of inspiration behind that [inaudible], is we could say if elliptic curve is going to happen, it's going to involve a KSK roll and there are some SSR concerns that may be not well-discovered, like for example, software compatibility, or algorithm maturity.

So, I think the fact that a key is being served, an elliptic curve key, doesn't change the DNS server operations or it makes the byte smaller on the wire. But for example, the SSR implication is: is ECC a good idea for the constituency of the root? I mean, I don't think it's bad, but if we were talking about something like [cost], then we'd have a big set of discussions about … Even though all the infrastructure will run the same, you've now put a crypto system out there that doesn't necessarily have as much support in the cryptographic community.

So, I don't know if we want to go down that direction. We could. I mean, that's one way we could look at the general bullet of elliptic curve crypto. It's like, to get there, like you said, takes a role and that's covered below.

The other thing to say is if ECC is in the future of the root or [inaudible] curves or whatever else, then what are the things that we should consider before it goes forward? Software compatibility, maybe regression testing. I don't know. What level do we want to do with that or do we want to take it out? What do you guys think?

UNIDENTIFIED MALE: Okay. It's actually up to which level we want to go, because if you look at it, the key rollover, it follows the DPS [inaudible], the document. Then the DPS and the DNSSEC practice and signing document tells you what you do for each of these things [inaudible]. So, maybe what we'd have to do is look at that document, how the document has been followed, but not moving forward because there are some [inaudible] companies which [inaudible] evaluate to see how ICANN followed that DPS. And this [DPS covers all these things] and then we just move on. So, how do you change the algorithm? All of these things are part of the DPS.

ERIC OSTERWEIL: Yeah. The DPS does sort of direct how things should go, but there's no measure of whether the DPS is saying to do things … That all the things have been though through or the practice in the DPS are actually sound. We may not decide we want to pick up the mantle on this, but just because it's written in DPS doesn't mean it's the right procedure to follow, for example. So, I don't know if we want to get down in that direction, but that was kind of the spirit of considering ECC. You're right. We could follow the DPS to do an algorithm role and get to ECC and the question is do we want to look a little deeper and say are there any SSR concerns with doing that or do we not? I'm deferring to the team on this one, so I'd love to hear other people's thoughts.

UNIDENTIFIED MALE: There's a whole bunch of operational benefits that come with the reduced sizes of the ECC stuff that are related to the stability. So, equal security, but better stability because of the smaller size, and somehow we need to point that out.

UNIDENTIFIED MALE: Isn't that really just a recommendation, though, rather than [inaudible]? Going along with the DPS side of things, that probably should be something that we review and see if it's actually being followed. And then that would cover a broad section here.

ERIC OSTERWEIL: Okay. Then, I will also suggest that we review some published work on the benefits of ECC in the root that's been published in academic journals. And I can take the item to go on the records. Okay. So, I'm not going to let us off the hook here. So, what is it that we would propose as a recommendation from this? It sounds like there's certain [inaudible] support amongst the team to keep it, so I haven't yanked it. So, are we proposing that we just [sensitize] people? It's not much of a recommendation. There's no measurement aspect of that or it's not measurable. So, what do we want to propose about elliptic curve, assuming we follow this thing all the way through to the end?

RUSS HOUSLEY: Well, if we decide that we want a recommendation, then I would suggest that we say follow this process to do a role to the new algorithm in some kind of timeframe, probably [add a] short one, given the number of pieces to the software that we'd have to make sure support the elliptic curve as well as RSA to do the roll.

ERIC OSTERWEIL: Okay. So, I proposed some text. How does that look? Okay, I'm going to move on and let's jump back at any point if anyone wants. Next one is DNSSEC below the root, TLD DNSSEC deployment. Were those two that got run together? No. They were just two [inaudible]. That's right. Okay. So, DNSSEC below the root and TLD DNSSEC deployment.

So, this could be as simple as producing statistics. This could be as simple as just measuring and reporting with some periodicity. Is that what we feel like is a good thing here?

UNIDENTIFIED MALE: And [inaudible] TLD DNSSEC deployment [inaudible] online [inaudible] which one has DNSSEC and [inaudible] DNSSEC deployment.

ERIC OSTERWEIL: Yeah. I'd just like to get a plug-in there for [inaudible] 15 years is there. But yeah, that's fine. And like you said – and it's come up in other places. There are lots of measurements out there for some of the things we're talking about. So, one of the recommendations could be give us a repo or at least a sort of permalink so somebody can go from ICANN into these stats or that they could be curated by ICANN even if they're authored to maintain somewhere. I don't know if that's what we want. Is that what we'd like to do here? Like Alain just said, these stats are maintained in lots of places by lots of people. What are we asking for here?

NORM RITCHIE: I wrote it down. I'll comment on that. I think this idea of having a permalink or something like that is kind of what I was aiming at, as before their provision of some data, some reporting, so that it is possible to see what's going on.

ERIC OSTERWEIL: Okay. How does that look? Okay. I'm assuming if anyone has a thought you'll jump in. Otherwise, I'm going to keep going because we've got a long way to go.

Okay. KSK roll frequency and process. So, obviously everyone here knows I have thoughts on this. So, I think – actually, I'll defer. Anyone have any thoughts to lead off?

NORM RITCHIE: [inaudible] embellish that to also look at the hardware security molecule replacement or whatever, like they've got to be in the middle now and change the battery, I don't know.

ERIC OSTERWEIL: So, this is a really big category. It could mean a lot of different things. So, KSK roll frequency and process. One thing we could do is we could say – and I'm definitely looking for feedback. So, one thing we could do is we could say what are the criteria that would justify a KSK roll either periodically or per instance and what are the acceptance criteria for deciding to roll or not roll? And some kind of auditing of that process, like formal [inaudible] of that process and some sort of auditing of some kind of whether it was followed or not. And that would include [acceptance] criteria, [exception] [inaudible], etc. That's one thing we could do and that would I think, therefore, also have us outline some of the concerns, like what would cause you, like the acceptance criteria would be based on what could go wrong in measuring that hazard [inaudible], that kind of thing. It's kind of a big mouthful, but it's one starting point. I see Jennifer has her card up.

JENNIER BRYCE: It's actually, Noorul has his hand raised in the room. I think he can speak, otherwise I'll relay your comment. But Noorul, can you speak? Go ahead.

NOORUL AMEEN: Can you hear me?

JENNIFER BRYCE: Yeah.

NOORUL AMEEN: My comment is that should we add DANE and DNS script under the DNS root to stack or we meet in a separate [inaudible] or we don't have any comment related to DANE and DNS script? Are we addressing those issues also?

ERIC OSTERWEIL: So, DANE can't really … The deployment for DANE would wind up having to be somewhere below … Would have to wind up being at a non-delegating zone, so it would have to be like in the zone that you have an identifier in, like [inaudible] or something like that. So, the support for DANE is basically that the root is signed.

NOORUL AMEEN: Okay. Thank you.

ERIC OSTERWEIL: Yeah. I think it's good to sort of keep that sort of stuff fresh, because among other things, that adds … Should hopefully remind us all that there are a lot of systemic dependencies, especially with something like DANE where suddenly the DNS, the root zone maintenance sort of affects a lot of other dependent systems and protocols. So, [inaudible].

Okay. So, KSK roll [inaudible] see any feedback from anybody. So, just to reiterate what I'm about to potentially pen. I think what we would do here … Go ahead, Alain.

ALAIN AINA: I think under the KSK rollover, maybe for the team to know ICANN does complete – or not yet completed for the first KSK rollover. We have some discussion going on right now on lessons learned from the first one and how do we proceed [inaudible]. So there is already some discussion going on on that. Maybe what we should do is monitor these kind of discussions and recommend that it has been done, [inaudible] require that the DPS [inaudible] because right now the DPS says that the key, the KSK [inaudible] after five years is what we followed to [inaudible] this rollover.

We have had a long, long up to five-year discussion on [inaudible] yes or not. If you look at SSAC has long, a lot of work and cyber community and [inaudible] public comments on shall we do it now or when? I don't know if you remember. So, there is some background of comment on this, so [inaudible] maybe get these things and put it under this KSK rollover topic [inaudible] roll the key or not.

So, I'm just pointing out we have had long discussion about this. Maybe we have just to go back to some of the documentation and what are they, the reason, why do you need to roll the key? So, we have already done some work on it. That's all. Do we need to go back and open again the discussion or shall we do this? The community has agreed that we should roll the key.

So now, next is frequency and the process. So, the question of do we need [inaudible]?

ERIC OSTERWEIL: Is anybody who is in the room part of the lessons learned discussion from the KSK roll? If so, we ought to just have that person take the pen for this piece.

ALAIN AINA: I think at least I am on the KSK rollover, at least ICANN [inaudible] rollover mailing list, so there are some discussions there. I don't know if there are other extra lists or …

ERIC OSTERWEIL: So, I'd say that the lessons that are trying to be learned are still being adjudicated, what lessons should be learned, what should be looked at. So, I think it will be an ongoing process and our recommendation, whatever it will wind up being, is going to be hard to … Your suggestion of making sure any lessons that are learned through the external groups that are learning them get enshrined at the DPS. It's very measurable. So, at some point, if the KSK roll list or whomever says we learned this lesson, then someone could look back and say, "Did that lesson ever show up in the DPS?" Then that's a good measurable. So, that's a good sort of side effect that we could put into a recommendation form. Do we want to request a briefing on anything or something like that? Okay, cool.

So, then, I think this one … I didn't get the HSM part of it, Norm. Do you want to do that as a separate bullet or do you see a way to sort of dovetail it in here?

NORM RITCHIE: So, your point is the seven-year battery life, make sure it's replaced before that or is that where you're going? So, if we did see a five-year rollover into a new HSM, that would just be [inaudible] buffer?

ERIC OSTERWEIL: Okay. So, I updated the text a little bit. This has [inaudible] people.

KC CLAFFY: I think it looks good. I think it would need to do some factoring out of process certainly, though, because I think all of these things fall under when you do something disruptive, have a checklist, figure out what the metrics are, check them all off before the plane takes off the ground.

ERIC OSTERWEIL: So, shall I make a separate bullet for inspection of the process?

KC CLAFFY: I just think the elliptical curve, KSK, TLD. Any potentially disruptive policy change, you need to decide what are the metrics by which you're going to decide, okay, it's safe to do the change and then go [inaudible] metrics. So, in the classic phrase, say what you're going to do and how and then do it and then say what you did.

ERIC OSTERWEIL: Okay. Yeah. That feels to me like it should be incorporated into the bullet points below.

KC CLAFFY: I mean, honestly, it goes to the other …

ERIC OSTERWEIL: That's what I meant. Someone made a comment that I think applies to the ones below.

RUSS HOUSLEY: I'll post a draft.

ERIC OSTERWEIL: I just want to point out Alain knows full well what he just said.

RUSS HOUSLEY: I will say that I'm the only one in the room whoever had [Mike St. Johns] as a boss.

ERIC OSTERWEIL: Alright. We'll [walk past that]. Okay. So, annual tabletop for rolling. So, this one to me feels like it's almost self-explanatory by itself in the sense that we could basically just say there should be an annual tabletop for rolling and maybe add something like a published report in an online repository with a permalink. What do you guys think about that?

RUSS HOUSLEY: I wonder if we're going to recommend five-year period for rolling, annual seems real off.

ERIC OSTERWEIL: Well, the tabletop would be testing procedures. And I don't know that we've agreed that we're going to roll the key every five years. I think at this point some people do think we're going to roll it every year and some people think we'll never roll it again.

RUSS HOUSLEY: I'm just saying they ought to be aligned.

ERIC OSTERWEIL: Okay. We could even leave it out and we could just say a periodic tabletop. Is that good? Okay.

JENNIFER BRYCE: Eric, Noorul has his hand raised.

ERIC OSTERWEIL: Sorry, go ahead.

NOORUL AMEEN: This question of [inaudible] two KSK rollover, but I have a concern for [inaudible]. There are instances of [inaudible] for a large scale cyber [exploitations]. So, do we have any comment on [inaudible] management for [inaudible]? This [inaudible] not directly related to this KSK, but any input for this [inaudible] would be fine for me. Thank you.

ERIC OSTERWEIL: Noorul, I’m not sure I follow exactly what you’re suggesting. Are you suggesting that we include a [treatise] on the way HSMs have been used for intrusion or something?

JENNIFER BRYCE: He said yes in the chat.

ERIC OSTERWEIL: Okay. One thing we could propose is we could propose a recommendation saying that there needs to be a statement made about the exploitability or exploits of HSMs that are in use for the root zone.

RUSS HOUSLEY: So, looking at the text that he’s talking about, HSM vulnerability were exploited. Do we have any comment on vulnerability disclosure for HSMs? I’m sure they're managed by the vendor.

NOORUL ARMEEN: [inaudible].

RUSS HOUSLEY: My question is, how is that different [inaudible].

NOORUL ARMEEN: [off mic].

ERIC OSTERWEIL: Okay. So, Noorul, I'll tell you what. If you feel like drafting something, maybe put it in a Google Doc and then direct people's attention to it at some point. That would be helpful.

Okay, so moving on, root KSK operation. I defer to the wisdom in the room. So, one way to look at that is the root KSK operation should be enshrined in the DPS, and maybe what we could take from that is that there should be some periodic statement of adherence to the DPS when there are root KSK operations? Or we just take it [off.] There's no reason that these things have to stay. So, does anyone feel we should – I'm going to propose we take this one out. It might be covered by a lot of the text above. Does anyone think it should stay? And then please speak to it. It's gone.

Okay, moving forward. Identify coordination operation of root zone. I need some help from someone on what the spirit behind this one was. Okay, I'll make it a new policy. I'm proposing a new policy. If we get to something that seems not 100% clear and nobody wants to speak to it, I'm going to yank it after one sort of, "Speak now or forever hold your peace." So, unless someone wants to speak to this, I'm going to yank it.

ALAIN AINA: Okay. Anyway, I'm not the one who put it, but I know that in terms of – I think it’s identified [inaudible].

ERIC OSTERWEIL: Okay, it’s about to get yanked. Okay, bye. Okay.

ALAIN AINA: [inaudible] we need a point, because for the root zone management, one of the key elements is the authentication system, how IANA or ICANN authenticate the [change] request. This goes to what goes to the root system management which use e-mail and sometime [inaudible] use a web system setup. So, we may want to look at how secure is this system.

ERIC OSTERWEIL: [inaudible]. Yeah, so just – sorry, I wasn’t on the mic. So Alain brought a really good point. I just pointed out that there's another bullet down below that’s a little bit more expressive of that point so we can talk about it down there. Okay, any questions, comments? No? I'll move expeditiously. Alright, so BCDR plan. I see Scott reaching for the mic.

SCOTT MCCORMICK: So, for BCDR, I don't know that anything exists currently for business continuity and disaster recovery planning. This is pretty standard across any sort of infrastructure. It also goes hand in hand with the tabletop exercises.

Also, it appears that government hasn't gotten its shit back together yet, but NIST 800-81-2 actually specifies KSK rollovers for DNS. 800-81-2, section 11.2.4. KSK key rollover.

NORM RITCHIE: That's a US government document. I don't [see it having] any bearing on this.

SCOTT MCCORMICK: Yeah, NIST is – while it's a US standard body, it's internationally recognized.

DENISE MICHEL: [When did that come out?]

SCOTT MCCORMICK: 2013, supposedly, is when it was updated. Originally 2006. Let's see here. Why is this being a pain in my ass?

ERIC OSTERWEIL: I feel like I should move that up to the part where we're talking about the DPS.

SCOTT MCCORMICK: Yeah, I was just making a side comment, sorry. That was for DPS. The title of it is Secure Domain Name System Deployment Guide, if you want to add that in there. By the way, 81-2. Yeah, best practices type of thing.

ERIC OSTERWEIL: Okay, so back to the BCDR plan. I'll put, “Ask for any references that point to this. Modulo that, request that one is created and published.” Sound right?

SCOTT MCCORMICK: Yeah.

ERIC OSTERWEIL: Okay, I've put a whole bunch of text in there, and somebody will go and fix them. Okay, the next one is name collision. I'm going to suggest that – I know this is a duplicate for what's in namespace abuse where we should probably decide which of the two places we’ll talk about name collisions. Do we think it’s a rootzone management problem, or do we think it’s a namespace abuse problem? Denise.

DENISE MICHEL: I'm really open to other suggestions. My inclination would be to keep it here, and I think many people around the table did a lot of frontloaded work before new gTLDs were launched to address this issue, and I think there's still some pretty serious challenges like [inaudible] discovery domains and others for which there are some serious SSR issues and some sort of systemic type of thing that need to occur, and a lot of collaboration with other players besides ICANN.

ALAIN AINA: I just wanted to support what he said, [the need is here under] the rootzone management. And when we go to the namespace abuse, it means something else.

ERIC OSTERWEIL: Okay. I see. Fair point. Alright, good. So it's not a duplicate. So then we should talk about how we'll turn this into something that we can make a recommendation around, because as Denise said, it's a very big area. So, does anyone want to take a stab at that?

KC CLAFFY: It's a big area, but like the CCT report has so many recommendations about other things that need to be done before there's any next round of gTLDs. And this may even be one of them, I can't remember. But this goes also back to disruptive policies and what is the metric for saying it's okay to do them. Name collision is obviously one thing. How do you know that this [manages the] risk of name collision to a minimum and it also goes into your – let's have peer-reviewed research and not just say, "Okay, hey, a consultant says it's fine."

ERIC OSTERWEIL: Go ahead, Denise.

DENISE MICHEL: So, I was thinking of issues in the name collision area in terms of current challenges and current rules and processes. Having contacted a number of entities within ICANN about the auto discovered domains and seeing the type of response and processes, I think it’s an area that potentially this team could add some value to. So, I wasn’t really thinking about policies for next round, but rather, currently, how are we doing when name collisions arise, and what's the process? So my thinking here is it’s pretty basic information gathering, so we get a sense of what the status quo is, what the responsibilities processes are, and how many collisions have been identified, how have they been dealt with? Just some pretty basic ...

KC CLAFFY: Is there a webpage of that process somewhere, or you don’t know? I haven't found it. As often is the case, just personal experience in trying to address the auto discover domain problem, I did not find – [and this is just] my personal experience. It may be there and I missed it, but I did not find documented reporting processes and ended up calling people I know to get this addressed in different areas. And that may be my misunderstanding of what the status quo is, but for me, it’s a great example of something I think we should have a general understanding of what the status quo is, and then from there, make a decision whether it deserves our further attention or not.

ALAIN AINA: And I think SSAC produced one or two documents on this name collision [inaudible].

DENISE MICHEL: [inaudible].

ERIC OSTERWEIL: So, SSAC has the name collisions acceleration party, or whatever AP stands for. They have NCAP. And so they're spinning up a big project to actually investigate name collision.

KC CLAFFY: I don't know if that is happening.

ERIC OSTERWEIL: Well, they're –

ALAIN AINA: [inaudible] document, but now they have a project. It looks like there's a project funded by ICANN to work on the name –

KC CLAFFY: [inaudible].

KC CLAFFY: Sorry, as far as I'm understanding, it’s still in the trying to figure out if there should be a project or what the scope of the project is, because a first proposal for a project that went to the board did not go through. It kind of came back in some way that is not totally transparent to me.

ALAIN AINA: Yeah, but I think – you do remember that there were one or two documents I can look at –

KC CLAFFY: They were project proposals.

ALAIN AINA: [inaudible]. You do agree that there is a proposal to do something –

KC CLAFFY: There is a proposal, but it wouldn't be SSAC doing it, because it's too resource-intensive, and I think that is part of the problem, is where the resource would come from.

ALAIN AINA: So, [inaudible].

KC CLAFFY: Yeah, and they want ICANN OCTO to manage it, because [it's too many resources even to] manage such a project. It's a huge research project. And yeah.

ALAIN AINA: Okay. I think from this discussion, we agree that the name collision is a big topic, because it's been discussed, and something – and the SSAC, ICANN trying to do something about it. So I think we need to look at that at least to see what is going on, and maybe see what we do about it.

KC CLAFFY: But again, that’s separate from what Denise is talking about.

ALAIN AINA: [Oh, yeah.]

KC CLAFFY: Okay.

ERIC OSTERWEIL: Okay, so I admit to being a little confused about where our collective head’s at here. So, what I've written is, “Review or discover domain issue, identify what the status quo is, review literature on name collisions.” This is all just kind of chicken scratch. I have like, “Disruptive, change policies, go/no go metrics criteria, current changes in policies, auto discover domains, etc., how to deal with the issues when problems arise.” I feel like that didn't even remotely capture what we were just talking about. So, do we want to just leave this and do a literature search and circle back after we have a better sense of what name collisions are? Because I'm definitely one of the people who spent a [lot] of my life in the name collisions world.

KC CLAFFY: Well, again, there's a futures topic that maybe goes in the future. Is there going to be a new round? If there's going to be a new round, what is the checklist? The name collision [inaudible] on that checklist. What's under that checklist? But that's separate from the operational issue of dealing with the problems that happen because of today's name collisions.

ERIC OSTERWEIL: Okay.

KC CLAFFY: [inaudible].

ERIC OSTERWEIL: Yeah, [inaudible]. So that's a good clarification. So then just see if I can try to channel that [while] restating it. So then we could propose that a sort of an understanding of the way in which name collisions are presenting themselves today, we could start doing assessment of understanding how name collisions are happening today, and decide if there's work for us to do or recommendations for us to make based on what's happening right now with the namespace and collision [in it now.]

KC CLAFFY: Are there people who can do that work on the team? Can you and –

ERIC OSTERWEIL: Yeah, if we know what that work is. Right now, I can think of a couple places where there are name collisions happening that I know of, and it's not necessarily clear whether all that falls into ICANN's purview or not. It may have when there was discussion about whether or not to do a new round of delegations, but we're specifically talking about things that are deployed now. So, if there are name collisions that are happening, are there remediations that can be done, and are those remediations affected by ICANN's role at all? Is that kind of where we would structure this line of inquiry?

KC CLAFFY: That is part of what the SSAC talked about a lot, is what is in scope for name collision research to unblock. Ostensibly, it's about unblocking the next round, and I don't think the board knew. I think the board took from one of the previous community, I guess, processes, is that some work need to be done to investigate the impact of name collision, and so they want more work to be done, but they don't know exactly what, so they punted it to SSAC, and SSAC is [inaudible] it's a big open area. So, they explored it in this document that I think Alain was talking about, but I don't think there was resolution on that. So, I don't know how far we go down into the weeds on that.

I think I can get you a copy of that. I think it's public, that proposal. We can start there. We can, like you said, go gather a bunch of links and then figure out what's the right thing to say concisely.

ERIC OSTERWEIL: So, my recollection of that, of the project proposal by SSAC's NCAP was that there would be three studies to be commissioned. One of them was going to be [inaudible] lit search, what's all the stuff that's been done on name collisions in the past in the literature. The next one was a measurement study to discuss what's actually going on now, and there was an outline of what SSAC or NCAP considered to be a name collision to sort of structure what the measurements they would actually cover, and the third commission project would be building remediations. And so I guess I knew that went to vote with the board, and I didn't hear whether it got ratified or not. so it sounds like, from what you're saying, KC, it did not pass the board when they voted on it.

Okay. Alright, so staff is taking an action to go and check in on that. So maybe we'll just leave this as a sort of background investigation, go and find out what the status of name collisions, published work, and the ICANN groups that are circling around it. Does that sound right for now, put a pin in it?

Okay, I have namespace abuse, but not as a category. I have it in the rootzone. So before I be cavalier about anything, do we feel like there's a namespace abuse issue inside of the rootzone management that's separate from the namespace abuse general category? Okay, I'm going to yank it unless somebody thinks there's a distinction to draw. Gone.

Verification of authority for change request, change management, management process change, etc., rootzone change management. Yeah, you're right, they're all the same. Does anyone think these are different? I think they're all the same. Okay, I'm going to delete all of them except rootzone change management, because I think that covers them all.

Okay. Rootzone change management. This one’s also kind of a big issue. So, rootzone change management covers putting new things in that covers changing data that’s in there, like nameservers and stuff like that. So, I'll sort of just speak for my own thoughts on this one and I'll look for audience participation where necessary.

So there's a process in place, it’s reasonably well-detailed and pretty elaborate, and so I think maybe what we’re asking for is some sort of stated adherence to the policy. Or are we looking for statistics from events? What would be a recommendation that we would be able to make out that could potentially be measurable?

Okay, I don’t see any hands, so I could yank it, but there were like four different bullets all saying the same thing, so I'm sure this is important. Go ahead, Laurin.

LAURIN WEISSINGER: So, I see this as an early draft, but essentially, we would probably have to see a document that outlines the management procedures fast, because what isn't clearly outlined cannot be tracked. Probably, there are resources that go into this direction. We would have to check. And then it would essentially go down a similar route that we had before, which would be essentially that there is some tool where these changes are tracked and included.

KC CLAFFY: That wasn't covered already before the pause? It seems like this is a basic thing.

ERIC OSTERWEIL: This is where we would have covered it before the pause. We didn't get to this group before the pause. So, this involves the rootzone maintainer and ICANN and NTIA, and this is well-documented and heavily orchestrated. So, that's why I'm asking what we want. Do we want to review the documentation, make sure that it's clear to the community, how it works, and then decide if there's anything more to do here, or just maybe treat it as done if it turns out everything [we would want is there?] Denise, go ahead.

DENISE MICHEL: All of the recommendations around IANA and PTI, is this well covered in the requirements for assessment and reporting in that area, or do people feel that additional due diligence is needed by this group. I'm a little confused, I think, on that.

NORM RITCHIE: This is one area where I think that it is going to be well covered, but I think this team needs to address and say, yes, big checkmark, well done.

ERIC OSTERWEIL: Okay, so I've put something in there that I think captures that, but maybe it doesn't. But yes, I think that's kind of where it sounds like our heads are at. Basically, we'll maybe ask staff if you can help us find the relevant documentation for this process just for what's [out] in the public sphere, and then assess whether it’s well-covered by existing reporting. And then if it turns out it’s not, we can decide whether we want to do something. If it turns out it is, we can decide if we want to just drop it. That sounds like what we’re saying. Cool, thanks. Yeah, okay.

NORM RITCHIE: [Clearly wants us to look at this.] The next point, [inaudible] sanity checks, that’s mine, and that’s actually part of the rootzone change management.

ERIC OSTERWEIL: I'm making a sub-bullet. Okay, so the next one is the last one in this area, and it says search encryption, HTTPS, I think it was SSL, etc., DOH? I'm not sure what the objective here is, so I'm going to ask if someone else feels like taking the baton on this one.

Yeah, so I'm going to yank this out because no one’s championing it. Okay. Real quick question, sort of procedure. Is lunch coming soon, or should we try and press on?

DENISE MICHEL: 30 minutes.

ERIC OSTERWEIL: 30 minutes. Okay. Does anybody need a – not going to give a biobreak, 30 minutes, unless somebody is in a lot of trouble. Okay, alright, we're going to keep going and we won't get all the way through – yeah, you can't leave, I'm going to ask to have the doors barred, please.

Okay, so rootzone system, and the example was L root. So, we'll roll into this and we'll get as far as we get before lunch. So, L-root operations SSR. So, there's a measurement function down below, but it's sort of a general one. So maybe if I channel this one correctly, maybe it's what sort of performance metrics and measures are published about L-root, and if none, do we want some? Does that sound like something we should be looking at?

Okay, so then if I've stated even close to the way the originator wanted it, then to elaborate on that, should we ask for certain statistics to be published about L-root on a periodic basis at a permalink? Go ahead, Norm.

NORM RITCHIE: Yeah. Again, I think we should look at the ODI. I think that's already there now.

ERIC OSTERWEIL: The ODI has –

NORM RITCHIE: I believe so. I saw a presentation on it, and I'm pretty sure it was there.

ERIC OSTERWEIL: Okay, so then I'll put something in there saying we need to investigate or we can ask to have some pointes to where L-root periodic stats are reported, and we can decide if that satisfies us, and then we can acknowledge that we had a question, and it's well covered.

Well, if there are any stats out there about L-root at all, then we check this box. But if there are certain stats that we think are important, that would actually help direct whether we can find what we're looking for. So, people have thoughts on what we actually want to find, this is a good time to discuss what would be important to know. Denise, go ahead.

DENISE MICHEL: Is there an SSR1 recommendation that touches on L-root, or am I misremembering?

KC CLAFFY: [inaudible].

DENISE MICHEL: Yeah, or am I misremembering?

ERIC OSTERWEIL: Okay, so just to reiterate one more time, if there are specific stats or things that we think are important to measure about L-root, this would be a good time to talk about them, because then when we go and look at, for example, if it's in ODI or rootservers.org or something like that, we can decide if the published stats meet our concerns. If we're just generally interested in having some status indicator of L-root, then almost anything will actually suffice. So, right now, I'll just leave it as we're going to need to go look at ODI and etc. for sources of how L-root stats are published. And then we'll circle back and decide if our itch is scratched. Does that sound right? Alright, cool.

Alright, so now I have best practice. Is that best practice for operating DNS infrastructure? Yeah, I think RSSAC just published a bunch of documents on best practices for a root server operator, right?

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: Okay, so should we then – are we recommending inspection whether L-root adheres to the best practices documents?

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: Okay. Okay, cool. Again, if anyone wants me to jump back at any point, let me know. So, L-root technical leadership, lead by example.

DENISE MICHEL: [inaudible] subcategory of best practices.

ERIC OSTERWEIL: Okay, I'll make a subcategory. Any objections? Okay. Capacity to handle all root traffic. I think what this means is in the event of other letters failing, can any instance support the entire load of the whole root system? Assuming that's the case, I think what we would probably have to do is back of the envelope math on aggregate root load, highs and lows, and global capacity. This one could be incredibly elaborate if, for example, we looked at not just global root numbers but we actually looked at where traffic was sourced per region, which catchment was going to catch, which amounts of traffic. It would be a very complicated management operation.

So, the question to us as a team is, how deeply into this do we want to go? The easiest answer is if we get aggregate numbers for estimated global root traffic and we look at reported capacity of L-root, is L-root capable of supporting all the load, and is it our expectation that it should be?

NORM RITCHIE: Well, this was mine, so it's my expectation that it should be.

ERIC OSTERWEIL: We can put that in the recommendation. And I know that other registries do that kind of thing, any given site needs to support the load for the entire deployment in peacetime. So, that fine. Is that something we feel comfortable with? Because that's a real easy [inaudible].

Okay. No, I think the more resilience we build, the better. I think that actually, that would be great. I think if someone were to push back for some reason, whatever, but yeah, I think it's a very good objective personally.

Okay, so system hardening. Do we want a statement from the operators of L-root to tell us about their hardening practice at the level that they feel comfortable exposing? And feel free to nitpick anything I write that doesn't look right.

RSSAC roles and responsibilities. Yeah, I don't understand. If someone could help me channel this one, that would be helpful. So, RSSAC has role and responsibilities, and L-root participates – oh, I see root server system. L-root was just an example. So, RSSAC roles and responsibilities kind of stated in the advisory committee.

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: So, we want some kind of inspection of that?

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: Okay, I'm going to yank it unless somebody [inaudible]. Okay, it's gone. Okay, recovery and resilience continuity.

RUSS HOUSLEY: So, is this just BCDR like it was in the previous section?

ERIC OSTERWEIL: It could be, except this is the root server system, so I don't know if there's a broader objective here.

RUSS HOUSLEY: I'm saying, is that what the same topics would be covered looking at the root system as the root update system?

ERIC OSTERWEIL: Yeah, unless it’s something about root server operators, best practices that’s required or something like that, maybe, but we could treat this as covered above.

Okay, DDoS handling. Okay, Russ proposes we yank it.

RUSS HOUSLEY: No, I was saying either one of those should go. So one’s gone, now there's one left.

ERIC OSTERWEIL: So this one could be a really slipper slope. I'm not imputing anything, but one way this could be really complicated is, are we proposing there needs to be a mitigation service on standby for root server operators? I don't think that's necessarily what it's saying, but that would be one way the root server system could effectuate some DDoS protection.

NORM RITCHIE: There should be some mention somewhere of what level of DDoS it can absorb before it starts losing its service. So, DDoS is a –

UNIDENTIFIED MALE: [inaudible].

NORM RITCHIE: Well, I'm just thinking overprovisioning. That's a simple way of protecting from DDoSes. Overprovision [inaudible] the question is by how much you do it.

UNIDENTIFIED MALE: [inaudible].

NORM RITCHIE: Very good point.

ERIC OSTERWEIL: We could propose that every RSO, root server operator, needs to have a plan in place that is inspected, if not publicly, by some agency within ICANN. Or I could just yank this one out.

KC CLAFFY: I don't think it's a bad idea in the spirit of brainstorming, but the lines of authority and responsibility with respect to ICANN and root servers simply are not clear. That's not to say that we shouldn't – if we feel that this falls within the area of SSR, that we shouldn't address it, but maybe I'm now making a case that we should look at this at at least a high level, and decide whether or not to go forward.

ERIC OSTERWEIL: We could also structure some thinking around potentially making a recommendation that ICANN facilitate a mitigation solution to RSOs if they don't have one but want one.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Yeah, like for example if they were to put a mitigation service on retainer and offer its services to root server operators that are getting buried or something like that. That's just a strawman, but we could do that as a recommendation if we wanted to.

BOBAN KRISC: Just for clarification, are we talking only about L-root operations?

NORM RITCHIE: No.

DENISE MICHEL: No.

BOBAN KRISC: Okay, in general.

DENISE MICHEL: Yeah.

RUSS HOUSLEY: So, I find this at odds with one we haven't talked about yet, which is the rootzone's signed, I can get it from anywhere, what's special about a root server?

ERIC OSTERWEIL: Okay.

DENISE MICHEL: Are you saying that –

RUSS HOUSLEY: Because the rootzone is signed, you can get it from anywhere. There's nothing special about a root server. It's giving you the same signed thing, right?

ERIC OSTERWEIL: Is it?

RUSS HOUSLEY: It is.

ERIC OSTERWEIL: How do you know?

RUSS HOUSLEY: If the signature validates, you got the right thing.

ERIC OSTERWEIL: [Not if it’s changed, the signature that was] [inaudible].

RUSS HOUSLEY: The TTL thing, it still was authentic at the time it was signed.

ERIC OSTERWEIL: I'm definitely happy to have this discussion at a very deep level, but I don’t think it pivots from the DDoS to that. So, maybe we can delay that conversation until we get to it down below.

KC CLAFFY: I guess the way I was thinking about it is, does it matter if there's massive DDoS attacks against a few of the root servers?

ERIC OSTERWEIL: In my opinion is the root server –

KC CLAFFY: I would say yes, this is worth looking at, but –

ERIC OSTERWEIL: I would say that I think the jury is out on whether root servers are special or not. Some people think they are, and to channel Russ, I think he's saying maybe they're not, or at least some people’s view is that maybe they're not, you can get the flat file somewhere and load it yourself.

And let’s say for example that’s not the case, that people want to keep the root server on. Then if they're getting buried by DDoS and unavailable, it’s a problem. So, one thing we could do is say ICANN needs to provide an option for critical infrastructure like RSOs to get DDoS support or advising from whatever. That’s kind of the best strawman I've got on this recommendation so far.

LAURIN WEISSINGER: Just as a question for the room, if we proposed something like that, why only for DDoS and not everything? Just thinking about that recommendation.

BOBAN KRISC: Yeah, the same. About [inaudible] general threats, and maybe we can focus on top five, I don't know, threats of Internet infrastructure, and then address them to say, “Okay, you need I don't know what controls to prevent this and I don't know what in place to mitigate such risks.”

DENISE MICHEL: I think that’s a great idea. Yeah, I think DDoS is just top of mind because of that big [inaudible].

BOBAN KRISC: And sorry for [bothering you] maybe, but we were very specific regarding the issues at the top of this one here. They were all regarding L-root operation. So, that brings the question again, are we talking about root operation general, or only specific at L-root? Because it’s really very specific when I take a look into it.

ERIC OSTERWEIL: Do we want to rebrand the category as L-root specific, or do we want to – I've lost connection, so I'm not going to be able edit for a few minutes, I guess. But do we want to make this an L-root specific category? Because it’s talking about the root server system, and it was using L-root as an example, but you're right, the first set were really all L-root.

DENISE MICHEL: I think there's both. I think there's L-root specific issues to look at, and then I think there's a broader threat handling by all root servers and best practices, things like that. again, it’s a different set of responsibilities with each one. [inaudible] controls L-root but is a one among many on the root server system, and –

ERIC OSTERWEIL: Okay. Sorry. But I think I'm having a senior moment. So, can we bottom line it? So, do we want to make it L-root specific, or no? We don't? No, okay. Okay, cool. So then back to this root server system protection from top-level threats, e.g. DDoS. Are we proposing that there be an investigation as to whether ICANN can offer services, or are we going to presume that services [– opportunities should be offered?] If we just say top threats, we haven't even outlined what all the threats are. So, we could do that in our follow-on work. What do we think?

RUSS HOUSLEY: It feels a little bit arrogant that we are asking ICANN to provide these services to the other root servers that they may not want.

DENISE MICHEL: I think just one step would be appropriate here, and that would be, what's the threat landscape and the processes, structures in place to address them? And once [we get at] that information, then I think after that, I think the next step is, are there some priority SSR issues that we think we need to address given this information of what the status quo is? Is how I'm thinking about it.

RUSS HOUSLEY: Collecting the threat information and sharing it with all the root server community makes a lot of sense.

DENISE MICHEL: Which may be where we go.

NORM RITCHIE: I'm guessing – yeah, so this might be as quick as talking to someone in IANA. I'm sure you've done this, wasn't documented, wasn't shared. Checkmark.

ERIC OSTERWEIL: Okay, cool. We could still leave it in, [a give me.] Alright, so root server system evolution. Okay, so taking a step back, the whole proposal here was, are there things for us to look into? So somebody may have been thinking, should we look at how the root server system has evolved or is going to evolve or needs to evolve? So maybe this is sort of a general – is there a line of investigation then? And if that's the case, anyone can jump in at any time, because I'm guessing here. Then the root server evolution – we don't really get to control the root server system, we're kind of like a high standard to it in a lot of ways. So, do we want to track it?

There's a lot of – oh, sorry, go ahead, Alain.

ALAIN AINA: There is a recent document published by RSSAC about these root server system evolutions. It includes [inaudible] but it also, I think, if I recall, it also includes how the system is designed, the root server system designed, how the root server zone file is distributed, [inaudible] we may need to look at and see if he has some SSR issue.

ERIC OSTERWEIL: Okay, so then to make sure I understand, basically, this category prompted your observation of the document and that you're proposing we review the document to see if there's anything else that we want to dig into?

Okay, L-root management strategy. Does [inaudible] get a promotion? Okay, so I'm not sure what the inspiration behind this one was. L-root management strategy could be some kind of – is there concern about auditing its management policies or how it’s being maintained?

ALAIN AINA: With how it’s being maintained, how it’s being distributed. You know, the Anycast system.

ERIC OSTERWEIL: Just make sure that’s published somewhere, or that we’ll evaluate it?

ALAIN AINA: Yeah. No, the strategy should include how it’s being maintained, how it’s being distributed and what are the criteria for selecting locations, what are the criteria for selecting locations where you put a copy of the L-root [inaudible] distribution. How they also respond to [incident, sometimes there's] some DDoS, you call for them to [inaudible] redistribute the node, and then maybe increase capacity on certain notes. I think all of these things are part of the strategy.

ERIC OSTERWEIL: Okay, I think I got everything you said. You were speaking fast, but I think I caught it. So if you take a look at what I typed at some point and something's missing or you want to change it, just jump in. But yeah, I think I got it all. I think I only have one misspelling.

Okay, so going forward, elliptic curve versus RSA crypto. I think this is covered above, right?

Visibility reporting of root ops report. I don't even know if this was mine or not, so I don't want to be too proprietary because I also don't know what I was talking about if it was me.

So, just verify that there are operational status reports produced. Well, I guess for root ops, you can't really – oh, for root ops like the secret cabal. Okay. I don't think we get any visibility into root ops. I'm not sure if there's anything for us to say here. I don't think that's actually anything ICANN can control anyway.

KC CLAFFY: They all do make stats available [inaudible] put at the top. So yeah, I don't think –

ERIC OSTERWEIL: So I just yank this one?

KC CLAFFY: I would vote to yank it. I do think we should mention somewhere that whole RSSAC governance model document that came out last year that this thing’s in a holding pattern, because it [has some pretty serious] recommendations in it.

ERIC OSTERWEIL: I don't know that document. Is that the kind of thing that would need to be maintained where we could make a recommendation that it gets maintained, or was it just kind of a point –

KC CLAFFY: It’s a pretty radical proposal for putting some structure around RSSAC that would require lots of resources and oversight. I just think we should mention it, we should be aware of it, and if we think it’s an SSR issue, which I think it is, then we should figure out what our position is with respect to it. I guess I can send the summary to the list.

ERIC OSTERWEIL: What was the subject of the document?

KC CLAFFY: I think proposed governance model for the root zone system. I'll go find it.

ERIC OSTERWEIL: Okay, so then that one might not turn into a recommendation so much as a note that we've reviewed it. Okay, alright. I left a little spot for KC to paste the link. Okay, root zone assigned, client can get it from any place and know it’s correct. Rootzone is signed is probably what it should say.

Okay, what's our view of the recommendation around this?

RUSS HOUSLEY: So based on the pushback from you earlier, just delete this one.

ERIC OSTERWEIL: Okay. Management process, gov RSSAC 0037 implementation. I need someone’s help with what the objective with this was.

JENNIFER BRYCE: I think that would be the same – the link that KC just pasted into the –

ERIC OSTERWEIL: Okay, cool. Alright, good. Okay, then –

UNIDENTIFIED FEMALE: Sorry, [inaudible].

ERIC OSTERWEIL: Okay, so alternate root deployment and coexistence. This one doesn't look that long. We might even be able to bang it out. So, accountability and transparency with respect to risks and benefits and annual report. So, again, I can't remember how many of these I did, so I don't want to step on anyone's toes if I'm taking license with what you said, but accountability and transparency with respect to risk and benefits, I think what this is basically asking for is some sort of analysis to be performed and published by ICANN about what the landscape looks like with alternate roots in it, and the accountability, transparency, we know what that means. Just in general, it means explain the accountability and be transparent about it all.

So I think what this is is we would nominally direct in a recommendation that this kind of a study be conducted. That sound right?

RUSS HOUSLEY: What I think you're saying is you ask them to publish what they actually see on the Internet, not what they could see on the Internet. I think that's important.

ERIC OSTERWEIL: Yeah, that's definitely what I said. So I've been saying commission a study, and you're saying just go off and look at the landscape. Is that right?

RUSS HOUSLEY: I want to make sure I understand what you're suggesting when you say commission a study to look at the actual Internet and what has been happening as opposed to a thought experiment of what could happen if there were additional alternate roots.

ERIC OSTERWEIL: Right. And the dash annual report tells me it should keep going. So yeah, it’s what it looks like today, and then a year from now, what it looks like and then publish [inaudible].

RUSS HOUSLEY: That I can support.

LAURIN WEISSINGER: I think this makes sense, and I think this also reflects the discussions we had there. So just monitor, track as usual.

ERIC OSTERWEIL: Okay, so I wrote something that I think basically just restates the above, but just for clarity. So again, just to remind everyone, feel free to change whatever. Okay, and then study [why?] Seriously. Okay, so –

LAURIN WEISSINGER: Sorry, I think this was something I put down. [Study why,] essentially, I thought it might be useful to include into that tracking essentially why these things are appearing, what are the reasons, etc.

ERIC OSTERWEIL: Oh.

DENISE MICHEL: [inaudible].

LAURIN WEISSINGER: Exactly, and this would just be like a very short thing.

RUSS HOUSLEY: I'm sorry, because I wanted to pass along a root that wasn't signed so that I could play with parts, you really want to say that?

LAURIN WEISSINGER: I'm not sure. This was a discussion item, right? Not sure if this is needed or not, this was just an idea. Would it make sense to include that? So for example for dot-onion, you could identify why that exists.

RUSS HOUSLEY: But that one's clear and doesn't have any speculation as rationale of actions. And that's where my worry is.

LAURIN WEISSINGER: I guess we could yank it.

ERIC OSTERWEIL: Yeah, I think things like [inaudible] make a very rational statement about why they exist, and I think the way that they could wind up getting used might be different than that. So I think –

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: Okay, tracking and measurement, deltas, etc. So, I'm pretty sure this one is mind.

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: No, this one basically is conduct like a measurement study and produce results, so this is basically like quantify the – it’s more than the accountability, transparency, it’s like, what are they, how big are they, how much do they differ from themselves and from the ICANN [inaudible]?

RUSS HOUSLEY: But isn't that comparing it, the annual snapshot, [inaudible] bigger, are they smaller, is it just this little piece? So it seems to me like it’s a piece of the above.

ERIC OSTERWEIL: Okay. Yeah, I’d be happy to fold that into the above. Okay, terms of reference, dot-onion, etc. I'm not sure.

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: Yeah, I'm going to yank it. Oh, that’s TOR. Okay. Okay, so yeah –

DENISE MICHEL: Acronym [inaudible]

RUSS HOUSLEY: Yeah, acronym [inaudible]

ERIC OSTERWEIL: No good deed goes unpunished. Thanks for trying to help us. Okay, so TOR and dot-onion, do we want to have a discussion about that as an alternate root coexist – actually, just in general, is there something that we want to dive into, or not? Okay, I'm going to take it out because I see no support.

Okay, impact versus coexistence. I think that’s covered above. ICANN coordination operation role. I don’t think we can claim ICANN has an operational or coordination role with alternate roots. But I'm happy to – I mean, one thing we could be proposing is that community try to be formed, but I'm not sure that that's got a lot of chance. Shall I remove it?

KC CLAFFY: Remove it.

ERIC OSTERWEIL: Okay. DNSSEC makes [alt] harder. Maybe that's a lot harder. Oh, makes alt root harder. Unless you have a different KSK. Yeah, I wasn't sure what it was saying. I wasn't sure if it was saying DNSSEC makes it harder for there to be alternate roots or just makes it –

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: Okay. Do we want to keep this and turn it into a recommendation? Struggling.

RUSS HOUSLEY: It's an observation, not a recommendation.

ERIC OSTERWEIL: Okay. I'll move it up to the title as an observation, and then I propose we adjourn for lunch.

RUSS HOUSLEY: Not quite here yet. I think that we – lunch isn't in the room yet, but I do think it’s time for a mental break.

ERIC OSTERWEIL: Yeah, I sense energy is critical here. Okay, so I'll turn it over to staff to help us know what the timing is. Or is that up to me to decide for how long?

JENNIFER BRYCE: It’s up to you, really. Lunch is being served right now, so however long you want to take a break for. It’s up to you.

ERIC OSTERWEIL: Okay. Russ says let’s do at least half an hour. [inaudible] ten minutes for biobreak ahead of lunch, or seven minutes, that way we’re back 1:10.

RUSS HOUSLEY: Okay, if we could get started. Jennifer, would you get the recording started and tell us who is remote?

JENNIFER BRYCE: Welcome back to SSR2 day two face-to-face meeting in Los Angeles on the 26th of January. The online participants at the moment are Noorul, and Kerry Ann was there just a minute ago, but it looks like she's gone, so [inaudible]. And the recording is live, so please remember to state your name for the transcript before you speak. Thank you.

RUSS HOUSLEY: Okay. Thank you, and I'm going to turn it back over to Eric to continue down this list to make sure that we understand what the brainstorming results are, and then it's very clear to me at least that there's a lot of stuff on this list, and we're going to have to go back through and do what we called yesterday ruthless prioritization.

ERIC OSTERWEIL: Yes. Welcome back to part one of the culling. Okay, so when we last left our heroes, we were all about to start SSR measurements. That should be fun. So now SSR measurements. Okay, so hopefully, everyone has it up.

Okay, so starting with the bullets that were taken from the [post it boards,] "Define what measures are important to track." So that is something that would fall to us. I think there's a couple strawmen down below, so maybe what I'll do is I'll skip that one knowing that down below, there are some specific instances somewhere. Actually, I don't see them.

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: Yeah. I thought there were some –

RUSS HOUSLEY: [inaudible] measuring geodiversity.

ERIC OSTERWEIL: Yeah. Where’s that? Is it that one?

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: SLA Compliance? Oh, measuring geodiversity [inaudible]. Okay, alright. Yeah, I'll kill the first one off because its too general and it gets hit down below. Alright, and health indicators, I think, is also something that we should pick up when we get down below. It’s sort of part and parcel. Any objections? Okay.

So, SLA compliance. SLAs for what with whom? I'm assuming that’s two different people on the same post it note talking to each other.

KC CLAFFY: [inaudible].

ERIC OSTERWEIL: Okay, so what did people mean when they said SLA compliance under SSR measurements? Is this the fact that there are, for example, registries that have contracts and that there's SLAs, and is it measuring that they haven't breached them? Is that the idea? What was the inspiration behind SLA compliance?

ALAIN AINA: I think part of the SLA, if you look at – whether it is the root zone or a root server, all of this thing has to [make] certain service level. So, [inaudible] how do [make] compliance to this? And this includes, are you able to handle certain normal queries, are you able to [make a response in time] to certain things? So, all of these things [inaudible] are part of service level.

ERIC OSTERWEIL: Okay, so I guess what I'm asking is, are we looking to create a report, are we looking for them to publish a report of SLA compliance? What would we do as far as turning this into something that we would be able to turn into a recommendation at some point? What would your perspective be on that?

ALAIN AINA: I think our point here is [have a] mechanism in place to measure SLA compliance.

ERIC OSTERWEIL: And remind me – we should specify for the SLAs that we're aiming at, you mean for contracted parties or like registries, or what?

ALAIN AINA: It depends on the parties, because if you are TLD operators, the SLA are part of your contract, but for IANA, I [think the] community adopted SLA for IANA services [inaudible]. And if you are, for example, a registrar, I think your registrar agreement also has some SLA.

DENISE MICHEL: Yeah, so the SLAs for registrars and registries have been covered in the ICANN SSR area that was discussed yesterday, and the elements that Norm's group was addressing for registrar, registry contractual obligations. For IANA SLAs, yeah, that's something that they regularly publish and then now is taken over in terms of oversight by the PTI. And so this may be – I don't know, Alain, do you think this may be sort of a confirmation, check the box, make sure this is being done and tracked and published type of thing? Yeah. Okay, sounds good.

ALAIN AINA: Yeah, for example, inside the naming [or] name agreement the IANA or PTI has some SLA, and there are bodies who receive these reports [inaudible] same for the number registry as well.

ERIC OSTERWEIL: Thank you. Okay, so this next one, measuring, and then this is meant to be, I think, an example, e.g., geodiversity of nameservers. So, this is one example of, I think, the idea that I had – so I'll expand a little bit on it – was that I think that my perspective is it'd be useful to require there to be a periodic report of certain indicators that maybe we – or if we don't feel up to it, we commission or look for somebody to give us examples of things that are worth measuring and reporting on in order to assess the SS and/or Are of things that include the root, and maybe to some extent TLDs, etc., other parts of the infrastructure that matter to us. And so this is sort of a very micro view of some of the things that I think are important.

So, this is my personal perspective. I'm happy to take some input from the team if you all like, but my one strawman here is the geodiversity of nameservers for like a registry, to sort of try and understand how wide its footprint is or something like that. It’s not clear immediately what the cratering effect or what the liability or danger or concern would be with having different levels of deployment, but my surmise was that we should start tracking these things as numbers and make them public and longitudinal.

ALAIN AINA: I think this is also another example what I just said, but [inaudible] if you are TLD operators, how you design your DNS has a geodiversity requirement. Same for the root server system, you have a requirement to diversify the nameserver, so it’s also part [inaudible] meeting the requirement.

ERIC OSTERWEIL: Yeah, that’s fine. I guess if there's something in an SLA, then somebody decided this was important, and I don't know what level they required it. So I was just proposing that we come up with a set of things we think are important to track. An SLA, that’s an agreement, so if you breach it, there's ramifications. I'm proposing we just measure things and we track the status of them.

They could be things that are included in the SLA, but if there's an SLA compliance check, it says you passed, you didn't pass. Maybe it gives you more insight. This would just be like here's the numbers. On day X, the value is Y, that kind of thing. I don't know, does anyone have any appetite for embracing this kind of measurement or not?

To be clear, I'm just proposing that we ask to have it done periodically, not that we necessarily do it ourselves.

ALAIN AINA: Okay, when I'm going to mention SLA, maybe the agreement part is more rigid, but I think the focus should be on the service level. For example, if you want to measure something, as you are saying here, measure a nameserver, you need to have the metric. When I measure, I should be able to have a metric to tell me, am I okay, am I doing well, am I not? Etc.

ERIC OSTERWEIL: Not necessarily. If you can devise a measure and turn it into a metric, that’s great. But in order to measure things, you don’t need to have a metric. You can literally just measure things and say, “This is what I've measured.”

ALAIN AINA: And what's the goal of if I just measure it?

ERIC OSTERWEIL: The fact that you're measuring things that you find interesting doesn’t mean you have to know all the uses for them ahead of time. Clearly, if you measure things that wind up being useless to people, then you’ve done no one any service, but you can't always know a priori what the utility of a longitudinal measurement is.

ALAIN AINA: But here we’re talking about SSR. So, for me, when I measure anything, I have to relate it to security, stability and resilience [inaudible] have to have a metric and say, okay, are you performing at this? Otherwise, I have a stability or security issue here, or resilience issue.

ERIC OSTERWEIL: So, to be pedantic, so you're saying geodiversity, you can't imagine how that relates to security, stability or resiliency? I can see how it matches to stability and resiliency. There's no metric there, but I'm pretty sure that geodiversity gives me some view into stability and/or resiliency.

ALAIN AINA: [inaudible] but how do we relate this to this work we are doing maybe?

ERIC OSTERWEIL: Yeah, that’s what I'm asking for people’s perspective on, is that doing measurements where you hope that there's going to be archival value or longitudinal value to doing them, and so you try and do measurements that might be useful down the road or ask to have them done is different than saying, “Here's a metric. Here's what I'm actually looking for specifically.”

So, what I'm asking is, do we want – it sounds like maybe the answer’s no. It sounds like maybe we don’t want to do a sort of, “We want you to periodically measure the infrastructure and here are some elements that you should measure.” And that’s fine. If we don’t want to do that, then that’s okay.

MATOGORO JABHERA: To the best of my understanding that if you are conducting a measurement, there is a baseline or some of the issues you want to check and see, are you deviating from the standard points which hu are referring to? And in that way, I think I suppose the [inaudible] input that if you are measuring for the geodiversity, then it’s very important to see that we have some of the metrics that we need to see from the measuring point of view if we are achieving it. so, I think something that we may need to discuss further so that we agree on the measurements, what we need to achieve out of it. Thank you.

ERIC OSTERWEIL: Okay. I'll take it out. [Availability of NS,] same thing? Okay. Quarterly report of – oh. Propagation delay and consistency of changes of zone contents across nameservers.

ALAIN AINA: I think for example it’s also part of the service level for if you are –

ERIC OSTERWEIL: No, it's not. It absolutely is not. No one has done this measurement. And it's been asked for many times in many different places. No one has done this measurement.

ALAIN AINA: No, I'm not –

ERIC OSTERWEIL: At any given instant, no one knows what the propagation delay for changes across root server instances is as far as I know. and it has been requested before.

ALAIN AINA: [inaudible] to meet, but [inaudible] measure is the [inaudible]

ERIC OSTERWEIL: But that's exactly my point.

ALAIN AINA: If you look at the document for example for the TLDs operators, I think there are some timing, you must meet the minimum timing, you must miss ... [that's the thought that I have.]

ERIC OSTERWEIL: Would it have been validated? That's the proposition. Okay, I'll [take it out.] Oh, I thought this was the same – okay, leave it in? Okay.

IANA registry availability measure –

ALAIN AINA: I think we are under SSR measurement. Security, stability, resilience measurement, right? These are the topics we are trying to manage. So for me, if we are under this, all these measurements should be related, and it looks like we are just ticking them off, but I think they were there for a purpose, to measure something, and we see how it's related or how it affects security and stability. Otherwise, we will just clean up everything there at the end of the –

ERIC OSTERWEIL: That has not been my experience with measurements. My experience with measurements has been that you measure a lot of things, and as you do it, you get better at making guesses at what's useful down the road. But oftentimes, when you're looking for data, you're glad you were measuring something that's long since gone, because when you go back, you're able to use it for something you hadn't thought of at the time if you've done a good job.

And there are other people in the room [that do] measurements as well, so I defer to the collective wisdom, but I don't believe you always know a priory what you're going to be doing with the measurements when you take them, that's why you're conscientious and you're detailed, and you construct your apparatus to try and record with high fidelity the things you think are going to be useful later. A lot of times, you are driving at something specific, and that shapes what you measure, but I found that you often generalize your measurements with the hope that you’ll be able to reuse them for new things in the future.

And so a metric is usually the opposite of that. A metric is usually a highly digested representation of things that you’ve measured, and so usually, it’s very hard to reduce that, because if for example you’ve got a normalized metric from -1 to 1, it doesn’t let you look at other things, but usually, if you derive that from more expressive data, you can reuse that expressive data if you're lucky.

ALAIN AINA:

Okay. I think I agree. So it’s just that we seem to disagree. So a measurement is needed, and there are all kind of data measurement going on in here, etc., and maybe we need more, but our concern here is how this measurement result could be used for our SSR.

ERIC OSTERWEIL:

And I'm disagreeing with you, and that’s fine.

ALAIN AINA:

And this is where we need to – otherwise, there are already people that are measuring data here and there, and there are a lot of things [inaudible] So if it is just to measure, then we have to see what is missing there [and what] we need. And then let’s say we need this kind of measurement. Here, we are talking about SSR measurement. So for me, let’s look at which kind of measurement, which kind of [inaudible] we need to collect to look at the SSR impact on the DNS. Because if I've got the data, the data are there, and if I can't use it for this work we are doing here, I don't see the value.

ERIC OSTERWEIL: And that is exactly the disagreement, the disconnect I'm talking about. Collecting the data and using it for something are different, and –

ALAIN AINA: [inaudible]

ERIC OSTERWEIL: Right, and what we’re doing is enabling future SSR investigations that will have archival data, longitudinal data if we put it in place now, even if we don’t know what the future investigations will need it for. So it isn't that I don’t think we should relate our measurements to SSR. What I'm saying is that we may want to consider we don’t know all the usages –

ALAIN AINA: [inaudible]

ERIC OSTERWEIL: – going forward and so we may want to put in place a facility to track data so it can be used in the future in ways that we don’t yet know for sure what the usage is.

ALAIN AINA: If it is collecting data for the future, I agree, so we have a purpose. Let's go, let's move on.

JENNIFER BRYCE: Kerry Ann also has her hand raised as well.

ERIC OSTERWEIL: Okay. Kerry Ann, please.

JENNIFER BRYCE: Kerry Ann, go ahead. We can't hear you at the moment. We still can't hear you, sorry. If you want to type, I can relay your comment.

ERIC OSTERWEIL: Kerry Ann, feel free to chime in anytime. Go ahead and interrupt me if you need to, that's fine. So, IANA registry availability measurements/security. We had a brief discussion. I think it's not represented elsewhere there. Yeah, so we had a brief discussion about what sorts of information and usage from the IANA registries is important, and I admit it, I haven't personally used the IANA registries for much more than just surfing and pulling them off a webpage, but there are places and times when the IANA registries are needed. And Russ pointed out that time zones in particular are very critical, and there's every reason to expect that they need to be available in a highly redundant way. So I think some investigation into the IANA registry service deployment and its SSR nature is important.

Before I riff off how we think we might go forward, does anyone have any comments or questions about that? Okay, then I'm going to propose that the way we might structure the IANA registry availability measurements is to say that – a deployment description of the service needs to be published. And I would propose some aspect of measurement. Maybe somebody would suggest what kind of measurement makes sense to put around that, because I don't believe there is a lot of discussion about it, at least I haven't seen any published online to describe how we can feel comfortable that the IANA registries are available and protected, etc.

NORM RITCHIE: Do you know what the other registries are offhand? I know the port assignment, but what other ones are there?

RUSS HOUSLEY: There are literally hundreds. No, but if you go to IANA.org/parameters, you'll see a multi-page lift of them.

ERIC OSTERWEIL: Alright, I've just put some strawman text in. And time zones right below there, I think, was just an example for that, so I'm going to make it a sub-bullet. Okay, next one, identify KPI for SSR measurements. I guess that's kind of like what we were talking about a while ago, except that this [inaudible]. So anybody want to speak to this one?

So identify KPI measurements, would that be us doing the identification of what the key performance indicators are? Is this us asking somebody to produce the KPIs? Okay. It doesn't say, so I think we could probably definitely say for root. Should we say for anything else?

Okay. ICANN internal data sharing analysis. Someone asked, what does that mean? ICANN internal data sharing analysis. So, ICANN internal data or ICANN internal data sharing analysis. I don't know. Does anyone want to give me some help on this? Nobody? Okay. I can nix it. Okay. We've been nixing pretty well.

Okay, IANA ICANN internal. That's probably ICANN SSR.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Okay. Alright. We're onto namespace abuse.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Okay. Special use names.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: I thought that was down below.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: This is just a formatting – this one may just be a formatting issue, maybe this is supposed to be somewhere else. I'm going to take special use names out because I feel like someone put that in there [inaudible]. Okay.

Contractual compliance, this is ICANN SSR. I assume those are two commas. Okay, so contractual compliance belongs to ICANN SSR, going to take it out? Okay.

Transparency with respect to abuse. Is this DAAR?

UNIDENTIFIED FEMALE: [inaudible] beginning of it.

ERIC OSTERWEIL: So, do we want to put a recommendation together of some aspect of DAAR? That was the suggestion.

DENISE MICHEL: Yeah. That was relating to ICANN SSR rather than DNS SSR, because it's an ICANN responsibility, contractual obligations, all that.

ERIC OSTERWEIL: Okay. So, transparency with respect to abuse. Is this DAAR? We could structure something here around requesting something of DAAR, some results of DAAR or something about that. Or maybe we could use this to say the DAAR data needs to be – we could make a recommendation saying the data needs to be public.

LAURIN WEISSINGER: Essentially, does the team think DAAR is sufficient as is? Yes or no. We can just do a show of hands. Based on that, we can – yeah.

ERIC OSTERWEIL: Go ahead, Denise. Denise, do you have a question?

DENISE MICHEL: Yes. So I just put in parentheses a question, really not seeking to limit but really seeking to clarify what the author of the sticky meant. I think Laurin raises a good point. Is there a whole range of abuse data that we should consider asking?

KC CLAFFY: There seems to be a lot of activity, according to the website, that OCTO's engaging with respect to DNS abuse analysis, and the community just doesn’t have access to it. We don’t have any way to know what's happening or what the value [inaudible] use of it.

NORM RITCHIE: DAAR’s a summary report on abuse, so therefore it’s not very actionable.

DENISE MICHEL: Very high-level.

NORM RITCHIE: Yeah. So you can see, yes, we’re bad, but what do you do about it?

ERIC OSTERWEIL: So into the point right there of transparency, so the DAAR isn't as transparent as people want because they want to see the data that produced the statistics.

NORM RITCHIE: Yeah, I think the keyword’s actionable data.

ERIC OSTERWEIL: Okay, so going back to what we’d be aiming at here, are we suggesting that DAAR’s a good start, that we want something different than DAAR, something different than DAAR? I kind of get the gist of what I'm talking about here, but I want to try and turn it into something that could eventually morph into a recommendation.

NORM RITCHIE: Yeah. I'm being careful because it’s kind of my thing and I don’t want to stand on top of the hill here.

DENISE MICHEL: Go ahead.

NORM RITCHIE: [No.] The DAAR also reports by registries, not registrars, and registrars aren't actually in a position to do something about it. So I think there's room for improvement is what I'm saying here.

DENISE MICHEL: A few bullets down is abuse data made public with API, major threat vectors and registries, registrars each month. So, I think we can synthesize a few things here and have a further discussion about abuse data that is within ICANN’s sphere and public access to it. I think there's both an information gathering and sort of qualitative assessment of its use and appropriateness of sharing it with the public I think is how I was thinking about this.

KC CLAFFY: Or even sharing it at all. Even if it werent public, but sharing it in a way that it can be used. And what I hear from the community is it’s difficult to figure out what is the return on the investment of community resources into those activities inside ICANN. And maybe it's there, the community just doesn't see it.

ERIC OSTERWEIL: Okay. So, I think I'm lagging on this. What I've gotten is that those two seem to be reasonably tightly related if we want them to be, and they probably do. And I hear the consternation, but again, I want to sort of try and focus us before we go back through and maybe this gets cold or not. What would we like to do with this? Are we interested in trying to move the type of analysis that DAAR is doing forward, are we interested in recommending some sort of enshrining of it?

I think we're all on the same page that this is an important aspect of namespace abuse, but what would we like to do with it here?

NORM RITCHIE: I think we would commend the evolvement of DAAR and encourage its further development along these lines.

KC CLAFFY: Again, along these lines is – maybe you could say, "Develop metrics by which we can measure how the community is benefiting from DAAR, how the community can measure it. And I think Norm had the word "actionable" in there mentioned before, and I think that's also critical, because data is only a means to an end.

NORM RITCHIE: So if you remember the CCT report, they actually go a bit further and they say that the registrars with a low rate of abuse should be compensated for that, and those that have a high rate of abuse should be penalized.

KC CLAFFY: That's an excellent point. I actually think – and this [is probably true] for a lot of these topics, but especially this one. We could just go into the CCT report and cut and paste and say we agree with the fine work that this committee did. The more people say it, the harder it will be to ignore.

NORM RITCHIE: If you also recall too, the CC team had action items for this team, and I think some of them set it around the –

ERIC OSTERWEIL: Okay. So, DNS abuse, what does this include? What have you done for me lately?

DENISE MICHEL: [inaudible].

ERIC OSTERWEIL: Yeah, I agree. Well, yeah, we have name collisions again, and someone brought up before that the name collisions under namespace abuse are different than name collisions in the rootzone management. So now is the chance for whomever it was – I forget who it was – to elucidate their point. Okay, so name collision, do we want to treat it as addressed above? Yeah, it might not be much of an abuse metrics. Or yank it out, we can always decide to put it back in later if we want. It is above. Yeah, but these are all work items, things we're going to do, so if no one got a good sense of what we would do around here – we can add or subtract to these later. I have a feeling there'll be a lot of subtraction, but there can be some addition. Nobody's [inaudible].

DENISE MICHEL: Well, I don't need to repeat myself on name collision and some of the things that I've experienced over the last year. I was interested in looking at current processes and name collision problems. And I think we've captured that above, so I don't know that we need it here as well.

ERIC OSTERWEIL: Okay, cool. Yeah. Okay, new gTLD abuse indicators. Why only new? So maybe that's gTLD, or maybe [inaudible].

ALAIN AINA: I think I proposed that, and I think we can join with the previous session that [inaudible] being agreed on the review agreement and text on CCT review report that has been captured. So I think you can take it out. Thank you.

ERIC OSTERWEIL: Okay. Delegation redirection, NS remapping. I guess this is probably what was just being talked about on various lists of people breaking into registrars and changing – is that a namespace abuse we want to tackle here? I think that’s just an info sec problem, right?

NORM RITCHIE: I think that one might be mine. I was thinking about NX redirection by an ISP.

ERIC OSTERWEIL: That’s down below.

NORM RITCHIE: Okay, this isn't mine then.

ERIC OSTERWEIL: Okay, well, delegation redirection, NS remapping. I'm not sure that’s a namespace abuse, I think that’s just a security incident. Okay, abuse data made public with API for major threat vectors, registries, registrars each month. Okay.

Reactive versus proactive compliance, one-off complaints response versus data-driven priorities.

DENISE MICHEL: This is part of what I think KC and some other of us were discussing about a variety of issues around responsibilities and how the whole [inaudible] compliance was abuse mitigation-related contractual obligations are structured and carried out.

ERIC OSTERWEIL: So, would we propose – in trying to map this to a [would-be] recommendation, would we be trying to propose a different posture or something? How would we turn this into something?

DENISE MICHEL: Yeah, it ‘s possible.

ERIC OSTERWEIL: Seems like one thing we could say is we think there should be like a cookbook created so that when compliance is being structured, there are some things that you can look at to make sure that the agreements have proactive versus reactive postures in them. I don't know, kind of guessing.

DENISE MICHEL: I think the CCT review and some of the abuse-related recommendations in there is probably a good place to start. Their remit was new gTLDs. Many things they’ve recommended have broader applications. It seems to me would be a good stepping off point. And I'm happy to come back to the team with additional information and suggestions of perhaps a path forward on this.

I'm not sure how detailed, how deep into this we want to go, but there are things like for example WHOIS inaccuracy requirements, both obligations on the part of ICANN in terms of WHOIS inaccuracies and how they approach it where they do an audit but they have a strong reliance on one-off complaints from the public. When you find a single WHOIS record that is patently inaccurate or false, you send in a one-off complaint to ICANN Compliance. And with WHOIS records largely pulled from the public view, now you no longer have the public doing most of the work in terms of identifying inaccurate WHOIS records. So you've got one of many broken systems now.

Again, that's just one small workflow in a lot of different abuse processes that involve ICANN.

KC CLAFFY: That one in particular, the WHOIS stuff is covered by the RDS group. They're wrote a lot of recommendations about this, although they may not have talked about GDPR so much, and also SAC 101 where we said it doesn't mean you get to throw everything away.

And I think, again, the more we say, "This has been said, we'd like to reiterate, we'd like to emphasize," repetition is learning maybe.

DENISE MICHEL: Why don't I take an action item to pull together the relevant recommendations out of the CCT review and the RDS review and SAC 101, and perhaps a couple of other SACs, and put them in one place for the team to take a look at? And we can discuss this more discretely. Does that sound like a good track forward?

ERIC OSTERWEIL: Yeah, that's great. That sounds awesome. This is an important issue. Okay, best practices and potential requirements, e.g. two factor for DNS. I feel like that is missing a beginning or something. Probably –

DENISE MICHEL: [inaudible]. Yeah, I don't think it was for DNS but for WHOIS record changes.

KC CLAFFY: I think that was capturing what, in terms of SSR, what is ICANN's role in facilitating or requiring best practices to increase the security, stability in the domain space, for example. Two-factor authentication is just an example of that. May not be the right example.

ERIC OSTERWEIL: No, that's a really interesting example, so I want to get the team's sensitivity around – that sort of sounds a lot like registry lock or registrar lock where basically if you want to change something, you need two-factor auth. So that's saying to somebody how they should run their infrastructure. Do we want to step into that? Because I think it makes a lot of sense, there's a lot of evidence that people agree, because it's a feature in some places. So, should we think about putting together a recommendation like that?

NORM RITCHIE: I don't think it was referring to registry lock, which I think is a good thing, but I don't think that's what this is referring to. I think this is more on accounts for a registrar. That's how I took it. So, should there be two-factor authentication required for registrar accounts to prevent people from hijacking an account or domain within an account or whatever?

ERIC OSTERWEIL: Okay.

NORM RITCHIE: Or broader, should there be security requirements for registrars? And of course then compliance and auditing with that.

DENISE MICHEL: Right. Yeah. Two-factor is an example, and it's different than registry lock, which is more involve and comes with a greater expense. There's a whole range of things that potentially could be done if we find it to be a priority in the SSR area. Anything from perhaps ICANN. or in collaboration with other, raising greater awareness of some of the key tools and best practices in this area [to moving to] making something a policy or contractual obligation, etc.

You'd be amazed how many companies don't have registry locks and aren't aware that that is an important tool for keeping a highly used, highly valuable domain property secure.

KC CLAFFY: I think SSAC bangs its head against the wall a lot about this stuff, so people will just implement the recommendations.

ERIC OSTERWEIL: Is there some sort of canonical best hygiene that we would all sort of normally take for granted but that we could use as sort of a stable reference point, normative reference for this sort of user authentication?

KC CLAFFY: SAC 74 I think [inaudible] this one.

ERIC OSTERWEIL: Alright. Okay. Definition of abuse types. Little bit general.

LAURIN WEISSINGER: This referred to the data sharing stuff, so that essentially there should be some form of reporting on what types of abuse have been registered and what falls under these categories. I'm not sure if we have to leave that in or if this is clear. That’s for sure. Definitely not as an extra point. I'm not even sure if we should put it into what we already have above. Might be good, don’t know.

ERIC OSTERWEIL: Okay, we'll probably wind up doing that as a consequence of the above stuff anyway. Okay, dot-onion. I'm not sure [inaudible] call that abuse.

RUSS HOUSLEY: Didn't we end up doing that one in the abuse section?

ERIC OSTERWEIL: Yeah, we had it in the alternate root section. We're not in the abuse section. Anyway, I think dot-onion – public but delayed. Going to pass on that one.

RUSS HOUSLEY: No, that was a sticky on a sticky, which was, let's make the information public, but don't make it available –

DENISE MICHEL: [inaudible].

RUSS HOUSLEY: Right.

ERIC OSTERWEIL: Got it. Alright, I moved it up. Okay, NX domain redirection, leadership IDN domain names, [inaudible]. I thought that was more than one. Anyway, Norm, I think this was at least partially yours.

NORM RITCHIE: Okay. That’s two points, that why it’s confusing. NX domain redirection is one point. So I don't know if that’s a concern. Probably not. I'm thinking [I’d] probably remove that.

ERIC OSTERWEIL: It is a concern in general, but it’s also business model, so to outlaw, you’d have to make it...

NORM RITCHIE: Yeah. We can probably nix that one. Leadership was a separate sticky I stuck on there, so that’s a separate bullet. It’s frustration coming through. Should the ICANN broader community take a leadership role in handling or tackling abuse? Because right now, it’s not.

UNIDENTIFIED FEMALE: [inaudible].

NORM RITCHIE: No. [Period.] And so there's many groups that talk about it but nothing really happens. That’s my own frustration coming through.

ERIC OSTERWEIL: You know all these communities where such things go on. Would you think that ICANN should identify the places where it has the purview to provide remediation that can't otherwise be done and then participate in these groups and then offer those services or reach out to those groups and say, “Tell us what we could do,” and then use its purview to help influence those groups?

JENNIFER BRYCE: Kerry Ann has her hand raised. Kerry Ann, can you go ahead, please?

KERRY ANN BARRETT: Can you hear me now?

KC CLAFFY: Yes.

KERRY ANN BARRETT: Finally. Hi, everybody. The only thing I would probably want to input on the discussion that you're having now is before we include it and even go down that road, is just to confirm – I don't know who’s more familiar with ICANN’s bylaws, just to make sure it’s something that they can do within their remit. It would make sense for us to recommend something that is that involved unless it’s something that is actually under remit that we could either have actioned or [inaudible] looking at more actively. [inaudible] that one.

NORM RITCHIE: [inaudible] actually do this, if I recall correctly, which is a good point. Bylaws can be changed as well though, right? The other thing is that the [CCT] also went on extensively about this, so we should reference that and perhaps cut and paste. Cut and paste, no, that’s off the record.

ERIC OSTERWEIL: Okay. IDN domain names [glyph phish.]

NORM RITCHIE: Yes, that was mine. Is that something [I want to] look at? I don't think there are that many IDN domain names, but that doesn't mean there's not going to be in the future. And I actually don't know where that is at right now as far as what restrictions and what you can have in IDN domain name. For instance, can you have a glyph phish on Facebook by putting in things that look like Os?

ERIC OSTERWEIL: I think there's an SSAC document with recommendation about this. I don't know what the number is. I don't know if KC's got [encyclopedia recall] for which – there's a SAC about homoglyph attacks, right? SAC document?

KC CLAFFY: [inaudible].

ERIC OSTERWEIL: So probably, you can just say, "Implement the sac document," whatever, because I think they cover it.

KC CLAFFY: [inaudible].

ERIC OSTERWEIL: I could be wrong, I just for some reason have the recollection that SSAC took that up at one point.

DENISE MICHEL: I think information gathering on this is a good first step. I do am curious as to what the state of ply is here.

ERIC OSTERWEIL: Okay. Yeah, there's lots of art on homoglyph attacks, so we could find something and come to speed on what has and hasn’t been done and recommended, etc. Absolutely.

Okay, proactive anti-abuse by registrars and registries.

DENISE MICHEL: I think that’s relevant to and can be folded into the previous items above.

ERIC OSTERWEIL: Is that a good place for it, or above that? I think that’s where we’ll put it.

NORM RITCHIE: Yeah, that’s good. I just want to expound on this a bit. With the kind of demise of public WHOIS, that doesn’t alleviate – before, the community did a lot of the proactive identification of abusive domains and relayed those to registrars. That’s not happening anymore because they can't do it. But the registrars still have the information, they can do it themselves. And the registries in some cases can also do it.

So what we're saying is that need is still there, someone's got to do it, so maybe they should.

ERIC OSTERWEIL: So, should that be its own bullet? Because even though it's sort of part and parcel with the above, it is tackling a big item, it is a big deal. Maybe we should pull it up by itself and point out exactly what you just said. The public WHOIS is sort of like the dodo. The problem and the data are both still there, so it's actually in effect shifted the responsibility. Enshrine that somewhere.

KC CLAFFY: The RDS document makes an exact recommendation about what you wanted. Denise says there needs to be a very clear process for submitting WHOIS inaccuracy reports and [inaudible] transparent and documented on the website. Interesting.

ERIC OSTERWEIL: Okay. IP space hijacking. That's really interesting, because some people do claim that IP is an address space. It's actually a namespace, and so –

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: But numbers are –

NORM RITCHIE: That’s mine. So we get concerned about domain name hijacking, and that’s obviously abuse, but then when you say IP space hijacking, everyone says, “No, it’s not.”

DENISE MICHEL: [inaudible].

NORM RITCHIE: I know.

DENISE MICHEL: [inaudible].

NORM RITCHIE: Yeah, can ICANN or the ICANN community do anything about it? Probably not.

DENISE MICHEL: [inaudible].

ERIC OSTERWEIL: Yeah, so announcing a prefix illegitimately, if you can determine that eventually, it may be allowed, like hijacking a fourth level domain [and somebody say] like this belongs elsewhere in the hierarchy. But one thing that maybe is under the IANA purview is whether a region attests to addresses that are not assigned to that region.

UNIDENTIFIED FEMALE: [A region or an RIR?]

ERIC OSTERWEIL: Yeah, an RIR. And then you would wind up talking about RPKI pretty quick. So you could say ARIN is – yeah, you'd have to account of the transfers. So assuming that IP space was never transferred, of the simplicity of it, you could say if the space is being announced in the wrong region, attested to by an RIR in the wrong region, that that might be a purview. But I don't think the RIRs tend to do that so much as it just gets announced in the wrong place. So I'm looking around for people's appetite on this one.

KC CLAFFY: I don't know, maybe we mention it.

ERIC OSTERWEIL: Okay, we'll leave it here. And the perpetrator of this kind of behavior is doing it at a place outside of ICANN's purview, so it 's sort of like I'm doing something in the active routing system, so the most I could imaging tying it back to ICANN is if that was being represented as being owned by a region other than who IANA had given it to, and it hadn't been transferred, to Russ's point. So it's sort of like it's two or three steps beyond where the actual abuse would happen, but we could leave it in there because it feels like something's there.

KC CLAFFY: One thing [I would] say is ICANN should make it clear what the roles and responsibilities are for this particular vulnerability, and what role it could play, which is a pretty limited one.

ERIC OSTERWEIL: Just to make sure I understand, so we could put some text saying ICANN should essentially do an informational statement about it?

KC CLAFFY: It is identifier abuse. There's no question about it.

DENISE MICHEL: So yeah, it's certainly within our purview. I would say we don't have to have an answer to it, but acknowledging it as an identifier abuse, perhaps without a home. And now I'm squarely stepping in the space of brainstorming. This could be one of those areas where we say this is an SSR concern, and we think ICANN should partner with XYZ to do some additional research in this space and elevate the discussion of what potential short- or long-term measures should be taken if we feel that that's the direction to go in. That's just kind of hypothetical. Or we think that this simply isn't right for addressing. This is not something that I'm really familiar with, so I'll leave it to Norm to guide us, or KC or someone.

KC CLAFFY: [inaudible] for addressing, it's just not clear what.

ERIC OSTERWEIL: The reason that I'm not nixing it personally is we haven't said almost anything about numbers, and admittedly, that doesn't mean we should run out and say something [and] misstep about numbers, but I think there is a meta point here that's really worth underscoring, which is that ICANN does have a role through its IANA function to deal with numbers, and we should outline what kinds of abuses or concerns there are there for us to point out. Because we talk about the IANA registry, a much often forgot component because it's really important to not forget about it, and the numbers are there too. It's just not a very operational role for ICANN, so abuse tends to happen in the operation realm, so that might be why we're struggling to connect these dots. But I feel like leavening this here for now and then we'll circle back.

DENISE MICHEL: Sure.

KC CLAFFY: Norm indicated – and the IETF may be the appropriate place to start a focused discussion on this, and ICANN has as liaison to the IETF, and that could be a path.

ERIC OSTERWEIL: Okay, actually, I just thought of it. So one concern is that when one region [attests to] space that's held by another region, and that would be disambiguated by an IANA global root. I believe the [IABs] made a statement about this at some point.

RUSS HOUSLEY: And they withdrew it.

ERIC OSTERWEIL: No, they didn't.

RUSS HOUSLEY: Yes, they did. So they said five equal roots is just fine.

ERIC OSTERWEIL: When did that happen?

RUSS HOUSLEY: After I left the IAB.

ERIC OSTERWEIL: [inaudible]. I think it would be just peachy to wind up suggesting some aspect of the global IANA root.

KC CLAFFY: I think the IP space hijacking is actually a very useful thought experiment, because the architecture and implementation of ICANN that makes it so hard to do anything about IP space hijacking is actually the same architecture implementation constraints that make it so hard for it to do anything about abuse. It's just sort of where it sits in the ecosystem, who are the players, what are their incentives. And we just ignore it like it's not in the room, but it's actually a pretty instructive phenomena. We just don't know what to say about it yet.

ERIC OSTERWEIL: Is it unreasonable to ultimately wind up with some kind of recommendation that says that ICANN should commission a study that outlines this and promote awareness around the problem? Okay, alright, let's think on this one. So, backburner.

KC CLAFFY: Yeah, let's move along.

ERIC OSTERWEIL: Okay, so registrar account compromises. Okay, so maybe we'll take an item to review that and see if there's some recommendation we can lift out of what's probably already recommended in there, that kind of thing.

DENISE MICHEL: Wouldn't this go under the registrar/registry subgroup in ICANN SSR rather than DNS SSR? I have an organizational question. This is fully within ICANN’s remit, right? Registrar account compromise, would that not be under ICANN SSR and the registrar/registry work?

ERIC OSTERWEIL: Okay.

KC CLAFFY: A lot of this stuff would be.

DENISE MICHEL: It’s a good addition, I think.

ERIC OSTERWEIL: Addition to move there or to keep it here too? Move there. Okay, I'll yank it. Okay, let’s just make sure that when we get back to that, we remember SAC 74. Okay, DNS lies. So, false responses from DNS lies, DNSSEC. Anyone have any thoughts while the rest of us digest? Okay, no support.

Okay, now we’re down to the last section, so now we have DNS flag day.

UNIDENTIFIED FEMALE: [Killed.]

ERIC OSTERWEIL: Killed. Universal acceptance. Not really, IDN’s not –

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: I don't think so. This is about like are the clients able to understand what's coming across to them from the DNS. So it's really about the software that's consuming from the DNS and how's it doing these days, right?

KC CLAFFY: [inaudible].

ERIC OSTERWEIL: It's a fair question. Okay, looks like it's about to be lost. Well, a lot of the stuff that we're doing is we're talking about doing some conscientious observation, so if we did decide it was an issue, we could say you need to track how many public versions of whatever the heck or doing however, support what fraction or something or another. But I think the first question is, is it in SSR? Sounds like we're not on the same page there. It could be a security issue.

Alright, thumbs up, thumbs down. How many people want to –

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: Yeah, but I'm pushing the agenda.

JENNIFER BRYCE: Kerry Ann says, ”I think we could keep it and track it.”

ERIC OSTERWEIL: Okay. That’s a thumb up.

JENNIFER BRYCE: Also Kerry Ann says it may have [shaping] recommendations later.

ERIC OSTERWEIL: Thank you. Okay, IDN. I think that’s covered by universal acceptance if it’s whatever. Should we just treat that one as a duplicate?

Alright. Homoglyph attacks browser display. It’s not completely different [inaudible]

KC CLAFFY: [inaudible].

ERIC OSTERWEIL: Okay, canonical form, lack of.

RUSS HOUSLEY: [inaudible].

JENNIFER BRYCE: Kerry Ann is asking if someone could elaborate. I'm not sure which point on.

ERIC OSTERWEIL: Okay. Kerry Ann, we'll circle back if you want to jump on audio or type it up. Okay, two strings that look the same have different bits in DNS, I think that's – I'm just going to delete that, it's a dupe, right?

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: DNS over TLS.

KERRY ANN BARRETT: Can you hear me?

ERIC OSTERWEIL: Oh, yeah, we can hear you.

KERRY ANN BARRETT: Some of the list that we have right now, [I think a lot of it really] [inaudible] in terms of technical details, and [inaudible] going into that level of granular detail [inaudible] some of those technical areas. I was wondering if somebody could elaborate as to how we came up with that. I missed it [inaudible] how we came up with that level of detail at the end here.

ERIC OSTERWEIL: I'm sorry, Kerry Ann, did you ask how we came up with that level of detail?

KERRY ANN BARRETT: Meaning, what were we thinking? If we go down to that level of detail at that point, when we get to that point, [inaudible] hoping to achieve to get into that granular level of technical [inaudible] getting really into the technical side of it [is] really granular. I just wonder what we are hoping to achieve from the review perspective. [inaudible]. Can you hear me?

ERIC OSTERWEIL: Yeah, we can sort of hear most of what you're saying but we’re kind of missing a few words at a time. So, are you asking how we wound up getting to such –

KERRY ANN BARRETT: I'll try typing it, and I apologize [inaudible]. I'll just type it up.

ERIC OSTERWEIL: Okay. Thanks. Sorry about that. Okay, while Kerry Ann types that up, we’ll move to the next one and then come back. So, DNS over TLS. There isn't. We could look at the SSR issue of having kind of cyclic redundancy with x.509, WebPKI verification, the bootstrap DNSSEC verification. But I don't know if that's something that we want to take on here.

LAURIN WEISSINGER: Do we want to put that into a kind of wider encryption point into future challenges? Not that this doesn't exist yet, but to kind of have one point about that.

ERIC OSTERWEIL: I feel like that's a much better suggestion. How do we enshrine notes like that? Because I don't know which document I put in that we –

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: Oh, so leave it here and just make a note of it? Okay. That was a great suggestion, thank you. Testbed [of] software variance, nameserver, resolver, etc. for regression testing.

LAURIN WEISSINGER: I think recommending to have something like that would make a lot of sense, very useful to be able to test, obviously.

ERIC OSTERWEIL: Something like that?

UNIDENTIFIED MALE: Yeah.

ERIC OSTERWEIL: Any other thoughts? ICANN, OCTO or something, or commission something or whatever. But basically, this is a service to verify plans for processes like KSK roll or something like that. Anything something's going to happen, there should be a test where we say run through the testbed and see how the regression test went.

LAURIN WEISSINGER: Just for example, you could imaging giving this to some research institution to set this up.

ERIC OSTERWEIL: Or contract or pay someone or whatever, but just the service needs to be there, is what I would say. Okay, where are the procedures tests? Applies to all. That must be a fragment, right? Okay, I'm going to take it out. I think it's a fragment of something [inaudible] jumping up and championing it. Okay, before any –

LAURIN WEISSINGER: Sorry, this was mine [inaudible]. This is a more general point for most of the things we had, which is essentially that we would like to see some form of procedures, checklists, something like that when it comes to a lot of the functionality. This is why it says applies to all, so it would apply to all the points we were discussing. Sorry, outside a category, that is.

ERIC OSTERWEIL: Okay, so I should delete it here and we should just weave it into our DNA like with these things, or do you think you want me to enshrine it somewhere else?

KC CLAFFY: [inaudible].

LAURIN WEISSINGER: I think this makes sense. Can we kind of put this in a general category or something like that?

ERIC OSTERWEIL: Okay, I tagged it as like a meta comment and I'll highlight it.

Okay, we're done with round one. I'm going to propose a ten-minute biobreak, which means that we'll be back here at 2:43 and change, and then we're going to do the culling.

Okay, we're picking back up. Is the recording paused? And if so, can we unpause?

JENNIFER BRYCE: Okay, thanks. The recording is resumed. This is the second afternoon session of day two face-to-face meeting. Over to you, Eric.

JENNIFER BRYCE: Thank you, Jennifer. Okay, yeah, we're going to go on a time bounded expedition until 3:30, which his just over 35 minutes from now, and we're going to go back through the items in the DNS SSR that we just went through, and we're going to do what we're calling the culling. We're going to go through here and we're going to ruthlessly expunge those things that we don't think are likely to yield high-value return if we go through them so that we can prioritize our work and focus on things that we think are likely to deliver the most value.

So, with that in mind, not, "Is this a good idea or a bad idea," but, "Is it worth prioritizing and keeping, and will it wind up being something worthy of our time or not?" I'd like to go through and just do a very simple "keep," and if you want to keep it, speak up, and if you don't, silence means it gets expunged. So in other words, everything that we're going to keep has to have some level of advocate support. In other words, if you don't speak and you care about something and it's gone, you only have one person to blame.

Okay, starting at the top, root zone management. The first one we have is – they've changed a little bit. Data sharing, data release. What data sharing and release is currently available? Am I reading this right?

RUSS HOUSLEY: I remember the last bullet here, "Get update from ODI." I think we need to do that step, so I think –

UNIDENTIFIED FEMALE: [inaudible].

RUSS HOUSLEY: Okay. That’s my thought.

ERIC OSTERWEIL: Yeah, if it makes sense to, that’s fine. Cool, so there was a little bit of support, which is more than zero, so it’s kept. Okay, next one. DNS root crypto is a meta category, so jumping into that one. “For all of the below disruptive changes in general, determine what the metrics of success are and the go/no go checklist criteria are, to be updated by KC.”

KC CLAFFY: Well, that was one I wanted [inaudible]. That bullet was something I thought should be [inaudible] out because it’s relevant way beyond cryptos, to the software compatibility stuff and any change.

ERIC OSTERWEIL: Okay, so I'm going to highlight it in green, per what we did with Laurin. If this is a meta comment, the green things mean sort of consider this generally going forward.

KC CLAFFY: Yeah, it’s fine.

ERIC OSTERWEIL: Green. Good. Okay, so elliptic curve crypto, review DPS and academic work on the efficacy of [inaudible] for DNSSEC proposed bla bla. Any support for this one, keeping elliptic curve considerations in? I see no support, I'm about to nix it. No one’s saying they want to keep it.

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: Okay, then yellow highlight means we give it [a future.] Yeah, you can do that if you’d like, Russ.

UNIDENTIFIED FEMALE: Next.

ERIC OSTERWEIL: Okay. DNSSEC [below or the root.] TLD DNSSEC deployment. Outline existing data sources for this, [inaudible] for this.

KC CLAFFY: [This one] again was like how much DNS [inaudible] root. Basically, just tracking it.

ERIC OSTERWEIL: Yeah, this is basically making – important to have an archive of this data available.

KC CLAFFY: That's important.

ERIC OSTERWEIL: Okay, it's kept. Next one, KSK roll frequency and process, look at HSM replacement. Literature search of past deliberations over whether to roll the KSK or not. KSK specified in SP 800-81-2, section 11.2.4. DPS to be amended with lessons learned from KSK rolls, to include process considerations, etc.

RUSS HOUSLEY: Given the recent HSM problem, I think we have to do this.

ERIC OSTERWEIL: Agreed. Kept. Okay –

KC CLAFFY: [inaudible] lesson learn that you talk about in here to turn into a checklist. Have a checklist [inaudible] by the – because that's what they said, "Oh, we have to do it once to figure out how to do it." Which is true, it should help, so let's make sure that we understand how it helps.

ERIC OSTERWEIL: Okay. That's in there. Yeah, I just screamed it in there so no one will ever forget. Okay, periodic tabletop for rolling KSK, ICANN to conduct and report results from periodic tabletop exercises of KSK rolls. I think it’s a good idea. Okay, kept, unless someone argues, which is fine if you do. Okay.

BCDR plan, ask for any references that point to this modulo the above, recommend that one be created, published and maintained followed by measured audits. I think that’s a little A. Maybe it’s a big A. [inaudible].

MATOGORO JABHERA: Is that not [inaudible] on the business continuity for the yesterday session?

ERIC OSTERWEIL: No, this is for the root.

RUSS HOUSLEY: Just for the rootzone [inaudible]

MATOGORO JABHERA: Okay. Thank you.

ERIC OSTERWEIL: Do people think it’s important to have a business continuity and disaster recovery plan for the root?

UNIDENTIFIED MALE: [Yes.]

ERIC OSTERWEIL: Yes? Okay, it's kept. Alright, name collisions. Review, audit, discover domain issue, identify what the status quo is, review literature on name collisions and status of NCAP. Does this group want to do some work on name collisions, or not? Okay, it's kept.

Rootzone change management, verification, etc. Review the document that outlines procedures being used to assess whether this is well covered by existing report, acknowledge if it is. Sanity checks of requests. This is basically when the root changes, are they being conscientious about it, and do we know what the process is, and is the process well-known to the community? Do we want to spend our time on a recommendation around this? Okay, I see a yes. kept.

RUSS HOUSLEY: If we're going to do that, let's say verification and authorization.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Okay, cool. Root server system, E, G, L-root. L-root operation's SSR. Review the existing report –

LAURIN WEISSINGER: Before you go to the second one, I have a question for first one, rootzone management. [Just also called] rootzone management, and there are two topics. One is TLD label management, which you don't have here, and there's a lot of stuff there. another one is NS and DS records management [in the] rootzone. So what about these two topics? Because we have here a lot of, I think, also recommendations, so we can just copy paste it over there.

ERIC OSTERWEIL: Do you mean in addition to that bullet, or elaborate on that bullet?

LAURIN WEISSINGER: In addition to that. [Not] in addition to that as a sub-bullet of the first one. So one should be TLD label management, and the other should be NS, DS record management in the rootzone. And there is also something about change management and so on, so we have also stuff there.

ERIC OSTERWEIL: Okay. We have rootzone change management, and I've added TLD label management and NS, DS record management as separate items. That look good to you? Any objections or any support? How many people think that's a good idea? Okay. I just want to make sure there's more than zero.

Okay, moving forward. It's reverse culling, Russ.

RUSS HOUSLEY: Yeah, I've noticed that. We're adding [inaudible].

ERIC OSTERWEIL: The day is young. No, it’s not. Okay, root server system E, G, L-root. L-root operations SSR, review the existing reporting, ODI, etc. on L-root stats. So, does anyone support keeping this? Okay, it’s gone.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: It’s not that these are – so we've already established that all these we consider to be good, the question is now priority. Like if we don’t want to be doing SSR for the next three years, and we want to wrap it up at some point, we want to sort of pick the things that we think are tractable and high-value enough that we can focus on them. So we've grown, not shrunk so far on the culling, so it’s fine if that is what it is, but this is a gut check, not to say whether these are bad. In fact, maybe what I should do is use the strikethrough.

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: I'm trying to find the strikethrough option. For some reason, I can't find it. The hotkey wasn’t – okay, that way we can keep it but we know we struck it. Alright, best practice, look for publication that indicates L-root’s adherence to publish best practices for RSOs, L-root technical leadership, lead by example. Who wants to keep this? Okay, we have support to keep it.

Capacity to handle all root traffic. Look at published aggregate stats of global root traffic and global capacity of L-root, ensure that stated capacity of L-root meets or exceeds global volumes. Who supports keeping this? Okay, I'm going to strike it.

Okay, system hardening. Publish statement from L-root ops of hardening that is done to infrastructure. Alright, it’s kept.

Root server system protection. Assess the threatscape of top threats, e.g. DDoS to the root system. Was the threatscape documented and shared with the community/RSOs? So I see –

RUSS HOUSLEY: This was done last July.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Okay, so then does that mean that we want to keep it and it'll be easy to write, or we should strike it because we don’t want to do it? What does that mean?

RUSS HOUSLEY: Because Lyman and Jim Reid wrote it.

ERIC OSTERWEIL: Okay. I'm not sure but I'm thinking it sounds like striking it. Are we keeping it or striking it? Who supports keeping it as an item? Okay, it's kept. Yeah. If it's already done, this looks like it'll be a slam dunk. So I could see why you want to keep it. Alright, we're going to come back to this one while I move forward with the culling. Everyone wants to look at the document. Please do enjoy. Alright, root server system evolution. Review existing root server ecosystem documentation, evaluate the need for further investigation. Who thinks we should keep this one? Struck.

RUSS HOUSLEY: We said the threatscape.

UNIDENTIFIED FEMALE: Yeah.

JENNIFER BRYCE: Kerry Ann says it's worth a yellow.

ERIC OSTERWEIL: Okay, so we'll make it a yellow. Okay. Yellow, punt it to future. Thank you, Kerry Ann. Okay, L-root management strategy, how is it being maintained, how is it being distributed, how do you obtain copies, site selection criteria, how do ops respond to incidents? What is the computation around increasing capacity? Do we keep this one? Who wants to keep it? Boban wants to keep it? Okay, and so does Laurin. Alright.

I'm starting to think we should have two assents to keep things, otherwise we're going to keep growing instead of culling. The new rule is two assents.

Comment on RSSAC document around proposed governance model for the root server environment. And there's a link, recommends the strategy, architecture and policy function to offer guidance on matters concerning the RSS.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Okay, I'll make that a sub-bullet.

KC CLAFFY: Implementing that work, that proposal that RSSAC came up with, would be millions of dollars, maybe per year. And the big question, like with many of these things we're recommending is, what is not going to get done because of that little bit [inaudible]? I think. We're not thinking on those terms, but I found it very compelling [inaudible].

ERIC OSTERWEIL: Okay, that sounds like an assent. I see heads nodding, we're kept. Okay, alternate root deployment and coexistence, DNSSEC make it all harder. Accountability and transparency with respect to risks and benefits. Annual report commissioned yearly studies the result, in public [inaudible] of the state of alternate roots on the internet risk and benefits tracking and measurement deltas etc. Cannot police but can report public impact versus coexistence.

JENNIFER BRYCE: Kerry Ann says to keep.

ERIC OSTERWEIL: I agree. That's two. Okay, SSR measurements. Top-level domain SSR measurement – I think these are just primers up at the top. SLA compliance. SLA for what, with whom? A mechanism to be put in place that measures SLA compliance. IANA services, TLDs registries covered in ICANN SSR, registrars covered in ICANN SSR. A mechanism to track and verify that SLAs are being met. Any support for this one?

JENNIFER BRYCE: Kerry Ann supports.

ERIC OSTERWEIL: Okay, that’s one. We need one more.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Kerry Ann. Oh, and Boban. Okay. Alright. I saw Russ salivating out of the corner of my eye. Sorry, Russ, will not be culled at this time.

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: Okay. Propagation delay and consistency of changes of zone contents across nameservers. Yeah, I think it's important, but that's only one voice. Okay, it looks like it's struck.

KC CLAFFY: [inaudible] find it?

ERIC OSTERWEIL: Yes, because the act of doing –

KC CLAFFY: For all we know, it's up there, we just don't know where.

ERIC OSTERWEIL: No, I know it's not up there because I've heard people ask for it before, and I know it's important. If you want –

KC CLAFFY: [inaudible].

ERIC OSTERWEIL: Okay. It’s kept. IANA registry availability measurements, security. Request a public documentation of the infrastructure and service level SSR aspects of how IANA registries are served and maintained, like time zones. Okay, Boban says keep. We've got one keep.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Okay, yeah. It’s kept. Sorry, Russ. Identify KPIs for SSR measurements. Request commission analysis of KPIs for the root, others.

UNIDENTIFIED FEMALE: Russ is going to go in tonight and just delete [inaudible].

ERIC OSTERWEIL: Can we lock Russ out of this document? Okay, I don’t hear any support –

JENNIFER BRYCE: Kerry Ann wants to actually keep that one.

ERIC OSTERWEIL: Okay. Kerry Ann wants to keep the KPIs. We've got one vote. Do we hear two?

RUSS HOUSLEY: I can't wait until we put names next to these.

JENNIFER BRYCE: She suggests to make it yellow, so it would be her problem.

ERIC OSTERWEIL: Okay, fine. We’ll make it yellow. That'll make Russ happy. Thank you, Kerry Ann. Okay, namespace abuse. Let’s add something. Transparency with respect to abuse. Is this DAAR? Review [inaudible] agreement in the of the CCT report, e.g. TLD abuse indicators, recommend future development of the DAAR and how the community can measure it, an actual mechanism, mechanism to evaluate the utility [inaudible] community abuse data made public with API for major threat vector registries, registrars each month, public but delayed. Support?

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Okay, it’s supported.

LAURIN WEISSINGER: I recommend cutting the text though.

RUSS HOUSLEY: Making it shorter?

LAURIN WEISSINGER: Make it shorter, yeah.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: This is just to provide us context.

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: You mean from the CCT report, or from what's up on the document?

LAURIN WEISSINGER: I thought we could shorten that text, but if you think it’s just explanation –

ERIC OSTERWEIL: There may not be a single word of this that’s kept. This is just so [inaudible]. Okay, reactive versus proactive compliance. One-off complaints response versus data driven priorities. Denise to pull together relevant publications on this, CCT reviews, RDS review, SAC 101, etc. Okay, I've got one assent. Okay, two. Good.

Best practices and potential requirements, e.g. two-factor for DNS, SAC 74. Should there be a security requirement for registrar accounts? Raise awareness of best practices. Here's a link [pointing to] implementation guidance SAC 74 for user registrar account access etc. Support?

JENNIFER BRYCE: Kerry Ann supports.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Do you want me to fold it in as a sub-bullet then?

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Okay. And Kerry Ann supported. Leadership. Give ICANN Compliance a big stick to lead abuse remediation initiatives and take action. Check the bylaws and possibly suggest directions to change towards. Take other review teams' recommendations into consideration, RDS RT, CCT RT. Got one support.

UNIDENTIFIED FEMALE: [inaudible].

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: Okay. Norm, yeah. Proactive anti-abuse by registrars and registries, enshrine that the problem and the data are still around, though public WHOIS is not, and this may have shifted the onus for solving, addressing this problem. This is basically paying the price for GDPR. I have one yes. Two yeses. Alright, [inaudible].

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: IDN domain name glyph phish. Information gathered on homoglyph attacks and threatscape, possibly recommendable implementation of SAC whatever they were talking about wherever they were talking about it. Homoglyph attacks, any support?

RUSS HOUSLEY: It’s purposeful confusion of the user.

ERIC OSTERWEIL: I know, I was going to say no one is volunteering to say we want to keep it, but we’re all talking about how important it is. So you’ve all just volunteered that you think we should keep it.

Okay, IP space hijacking. Acknowledge as identifier abuse and SSR concern, propose partnership and research investigation into remediations and longer term. We got one. Alright. Come on, Boban. Do the right thing.

RUSS HOUSLEY: Well, isn't this what the [NOGs] are supposed to do? Why should we do it?

ERIC OSTERWEIL: The question, I think, that we got hung up on with regard to this was since numbers is a function, should we find something that we can address in the number space? Not because we’re looking for work, but because this is an important part of ICANN that may wind up being unaddressed in a security consideration.

KC CLAFFY: [inaudible].

ERIC OSTERWEIL: Okay. I don’t see enough support, I'm about to strike it. Struck. We culled something. We’re almost done, totally under time. Okay, software interrupt, universal –

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: Well, I have a plan. I think you're going to like this plan. Okay, universal acceptance, e.g. homoglyph attacks, browser display, umlaut –

RUSS HOUSLEY: We just did that one up above in the IDN [stuff.]

UNIDENTIFIED FEMALE: [inaudible].

RUSS HOUSLEY: Right, just whack [this one here.]

ERIC OSTERWEIL: So the reason it’s here is that this would be looking at the endpoint software.

RUSS HOUSLEY: Yeah, but just move it, because it’s all an IDN issue.

ERIC OSTERWEIL: Okay. I'm not actually paying attention to what I'm reading, I'm just managing. I'm trying to be a good manager. Alright, this is why I suck at management.

RUSS HOUSLEY: You're saying good managers don't pay attention? That's what you've just said.

ERIC OSTERWEIL: Said it loudly and proudly. I'm in academia now, I can say that. Okay, the only one left is testbed of software variants, NS resolver, etc. For regression testing, recommend that this facility be created, maintained and used. I vote for this one.

RUSS HOUSLEY: Only Eric wants that.

ERIC OSTERWEIL: No, Laurin just agreed too, so I got it. Okay, I have an idea now. So we've successfully finished our pass through the culling. Well, successfully might be in air quotes.

RUSS HOUSLEY: [inaudible].

ERIC OSTERWEIL: With our remaining time, should we go through and see who wants to volunteer to lead these?

RUSS HOUSLEY: Yes.

ERIC OSTERWEIL: One at a time.

RUSS HOUSLEY: If we don't have a leader, it's not going to get done.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Okay.

RUSS HOUSLEY: No, if we can't do that, I think we have a real problem with getting the work done.

ERIC OSTERWEIL: Okay, so then let's do that, and at this point, I'd like to propose the following procedure. If your name gets put next to something, you are just a point of contact, it doesn't mean you're alone, and you can draw people in and you can get agreement from people to help you. But it means that you're the point of contact, so you kind of have the responsibility, but don't think it's just you.

RUSS HOUSLEY: [inaudible].

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Yeah, and you're responsible for getting it written. You write it, or else you make sure someone else is doing it. But it’s on you to get it done, yeah. But you can also find that if no one will volunteer to be that person, that something will get culled, right, Russ? Yeah?

RUSS HOUSLEY: There will be a culling.

ERIC OSTERWEIL: Go ahead, Denise.

DENISE MICHEL: Yeah, and I think we need to do just a stop and check for a day or two so our colleagues who weren’t able to join us here also have a chance to catch up, volunteer for something if they so choose.

ERIC OSTERWEIL: Yeah, that's a really good point, and also, that means that there doesn’t have to be just one name. So for example, if something’s taken, someone says, “hey, I want to do that too,” of course, if three people in the room want to jump on anything, there's three names then.

UNIDENTIFIED FEMALE: Right.

ERIC OSTERWEIL: Okay, let’s do it. So we’re back up at the top, rootzone management. Data sharing, data release. What data sharing and release is currently available? Who would like to be the POC?

KC CLAFFY: Not me, but I do want to say something about this, is that –

RUSS HOUSLEY: [inaudible]

KC CLAFFY: Right, don’t cull it. For the [four URLs] that are up here – and I think this also needs to be factored out, because I think it’s true for a lot of stuff, is that there's a ton of stuff on the ICANN website, it’s just very hard to find. I take the point, what data sharing and release is currently available, but I think the recommendation has to be something about website, making the website more accessible and making this data easier to find. I don't know how to make that quantifiable so SSR3 can verify whether it’s been done, like permalink, we keep throwing that word around like that's going to be magic pixie dust. But I think that’s really the issue, because I suspect that there's a ton of data on there, that there's no more data that’s actually needed but it just needs – well, with the possible exception of ODI and ITHI, but all of the roots have stats. And indeed, the roots are doing their own stats, and so to the extent that they might be – one thing that adds to their suboptimal accessibility is that they're all different modes of doing stats.

UNIDENTIFIED MALE: Right.

KC CLAFFY: But I think we need to be careful, because I don't think ICANN can go force all the roots to do the same [inaudible] tool or whatever.

ERIC OSTERWEIL: No, but you just hit on a very important –

KC CLAFFY: [inaudible] there could be an API or something of the like.

ERIC OSTERWEIL: There should be an API, because exactly what you said, rootservers.org has as lot of data and Hedgehog has as lot of data, and DITL has a lot of data, and they're all in different formats. And if you know from firsthand experience, if you want to actually do something with that, you spend a huge amount of time massaging it and getting it together. If someone were to say – and I think this is part of the purview of ODI, this is a way to go and get data and use it in a homogentisic way – and so maybe if we look at ODI, because I don't know real well, I think someone else in the room probably knows a lot better than me, I think that's kind of one of its stated objectives, to make this actually usable and ingestible and find it – it's not so much that it has to be all in the same place as it has to be in the same format, same place – it should be.

KC CLAFFY: Well, I would assume that that aspiration would apply to everything in this list, everything on this page that has data, like DAAR. We should have an API to DAAR, or whatever that means, whatever aspect of DAAR might be shared or useful, or not.

DENISE MICHEL: For this one –

RUSS HOUSLEY: We still need a name.

DENISE MICHEL: Then would your action item not be something like so we'll ask – so ICANN staff that supports RSSAC to dump all the relevant links on one page for us?

UNIDENTIFIED FEMALE: [inaudible].

DENISE MICHEL: At least you'll have all the links, you won't have to spend lots of time searching through the ICANN website. You can take a quick look at the links and then decide what you would want to propose as a next step, potentially a recommendation. Does that work for you?

KC CLAFFY: I think so. I'd have to think about it, because like I said, RSSAC spent a ton of time, there's a whole RSSAC document on this, RSSAC 002 or something, rootzone measurements, and I think they're all trying to implement that at this place. But I guess somebody would have to go –

DENISE MICHEL: So why don't we just start with agreeing to pose a question to the ICANN staff, [support – our staff,] can you please build this, add additional links and try and help us put in one place all of the relevant links and statistics here?

KC CLAFFY: [inaudible]. I'm trying to be helpful here.

ERIC OSTERWEIL: Okay. Alright. I want to ask for someone to volunteer to hold the pen on this one. Thank you, KC. Okay, DNS root crypto, for all the below, bla bla, elliptic curve, DNSSEC below the root –

UNIDENTIFIED FEMALE: I nominate Russ.

ERIC OSTERWEIL: I haven't checked my memory to make sure that there aren't any name collisions with using initials, but I'm just putting initials.

Alright, BCDR plan, ask of any refences, point to modulo, [inaudible] recommend that one be created, published, maintained, followed, measured by audits. Boban. Name collision, review, audit, discover domain issue, identify what the status quo is, review lit on [inaudible] collisions, etc. [inaudible].

So, did you say you're ok being –

UNIDENTIFIED FEMALE: Yes.

ERIC OSTERWEIL: Okay. Okay, rootzone change management verification. Review the documentation [outlines procedures being used, assess] whether it's covered by existing bla bla, sanity checks, yada yada. This one is about to get culled. Would anyone like to volunteer to hold the pen on this? Going once.

LAURIN WEISSINGER: A question from me on this first. Laurin is asking the question. Isn't this another one where we would have to ask staff what is currently happening?

KC CLAFFY: [That's true with any of these.]

LAURIN WEISSINGER: I say we do it.

ERIC OSTERWEIL: Okay, so I think you just volunteer. Okay. Alain’s just left the room, so he's going to get the next one. Next six, sorry. That’s right. TLD label management. Okay, NS, DS record management. Is that him? Okay, root server system, L-root, best practice, look at publications indicate L-root’s adherence to published best practices for RSOs. L-root technical leadership, lead by example.

KC CLAFFY: [inaudible]

ERIC OSTERWEIL: No, best practice, we didn't do best practice yet, we’re still up here. Anyone?

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Okay. [inaudible]? Okay.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Comment on RSSAC document around proposed governance model for the root servers environment, [blah,] recommends a strategy, architecture, yada yada, performance, etc. Who would like to own this one?

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: Okay. If you need to, but you can also look at this and say that it's a rabbit hole and that you don't think it's what we should do, and we can cull it later too. So, if you think it's a simple operation and then you get knee deep in a quagmire and you say no, forget it –

KC CLAFFY: Well, no, [inaudible].

ERIC OSTERWEIL: Okay. Thank you. Okay, alternate root. Accountability and transparency with respect to risks and benefit, annual report, commission yearly studies, the resulting public reports of the state of alternate roots on the Internet, risk/benefits tracking measurements, cannot police but can report [inaudible]. I'll take this one.

Okay, SSR measurements.

UNIDENTIFIED FEMALE: I encourage you.

ERIC OSTERWEIL: Yeah.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: You can review slides first. Okay, SLA compliance.

JENNIFER BRYCE: Kerry Ann has said that she's interested in the SLAs. Maybe –

ERIC OSTERWEIL: Okay. Thank you, Kerry Ann. Propagation delay and consistency of changes of root content of nameservers. Yeah, I'll take it.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Okay, I'll put it in there with you. Okay, IANA registry availability measurement [security request] public documentation of infrastructure [inaudible] aspects of how IANA registries are served, maintained, time zones, etc. I think this one’s Russ’s, he's the one who brought up time zones. Is there anyone willing to bite the bullet on this one? Nobody. It’s going to get culled.

KC CLAFFY: Kerry Ann, don’t you want this one?

JENNIFER BRYCE: She said a couple minutes ago she's not running away but her plane is actually taking off.

KC CLAFFY: She definitely gets this one.

ERIC OSTERWEIL: It sounds like a yes. Alright, we either assign it to Kerry Ann or we cull it.

KC CLAFFY: Assign it and then [inaudible]

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: Alright, futures. Wait, this isn't futures. This is, what kind of infrastructure is IANA serving things from? Not the KPIs, the IANA registry availability. This is the one we're on. Okay. Namespace abuse transparency with respect to abuse is DAAR, review [inaudible] CCT report [inaudible] recommend future development of DAAR, is it an actual mechanism, yada yada.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: That one needs to be the most well-done recommendation based on the authorship that just signed up for it. So good luck to you all. Reactive versus proactive compliance, one-off complaints response versus data-driven priorities. Denise will pull together a bunch of stuff. The one about reactive versus proactive compliance, one-off compliance, one-off complaints. You said you'd pull together a bunch of stuff.

DENISE MICHEL: Yes.

ERIC OSTERWEIL: Leadership, give ICANN Compliance a big stick to lead abuse remediation initiatives and do great justice. Who would like to pony up on this one? Going once.

UNIDENTIFIED FEMALE: [inaudible]

ERIC OSTERWEIL: Okay, does that mean I can put [an R?]

UNIDENTIFIED FEMALE: [Norm.]

ERIC OSTERWEIL: Okay. Proactive anti-abuse by registrars and registries, enshrine that the problem of the data still around though the public WHOIS is not, and this may have shifted the onus for solving and addressing the problem. I'll help too because this is GDPR, has to be. [inaudible] means it's got objects.

Okay, IDN domain names, glyph phish, information gathering on homoglyph attacks and threatscape, possibly recommend implementing SAC something or another, universal acceptance, and tracking support and software. Not seeing support.

UNIDENTIFIED FEMALE: [Well, someone's got to do it.]

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: This is IDNs and homoglyphs. It's about to get culled. Alright. Good man, Russ. Yeah.

UNIDENTIFIED FEMALE: [inaudible].

ERIC OSTERWEIL: Oh my, how the worm has turned. Okay, last one. Culling round two, equally unsuccessful. Testbed of software variance [inaudible] regression testing – I've got this one.

Okay, so we finished the second round of culling. Both rounds of culling went in record time and were phenomenally unsuccessful, but we have now assigned duties to people. You all should feel empowered. I think almost everyone in here has something to do, right?

RUSS HOUSLEY: No, there's a couple people [inaudible].

ERIC OSTERWEIL: Oh, yeah, Noorul. Is Noorul online, Jennifer? Oh, man, I propose we go back through and we see where Noorul should fit, because he's got a lot of expertise. So, does anyone want to – I'll do another pass. Who are the people that aren't here? Noorul's not here, Kerry Ann counts because she was here for part of it. Who?

UNIDENTIFIED MALE: [inaudible].

ERIC OSTERWEIL: Zarko. Anyone else? Because we can go through with those names in mind and see who would like to – Naveed? Yeah, Naveed. Okay.

LAURIN WEISSINGER: A question. Why don’t we just create an e-mail with a table where we can see who’s having what and they have a day or two to add themselves to it? That might be fairer.

ERIC OSTERWEIL: That’s an excellent idea, Laurin. That’s a fantastic idea. I can think of one name of someone who can do that, because he thought of it.

RUSS HOUSLEY: Jennifer.

ERIC OSTERWEIL: Alright. Okay. Jennifer, you totally just saved Laurin. So, Laurin, you'll be buying Jennifer a beer later, I guess, or something like that. Alright, cool. Because usually, if you speak, you get the duty. Alright, cool. I declare DNS SSR workstream-a-palooza round one complete, Russ, and back to you.

RUSS HOUSLEY: Thank you. We have a lot to do. More to do than I actually had hoped. So, tomorrow, we will end up having to take a look at the workplan to make sure that we have a way to do this. Alright, so the next thing we're going to do to make good use of this time, I'm going to pass the mic to Laurin, and we're going to hopefully reach consensus on the SSR1 text. I'm sorry, we'll be back in 15 minutes to do that. So if you haven't read it in a while, read it now.

Okay, if everyone could get their stuff and get back to their seats so we can move forward. Next thing up is consensus on the text for the SSR1 recommendations. Laurin, having made the last edit pass through this shortly before the last plenary call, is going to walk us through it. The big thing is each of these that's not implemented and so on has either a recommendation or a forward pointer. Make sure we agree now that we're more familiar after the last two days of what there is to be forward pointed to, and so this should be the last time we talk about this section of the document.

LAURIN WEISSINGER: Okay. I'll just run through the recommendations one after the other, and I will focus on essentially always the last bit. So, is this recommendation still relevant, and what further work is needed? Or if there's already a recommendation, I'll be focusing on that. But I will kind of read out the recommendation so we know what we're talking about.

Recommendation one, ICANN should publish a single, clear and consistent statement of its SSR remit and [inaudible] limited technical mission. ICANN should elicit and gain public feedback in order to reach consensus-based statement.

Recommendation remains relevant and SSR2 had discussions regarding the development of a clear and consistent statement, as well as how to get public feedback on such a statement.

Further work is needed to bring this process to closure, especially because of the inconsistencies between different versions of the remit, see [further on] number four.

This recommendation remains relevant and we're proposing new recommendation on this topic later in this report. So, there is a recommendation coming up. Any comments on that one?

KC CLAFFY: [inaudible] making the diction consistent in this document, because sometimes, the new recommendation is in this section, and sometimes, we punt it to the future. I think we need to be – well, I don't know, or maybe we need to consider whether we want to be consistent about how we do that. And a second thing about consistency is I think we need to say whether – we need to use the same language throughout, and maybe you guys have done this for most of this, but I saw a little bit of inconsistency on, "This recommendation was implemented, this recommendation was not implemented." And then we have one that says, "This recommendation was not fully implemented."

And I notice the RDS report, and I think the CCT report, uses the phrasing, "This recommendation was partly implemented," like glass half full instead of half empty. And it's not so important which hone, but I think we ought to be consistent, and at the end, there's definitely a paragraph in the CCT and RDS report that says this number of recommendations were implemented, this number were not, this number were partly. So, we need to be clear if we have three categories, if it's yes, no, some, or if it's more than three. We just need to know as we go through this.

DENISE MICHEL: I would agree that we need to edit for consistency in terms for sure. I would suggest, given the way this review team's mandate is laid out in the bylaws, that we separate from our assessment of the SSR1 implementation from new recommendations. And if there is a specific recommended action that follows from our assessment of an SSR1 recommendation, I suggest we put in a statement that says additional work in this area is recommended, and then take all the new recommendations tied to SSR1, put those in our recommendations section, put an asterisk by them with a footnote that says, "This is a follow-on recommendation to SSR1." Something like that, I think, might be a good way of structuring it.

LAURIN WEISSINGER: Essentially, it is written along those lines. So, if some things are missing, this is just mentioned in the last paragraph, where people have written specific recommendations with the title, this is a recommendation, it is in the document as a recommendation right now.

MATOGORO JABHERA: Yes. Thank you. And I was also curious to see on how we are capturing the recommendations especial for the previous recommendations, because from the ICANN side, when we're doing the review, in most cases, there were [statements made] that recommendation was not smart, was not clear, so I think it's very important to have a phrase that give a room that the interpretations of what has been interpreted by the ICANN before the implementation be clear so that in case the next review's coming, then it understands what was the interpretation of ICANN team before the implementation of the recommendation, because without that kind of statement, then you find it's very difficult for one to conduct a review especial in case the next team [is also] undertaking the same review. That was my first observation. Thank you.

LAURIN WEISSINGER: So I think for what was mentioned, this is essentially a recommendation. At least in my eyes, it is a recommendation in itself. So that's to say if ICANN is to implement SSR-related recommendations of any sort, not only from this team but more generally, they have to establish these baselines so that they can also measure themselves against what they are trying to do. Does this make sense to everybody?

Okay, then I will quickly make a note at the bottom of this document with this recommendation. Recommendation 2 – or is there anything on recommendation 1 left? Okay, I assume no.

Recommendation 2, ICANN's definition and implementation of its SSR [remit] and limited technical mission should be reviewed in order to maintain consensus and elicit feedback from the community. The process should be repeated on a regular basis, perhaps in conjunction with the cycle of future SSR reviews.

We say this recommendation is still relevant given the SSR activities and challenges that the ICANN community faces. Further work is needed. Specifically, regular reviews of the SSR remit have not happened. There have been no opportunities to comment specifically on the mission statement since 2013. Current definition make it difficult to assess the implementation.

[There] follows our recommendation. Using a process that is aligned with the community review of the ICANN strategic plan and ICANN operating plan, each time the SSR framework is updated or changed, the community should have an opportunity to comment on ICANN's [inaudible] and implementation of its SSR remit and limited technical mission.

Everyone happy? Number three, once ICANN issues a consensus-based statement of its SSR remit and limited technical mission, ICANN should utilize consistent terminology and descriptions of this statement in all materials.

We said that this is still relevant, and that we did not find procedures that are used to ensure that these defined terms are used in all materials and communications. We did, however, find that there are inconsistencies.

Further work would include updating current definitions where needed, publicize them appropriately and establishing procedures to ensure consistency.

Our recommendation is to develop a public glossary for the ICANN community, and then develop procedures that ensure the terms in the glossary are used in all materials and communications and revisited, and if necessary, updated on a regular basis. This process should have an owner within ICANN Org who would also be responsible to provide clarification of the terms when needed.

KC CLAFFY: I'm trying to put myself in the head of SSR3 and see this and how would I know that it’s been done. That applies to all the recommendations, but I wonder if we need to think about the measurability of these things. And of course, how are we going to go find this glossary? Are we going to google for ICANN glossary? Because we did a whole crapload of that for this review.

[I don't know, minor thinking.] Can you put these in italics or something if it’s a new recommendation for each of these?

LAURIN WEISSINGER: [inaudible]. My interpretation of that would be, is there a glossary, yes, no? Has it been updated? So with version control, which we should probably include. And having an owner, that can be checked. So, I would say we add the version control and then it should be trackable. KC, is that okay?

KC CLAFFY: [Yes, that’s okay.]

ERIC OSTERWEIL: Can I ask a question? Regular basis, is it concerning to actually give a target for what the period [inaudible] is just so it’s measurable for SSR3? Like once a year, once a quarter? Whatever, just something.

UNIDENTIFIED FEMALE: [inaudible].

LAURIN WEISSINGER: We can say annual, but it might be that something comes up that you want to do outside that annual cycle.

ERIC OSTERWEIL: How about specify that it has to be at least touched with the last update –

LAURIN WEISSINGER: Okay, at least annually.

ERIC OSTERWEIL: At least annually, including if there's no changes, with an update stamp on it or something like that.

LAURIN WEISSINGER: Okay, everyone happy with the text now? I take silence as a yes. Okay. Recommendation number four, ICANN should document and clearly define the nature of the SSR relationships it has within the ICANN community in order to provide a single focal point for understanding the interdependencies between organizations.

We say this recommendation is still relevant. Whenever questions about ICANN's SSR relationship arise, there should be comprehensive and formal [focus point for] understanding SSR relationships with other organizations in- and outside the community.

Further work is needed to update this document and to provide a new resource that meets the intent of the new recommendation. This could be a similar table that is kept up to date. It should indicate what relationships exist, what aspects they cover and how they're maintaining in contrast to the current form where no indicative information is given for the majority of entries. If information is to be omitted in the public-facing document, information should still be filed.

So, this is one where the idea is – so this is what Denise was talking about. So here, we're just saying this has not been implemented properly, and we give some pointers as to how this could be done. This is why it's not a full recommendation. However, if people aren't happy with that, we can put his in recommendation 4.

KC CLAFFY: All of these recommendations that we have here we also need to have later [in a sort of] all the recommendations together and asterixis if it's an SSR1 sort of rewrite. But in this case, is there a rewrite, or is it you're just going to use the old recommendation four and, say, add this clarification to it? Now we seem to be of the method that we used in the last three.

LAURIN WEISSINGER: The idea is essentially here that no recommendation was written, and in the text, we're just referring to how the initial recommendation could be implemented but has not been implemented. So, the question is, do we want to write a recommendation for that? If we do, we have to write a recommendation essentially per recommendation, because there are very few that have been fully implemented. To continue on this, this would mean that we're coming in with 25 or so recommendations just on SSR1 alone.

ERIC OSTERWEIL: Honestly, my just personal opinion, not hats or anything like that, is that if that's our response, if that's our view of things after we've looked at the implementation status, then that's fine. In other words, if SSR1 said this is important and we say, "Yeah, it's important, it wasn't done," I think we're essentially recommending [it does again,] and I don't think that it's our fault that we have however many recommendations we come up with, plus however many there were before. I think we shouldn't shy away from it just because that's a big number.

But I do agree with KC's point that I think when we get down to the actual writing, the recommendations section should all be in one place.

KC CLAFFY: [inaudible]. As a reader of the segment, I do actually want it to be here as well as in some sperate executive summary of all the recommendations, because here, I want to say, what has the review team done to make it clearer? And I don't get that from this text for this recommendation. And even I'm still a little struggling on the previous ones to make it measurable. Like I think one aspect of this that made it hard for us is there isn't a single permalink page for this information.

UNIDENTIFIED MALE: [inaudible].

KC CLAFFY: I know. And for example, we say this could be a similar table that is kept up to date, it should indicate what relationships [inaudible] it feels already – information needs to be omitted, information should still be filed. I don't know what that means. Filed where? I want a recommendation to say so and so should do so and so, and it should be in an easy to find place.

Even in the previous one where you said there should be somebody assigned to this, I think we should say the person who's assigned to this's name should be on the page so that SSR3 people know and don't have to go dig around and try to figure it out.

LAURIN WEISSINGER: I think this would be tough to do, because we don't necessarily know who would be responsible right now, and particularly not who might be responsible in a year.

DENISE MICHEL: May I make a suggestion? I think after we're done with the final report, I think a set of post-implementation page be created. We've committed as part of this process to be available for implementation questions, so I think when the dust settles and we're sort of done with the final report, before we go our separate ways, create a table with key contacts for the various recommendations, I think it'd probably be easier than incorporating everything as we go into this report. There are going to be many things we're going to be just swarming on, it'll be hard to identify a key person, a person's name may be tracked from the overall consensus recommendations.

[inaudible] I really like your idea though, and that's super useful to have, contact this person as a lead on these recommendations. That'll be really helpful in the future, and for staff as well implementing them and others.

LAURIN WEISSINGER: In relation to writing SSR1 recommendation 4, do we want to add a specifically recommendation-worded recommendation?

KC CLAFFY: For one, two and three, there's a section underneath our assessment that says new recommendation, blah. This is the first one that we don't have that, even though the paragraph above it is basically a new recommendation. So, my question is, why are we being inconsistent about this?

LAURIN WEISSINGER: This is my question: do we write it? It was not available in the documentation. So, essentially, this is what I was saying before. If there was no document recommendation written, in some cases, there is no recommendation yet. So we're writing one right now. Right?

KC CLAFFY: [inaudible].

UNIDENTIFIED MALE: [inaudible].

NORM RITCHIE: [inaudible] a lot of recommendations, and some are obviously going to be more hard-hitting than others. Some are even fluffy. Are we going to weight or prioritize these in any way, or are they just all going to say "recommendation" so you have –

UNIDENTIFIED FEMALE: [inaudible].

RUSS HOUSLEY: What do you mean by prioritized?

NORM RITCHIE: Well, not – weight.

UNIDENTIFIED FEMALE: [inaudible].

NORM RITCHIE: Yeah. “This is big, this is nice to have.”

ERIC OSTERWEIL: [inaudible] text around something that we think was kind of vague and we’re trying to help to implement, we could just say it was not implemented instead of – we could do it this way, and that’s where we’re getting kind of wound around the axle. We could just say, “We didn't find that it was implemented.” Done. Right?

KC CLAFFY: Move all the other recommendations above, where we insert it.

ERIC OSTERWEIL: Wherever we’re coming to [inaudible] over trying to write text, and is it measurable and smart and etc., if we don’t have to say anything, we don’t want to say anything, we could just say we found that it wasn’t implemented. [Pass.]

KC CLAFFY: For all of them, we went through this exercise of saying it’s still relevant. If it’s still relevant, then what? I think that’s even part of the question, what else is needed? So we already did back ourselves into a corner by designing it this way, I guess.

UNIDENTIFIED MALE: [inaudible].

KC CLAFFY: No, I'm not happy about this either, I think it’s going to be a spaghetti document. But all I'm saying is we need to be consistent about what we’re doing.

ERIC OSTERWEIL: Okay, so Laurin, you’ve done a good job writing some text and there's some things in there like you could do it this way, you could – should we just sort of make Laurin’s text more directive and say it like, “Do this?” You're being nice in the text saying different ways you could do different things. Why don’t you just say, “The recommendation was not implemented. We want to see the following.” And then this tractable, specific, concise.

KC CLAFFY: The document, because –

LAURIN WEISSINGER: So, essentially, the problem is the following. This document is based on a table, and there was supposed to be an editing process by the whole team. This has not happened sufficiently, full stop. And this is the problem we're facing right now.

While I did a lot of editing and Russ did a lot of editing, we are not able to essentially crate this out of nowhere. This is what I was trying to say before in response to Denise's points. This is essentially the problem. I cannot just write all these and come up with them.

KC CLAFFY: [inaudible] otherwise, you decide you punt it, you say we're not going to include a recommendation inside the assessment of the previous recommendations, you're going to put those in some other document later, and you leave the reader – and I'm not saying this isn't the right thing to do, I just want to point out – going, "Oh, they've said it's still relevant today, and yet we have no idea what they're going to do about it."

DENISE MICHEL: Yeah, I'd say further work is needed on this recommendation, and then if the team feels that that work should be part of our recommendations, then let's put it in the recommendations section, say this is a follow-up to SSR1 recommendation blah, and we recommend the following actions be taken, is what I was thinking we were going to do.

LAURIN WEISSINGER: I would be happy with that, and I think it makes more sense. I was raising this on a call before, because we don't know what our other recommendations are, and I think this is why some of it is, to some extent, up in the air.

So our assessment is there, but the follow-up recommendation is not there yet, because we don't know if there might be a recommendation that covers multiple of the ones we speak to. Coming back to before, this is one of the reasons why I just can't sit down and write them right now.

ERIC OSTERWEIL: Plus one to what Denise said.

LAURIN WEISSINGER: Okay. So, I just put the 4 into a recommendation-type wording already, and we're just going to move on to 5. Is that okay? Okay, ICANN should use the definition of its SSR relationship to maintain effective working arrangements and to demonstrate how these relationships are utilized to achieve each SSR goal.

We say the recommendation is still relevant today. ICANN should be encouraged to do routine SSR reports and should [inaudible]

[END OF TRANSCRIPTION]