ICANN70 | Virtual Community Forum - Joint Meeting ICANN Board and SSAC
Wednesday, March 24, 2021 - 14:30 to 16:00 EST

>> Recording in progress.

WENDY PROFIT: Hello, and welcome to the joint meeting between the Security and Stability Advisory Committee and the ICANN board.

My name is Wendy Profit, from ICANN Org, and I'll be the remote participation manager for this meeting. Please note, we are holding this meeting as a Zoom webinar. Be advised that the floor on this session will be reserved exclusively for the interaction between the Security and Stability Advisory Committee and the ICANN board members.

We therefore have the members of both groups promoted to panelists today and they are the only ones able to speak in the room. Please note that the SSAC panelists on the call are those whose names were provided by the SSAC treble.

For our panelists, please raise your hand in Zoom in order to join the queue to participate. All panelists are muted by default, so you may proceed to unmute yourself when you're given the floor.

Before speaking, if you would please ensure that you have your audible notifications muted and clearly state your name. Please also bear in mind to select the language that you will be speaking within Zoom, including English.

Also, please remember to speak slowly for the scribes and the interpreters.

Bear in mind that the board will only take questions from the constituency with whom they are in session.

Consequently, the Q&A pod is disabled on this webinar.

Interpretation for this session will include English, Spanish, French, Arabic, Chinese, and Russian.

Click on the interpretation icon in Zoom and select the language you will listen to during the session.

For all participants in this meeting, you may post comments in the chat. To do so, please use the dropdown menu in the chat pod below and select respond to all panelists and attendees. This will allow everyone to see your comment.

Note that the private chats are only possible in Zoom webinars amongst panelists. Therefore, any message sent by a panelist or standard attendee to another standard attendee will also be seen by all other hosts, cohosts, and panelists.

This session includes automated real time transcription, which you can view by clicking on the closed caption button in the webinar tool. Please note, this transcript is not official or authoritative.

Finally, we kindly ask everyone in this meeting to abide by the ICANN Expected Standards of Behavior. You may view these on the link provided in the Zoom chat.

Having said this, I will now give the floor to Maarten Botterman, chair of the ICANN board.

Maarten, the floor is yours.

MAARTEN BOTTERMAN: Thank you, Wendy.

Thank you everybody, Rod and SSAC, for joining the ICANN board for this session so we can actually not only look at each other's

papers, but also talk together interactively. And that's what we look forward to do.

So, for this session, Merike Kaeo, the SSAC liaison to the board, will moderate the session from our side.

So, Merike.

MERIKE KAEO: Thank you, Maarten.

And welcome to all my board colleagues and my SSAC colleagues. So very excited to have this session and have some very fruitful discussions.

The agenda for today will be from the SSAC side, we will be presenting our recent publications, as well as some ongoing work. And after each of these presentations, I invite my board colleagues to ask any questions, either for clarifications or, you know, other related questions they may have on the work items.

And the recent publications that we've had are as follows. You see this on the agenda slide.

Some that were just -- came out in the last couple of days or will be coming out shortly. But we just recently published SAC116, which are the SSAC comments on the SSR review team final report.

SAC115, the SSAC report on an interoperable approach to addressing abuse handling in the DNS.

SAC114, which are the SSAC comments on the GNSO new gTLD Subsequent Procedures Draft Final Report. And then also the Name Collision Analysis Project and ongoing work right now in the SSAC with the work party on routing security.

So without further ado, I will let Rod open it up.

ROD RASMUSSEN: Thank you, Merike.

And thank you to the board for spending the time with us today.

We have a lot of work that has come out, literally, hot off the presses in the last few days, as well as significant work that we've done over the past period since our last -- since the last virtual ICANN meeting, and some ongoing work that we wanted to spend some time discussing.

We really look forward to having an interactive session here today. We have some fresh materials, and it's a great time to be answering your questions and getting into some of the more details that may not be evident from just reading the reports themselves and spend some time discussing ways forward.

There are a lot of security issues that are top of mind across the ICANN community right now, the SSR2 report having just been put out. We have just published a long-anticipated and promised report on DNS abuse, which may be the first of many different pieces of work there. We'll have that discussion around what that all entails.

And then issues with the subsequent procedures and next rounds of TLDs have -- we took a look at that from the SSR perspectives and have a lot of comments in there, both very directed and more meta issues that I think would be good to be having a fuller discussion with the board and the broader community about as we go forward on these things.

And then some ongoing work that we have there.

So the first one here is on -- we're going to go back, basically, in reverse order with the latest publication, which is our comments

on the SSR2 report. Let me see which slide you're on here. I've got four windows open here.

If you go forward a couple of slides. And I'll be covering this one for this session. There we go.

So just to give you a quick flavor for this, if you haven't had a chance to take a look at this yet, it's a very short response, which I think that will probably surprise a few folks in the community since this is the SSR report.

But this is the area that you might say is fundamental to the SSAC itself. And there are a lot of things in here. A lot of -- a diverse set of topics, with very specific recommendations around how to address these various SSR issues that have been brought up within this, you know, years-long effort by the SSR2 review team.

And so at this point, we -- instead of diving into trying to do a very, you know -- a super thorough analysis of where that ended up, we really focused on our support of the conclusions behind those recommendations. Not necessarily the recommendations as written themselves, but the basics on what was behind this, and wanted to emphasize that the issues that are brought up in this SSR2 report are really important and should be addressed and prioritized. And that we, as the SSAC, are committed towards

working with the board and the organization on these individual aspects, having discussions about how they could be addressed and thinking about, you know, moving forward into reviewing those things and how they might be implemented or eventually adopted in some form within the community, doing our part to help shape those things that are the most pressing and then the ones that have board -- the board may have the biggest questions around.

We also wanted to make sure that we had given our appreciation for the amount of work that the SSR2 team did and making sure that they used the SMART approach -- that's an actual -- that's all caps, SMART. It's a metric-based approach, which is useful in codifying how you're going to be able to achieve goals, et cetera. And given those prioritizations.

May I have the next slide, and then we can open this up to discussion.

Yeah.

There were a couple of things we brought up. And just more as flags within the document that we submitted around making sure that there are really the resources and the ability for the organization to be able to implement a lot of stuff, there's a lot in

there. And SSR2 report does reflect that there's a lot of things in there. And they had time scales for -- that were, you know -- they tried to be pretty realistic about how long some of those items may take. But there is a lot of resource that would need to be dedicated towards addressing those issues, regardless of the approach taken. So that was something that we wanted to make sure that -- to raise that as a concern around just overall being able to take all those things on and prioritize them, et cetera.

Again, not necessarily a criticism of any sort. Really just a, wow, there's a lot of work to do here. Can we actually get this done?

And then there were some areas where, based on the feedback from the initial draft and feedback that we had provided, which was very detailed input to the draft report that was taken back into account, there were a few areas where the SSR2 team came up with different approaches than what we may have recommended in our response. And that's not necessarily a bad thing. There's lots of ways to approach these issues. And I think based on just hearing some different responses throughout the community, that there would be quite a bit of feedback as to how to address these issues and whether the ways proposed by the SSR2 team is appropriate or not.

But our -- And we didn't get into those details. What we really wanted to emphasize was that these are important issues that do need to be addressed in some form or fashion and that we will be doing our bit to help the board and org as much as possible as you move through this and prioritize and look at implementations and things like that and provide some directed input on specific issues as they become ones that need to be addressed.

And with that, I think I will pass it around for questions and clarifications, et cetera, that folks would want to have on what we've said here.

MERIKE KAEO: Yeah. Thank you for that, Rod.

And I did see a question. I was going to answer -- I typed in the question -- the response. But I just want to reiterate that the SSAC does give the board a 48-hour preview of its advisories and work, whenever feasible. And this was done with SAC116 and 115. So they are not yet public, but they will be public by the end of the day today.

So just for anybody that's following along and looking for these publications.

But I believe, Danko, you had a comment or question?

DANKO JEVTOVIC: Yes. Thank you, Merike.

My name is Danko Jevtovic. I'm part of the two board's liaisons to the review team. And Kaveh and myself, we are also chairing the board's caucus on the SSR2.

So, first of all, thank you for this advisory. And, yeah, you are right, I was a bit surprised that it's so short. But the point, the main point I'm reading here is SSAC's willingness to help us in this process.

So this was a very long review, and the board is very thankful for the review team for doing their work, and also for SSAC's support throughout all of this process.

And we are now -- we have to do the board section on the review recommendations, if I remember correctly, by 25th of July. But the public comment period is still open until some date beginning of April, 9th or so.

So the board, through the caucus, has started to go into all the (indiscernible) recommendations. And as you noted, it's a lot of work. And, of course, we will have to prioritize.

Also, as you noted, recommendations are there, but we also do see the underlying questions or issues that are very important for board's consideration about the security and stability that's very important for us. So I would actually like to ask SSAC, because you stated in your comment that you are committed to supporting the efforts of the organization and community in responding to the SSR2 final review and to provide further datas and commentaries.

So the question from the board would be, what type of analysis can the board request from the SSAC as we move towards the consideration of the final report? And, of course, once we oversee implementation of the accepted SSR2 recommendations.

Thanks.

MERIKE KAEO: Rod, do you want to answer for this one?

ROD RASMUSSEN: Sure. And thank you for that. That's a really important question, Danko. And it's -- it's really one that I think is one that's -- one we should be taking up in a dialogue.

There are lots of ways to approach that. There could be a longer-term, deeper dive into these issues. You know, the public comment period is -- and I know that it got extent just before it was going to be over in the first place. But taking a look at just the massive amount of things that were really in the SSAC's, you know, kind of remit that were included in that and just the ability of resources, it was not really feasible for us to do it justice.

But one could do that. I think more the approach that I think we'd like to take is to look at issues that are ones where there are questions. Now, there's -- some of the recommendations and topics in this report are pretty straightforward and probably don't need a lot of kind of interpretation or debate, et cetera. But there are some that are very interesting, let me put it that way, in there that can certainly be dug into quite a bit and have some -- you know, if there are specific questions to be answered or areas where it would be good to have further, you know, expert opinion brought in, we have that capability of being able to concentrate on, you know, an issue or two at a time and do that better justice for the board and maybe the organization, depending on what

stage we're talking about, to be able to have some further thought put into this and feedback.

And anywhere in between. I think this is a good opportunity for us to discuss how we may be able to interact and take advantage of our limited but very useful volunteer hours that we put to this, to our membership, and provide a resource to the community that can be useful.

This SSR2 review is fundamental towards ICANN's mission, which is one of the things we wanted to emphasize with this short report and how can we best leverage our capability to help move these items forward.

Hopefully that's helpful.

DANKO JEVTOVIC: If I may respond briefly, yes, it's very helpful. And thank you so much. We are counting on you. Thank you for this encouraging statement.

And just, for example, one of the items I noted in your comments, it's about SSR1 recommendations. The review team found out that none of them were fully implemented. But as you noted in your report, those recommendations are not defined -- specified

in a way that they can be clearly set. So the Board also has a challenge because of the review team in their recommendations said they have to be revisited. But the question is, it can be defined from different perspectives. So we might need expert help in those.

Some of them, as you noted, were better defined in the specific SSR2 recommendations so it's easier. But this general statement of going through all of this is not easy.

And as a personal note, I must say that it happened before I engagement in ICANN in this way. I was with the ccNSO and managing a country code registry. But we know some of the people who are on the SSAC were engaged in ICANN at that time. So some help might hopefully come from that end. Thank you.

ROD RASMUSSEN: On the SSR1 recommendations, to be fair to everybody in the ICANN world, all of us have evolved in how we're doing these things, right?

So putting those recommendations into context in the SSR2 recommendations and recasting those with actual metrics, et cetera, I think is a useful step. Certainly they would make it a little

easier for a SSR3 hopefully to be able to give a final determination -- (laughter) -- on whether they are implemented or not.

DANKO JEVTOVIC: Thanks.

MERIKE KAEO: Yeah. So thanks for the dialogue. I will also add I am on the Board SSR2 caucus. And I would very strongly encourage that as there are topics where there's SSAC-related input, that would be useful to then ask the SSAC to maybe have -- you know, create a meeting to have a dialogue around these items, especially because there are different alternative views that can be had for different security aspects, which are not wrong, right? They're just alternative views. And so it may take -- the discussion may be better than actually trying to get something in written word. So thank you very much for that.

I also state that a lot of the SSAC members are in multiple work parties. So with the SSR aspects, because there's so many details to be covered -- and the time for comments, even with the extension was really rather short, that the SSAC did feel, as Rod had stated, that a dialogue would be much more effective and efficient overall.

All right. Anybody else want to comment on the SSAC's SSR2 report or comments, rather, to the final report?

Okay.

I don't see anybody chiming in, so let's move on to the next topic, which would be SAC115.

ROD RASMUSSEN: Thanks, Merike. I will hand it over to Jeff Bedser here in just a moment, if he's been promoted and is there.

This is great to see. There's almost 200 people listening in on this. This is terrific participation by the community.

I wanted to set this up a little bit. SAC115 is a look at the handling of abuse reports. And we spent over a year on this. It's evolved over time. And instead of having one big giant comprehensive report on DNS abuse, what we did was we looked at a particular area. There are many other areas that can also be examined. What we looked at here is the identification or porting and handling of abuse and appropriate parties to work with and some thoughts around that, which I will let Jeff dig into here in a minute.

At the end of this, we have come to a recommendation that we engage in a broader dialogue around how to do this because the DNS, as part of the abuse ecosystem, is a part of it, not the entirety of it.

And there are a -- it's a broader universe and a problem set that is befuddled and created great consternation for decades now in how to deal with this. There may be a way forward given the impetus, both in the ICANN community and elsewhere, around trying to standardize the approaches to this, whether it's across borders or even just within borders. There are a lot of complexities to this issue. But we believe a dialogue moving forward will be helpful.

You will note as well there were some -- we published some alternate views and some sense within the work. As I said, we've been at this for quite a while. And this is an area where our recent upgrades to our operational procedures, we have a process to provide thinking where we have members who have some different thoughts about how to approach things, can get that in there while at the same time we keep our -- the SSAC advice out there so it's not watered down or diluted. That's important. I think it's -- those areas that are touched upon in that section of the document are the ones that have a lot of interest in debate

and those are the things to take into consideration as you are reading this as well.

There are lots of approaches towards looking at these problems. So I want to just help set that context.

Jeff, do you want to talk about -- we've got three slides on this. If you want to run through that, if you are available.

JEFF BEDSER: Sure. Thanks, Rod. And thanks, everybody, for taking the time today. My apologies for being slightly late for this call. Life got in the way, but luckily I jumped in just in time for this section. So something must be working out for me today.

As the title of the document says, the keyword is not abuse or DNS but it is interoperability. Basically, we took the approach that this network of networks that we all work on, work in, and facilitate to even this meeting is based on a principle of interoperability and everything working together. And, basically, what this paper tackles is the issue that interoperability is not something that's been common in the DNS abuse space. We're talking about a space that has many different businesses and many different players and with different sets of guidelines and rules, which is the gTLDs versus the ccTLDs, registries, registrars. And, of course,

you've got hosting companies and you've got content-delivery networks and all those issues. So there isn't a common interoperability model to manage abuse throughout there. We think there's a problem space there that can be addressed that can move this topic on DNS abuse forward within the ICANN community.

So we do work on some -- defining some aspects of the problem. We talk about what existing supporting mechanisms and resources are around.

We talk about primary points of responsibility for abuse resolution. When I say "responsibility," I'm talking about those who are taking the responsibility to get it resolved. I really don't have a lot of time for "This is not my responsibility, this is another party's responsibility." It's not about who is responsible but will responsibility to reduce the abuse.

Evidentiary terminology and standards, it is based on what we looked at in this paper. And evidence response to abuse is the best one moving forward. Wherein, when a report of abuse comes forward to any player in the infrastructure, who will take the responsibility for getting the abuse addressed? Having it well-evidenced on a standard that everyone agrees to is the best way to move the ball forward quickly because at the end of the day,

we all acknowledge that the shorter the life span of a domain being used for abusive purposes, the less victimization there will be from that domain and, thus, how better the ecosystem is across the path there.

Escalation path between parties need to be established and worked on.

And then, of course, reasonable time frames for action and depending on the severity of the incidents, severity of the type of abuse.

And then, of course, availability and quality of contact information so that there is a party to contact to get abuse resolved wherever in the ecosystem it should get resolved.

The proposed path we came up with looks towards harmonizing efforts to address abuse across this vector and looks for the community to engage in further efforts to work through interoperability on abuse handling across the ecosystem.

Next slide.

Well, I think I may have gotten ahead of myself slide to slide. Apologies.

The lack of coordination does lead to inconsistent approaches. And opportunities do exist for the creation of a single entity, a common abuse response facilitator, if you will, that could convene to facilitate, guide, and provide clarity and predictability so that when something does get escalated, how do you escalate it, how do you know where the right point in the ecosystem is to enter a complaint of abuse based on the type of abuse. All those things can be worked out by a common facilitator.

ICANN has played similar roles in another initiatives that overlap with its mission. But the remit will extend to the wider Internet ecosystem, which is one of the reasons, again, we're not recommending necessarily that the ICANN Board take a direct action on this but facilitate and encourage common interface with not just the members of this community and contracted parties but the other parts of the ecosystem where the abuse also does reside.

Next slide, please.

So Recommendation 1 is that SSAC recommends the ICANN community continue to work together with the extended DNS infrastructure community in an effort to examine, refine the proposal for a common abuse facilitator, and to define the role

and scope of work of a common abuse response facilitator using SAC115 as an input, which is the name of this document.

This community effort should include domain registration providers that are part of the ICANN community, communities beyond the ICANN community, such as DNS infrastructure providers, content-hosting providers, incident response community, and, of course, the anti-abuse community that detects the abuse. Other organizations that have worked on Internet abuse as well.

And while SSAC acknowledges the opportunity and need to create the anti-abuse efforts in this report, it's not advocating for any further organizations or entities to fulfill them.

I think that may be the last slide, but let's check. Is there another slide?

ROD RASMUSSEN: That is it.

JEFF BEDSER: That is it. So back to you, Rod.

ROD RASMUSSEN: On the last -- on the recommendation there, one way -- We frame it this way within the paper, but I think it's important .

Probably want to add that to the slide for our meeting tomorrow, come to think of it.

The thing is we think about the Internet as the interoperable network of networks, and we've come together and created standards for how to actually interoperate whether that's the dissemination of identifiers, that we're all familiar with here, or the standards by which traffic is recognized and shunted around and what the format of that traffic looks like, et cetera, et cetera, et cetera.

The idea here is that we need to think about handling abuse in a similar fashion and how can we interoperate with ways that we can create efficiencies and meet expectations, et cetera. And the world that the -- and the rules that we have within the identifier space, in particular, name space, are a part of that, but they're not the entirety of it. And solving a problem in one place is not necessarily going to solve it for -- make it a compatible solution for other parts of the ecosystem. So where can we do that together?

For those of you following along with the Internet Jurisdiction Project, they just released their new -- what do they call them now? They call them cookbooks. There's a very, very cute name. I'm spacing, I'm not remembering what they call them. But their approaches to some of these issues, that is an example of an effort in this space. There are many others as well.

But because we've been having this conversation within the ICANN community itself and saying how are we going to deal with this -- and there's been a lot of desire to do so -- can we make sure that whatever we're doing in trying to address these issues actually is compatible across the entirety of the ecosystem where abuse is being handled and it's got to be handled by the appropriate folks who have the -- the ability and capability and -- to be able to be able -- to be able to address those things in the appropriate fashion.

Göran, you have your hand up. Please.

GÖRAN MARBY: Thank you very much. I -- if I may, just a couple of questions on the presentation we just heard.

But you might have answered some of them, because is this in addition to a potential policy or is it instead of a potential policy?

ROD RASMUSSEN: So the -- probably in addition to a potential policy is -- any policies done within the ICANN sphere is going to be necessarily limited towards what ICANN can actually create policy in. And that would be, you know, a gTLD and perhaps ccTLD and gTLD type policy area. The problem space is bigger than that, but it intersects. If you think of a Venn diagram, there's a big intersection between things that ICANN can do and things that are -- you know, that abuse touches on. There's an area that overlaps.

And there may be policies within the ICANN world that will address the issues, especially when it comes to how to properly handle abuse issues that involve the identifiers themselves and the need to respond within that -- within that as a solution set. But those should still be compatible with a broader view on how abuse is tackled. And that gets outside of ICANN's remit. Fully admit that's one of the things that folks who had some concerns about our document brought up. So it's a matter of how do we try and craft things that are smart for within the area that ICANN does have remit that are compatible with what other people and other efforts are doing, especially since abuse can cross barriers, so to speak, or cross boundaries -- not barriers -- boundaries between those two universes, where there's several different parts of an abusive activity, and some of that may involve an

identifier that needs to be addressed versus -- yet there are many other components of it as well.

So having a -- I think -- you can think of ICANN having an important seat at the table in that discussion and then helping driving that forward, but it's not simply something ICANN has any -- the community and org, et cetera, have any capability of solving on its own, if that makes sense.

GÖRAN MARBY: It makes a lot of sense. I'm sort of in the listening mode. And that question came up to me. Because I'm always afraid that we end up in the same discussions, like we end up with how are we going to do compliance with this and who owns this role and what is the definition of abuse?

As you know, there are -- speaking to GAC members and others, once they realize if you go away a little bit from the target abuse we have, we might end up in freedom of speech legislation, freedom of expression legislation, for instance. So it becomes very -- as you point out, Rod, it becomes very entangled. And then, of course, you have privacy legislations, et cetera, et cetera.

But thank you. I always think it's interesting to hear new ways of trying to solve an issue.

ROD RASMUSSEN: And I think -- and this got brought up by a couple of our members. I was trying to think about it in this way of interoperability and just putting a different light on it, which I think is a useful analogy, because it's one we're used to. It's why these multistakeholder models were created, whether it's us or the IETF or various other bodies that have come up to try to address the various things going on on the Internet.

There's -- there may well be an opportunity here to do something where you think about the interoperability of dealing with the different issues that arise.

And I see there are some questions about the definitions of abuse. We didn't try to redefine abuse. We pointed out that there are some areas that have been used commonly within the ICANN sphere. We didn't come up with and try and redefine things, as far as that goes, within the paper, and, rather, concentrated on how to deal with the signaling, so to speak, of dealing with abusive issues and not yet -- putting yet another definition out there, so to speak.

At the end of the day, you can think of abuse in a very generic form is that something is going on that is impacting somebody else,

and they would like that activity to be modified in some way. And that's a very generic term.

Again, there's a whole bunch of legal stuff and a whole bunch of technical stuff, et cetera, et cetera. Just at the end of the day, having a way of being able to properly notify parties that are involved in activities that are being viewed as abusive by others is a generic kind of technical and interoperational thing that can be done without having to get into the detailed legalities of what's what. So, in other words, you can solve a -- you can create systems for solving problems. Whether or not those problems will be actually addressed or not becomes more of a legal and other area of types of places to create the -- craft solutions. That is not what the scope of this paper is. The scope of this paper is around how do we -- how do you best figure out who to send -- who to work with and how to escalate things and what those things -- what some of the various challenges are in doing those things.

Hopefully, that helps put a boundary around what we've tried to do with this work for you.

MERIKE KAEO: So anybody else from the board have any questions on -- regarding this particular advisory?

Becky.

BECKY BURR: Thanks. And thanks to the SSAC for this.

You guys are not going to be surprised to hear, because I'm sure you have heard from the community that there's concern about SSAC sort of weighing in on a policy issue that is subject to the policy development process in the community in the absence of the kind of security, stability, and resilience issue that really is, is the DNS going to run? How many -- you know, we heard the last time around that, you know, some number, some large number, of new gTLDs could be added to the root without destabilizing it, provided was done over time in a reasonable way. And so some of these issues related to balancing the value of introducing new gTLDs on the one hand and addressing issues like abuse as part of this process on the other, were part of the policy development process, although, admittedly, the subsequent procedures folks suggested that the approach to -- to abuse had to be holistic across the gTLD environment, not just the new gTLDs, and has made that suggestion going forward.

But I'm just curious as to a -- a sort of pretty broad, blanket statement regarding rethinking whether this is in -- whether adding new gTLDs is consistent with ICANN's mission in light of

what we've heard in the past regarding the fact that the introduction of new gTLDs, at least up to a point that we haven't reached yet, does not pose a fundamental threat to technical security issues.

MERIKE KAEO: So should we be going through SAC114?

ROD RASMUSSEN: I was going to say, it sounds like you're reading ahead.

MERIKE KAEO: Yeah.

BECKY BURR: Oh, I'm looking at 114 now. Sorry.

MERIKE KAEO: Yeah, that was just the introduction for what we were going to talk about.

So, Rod, how would you like to handle this?

ROD RASMUSSEN: Well, actually, if you could -- whoever's got control of the slides, if you can move back one slide. I've got, like, six windows open, 'cause I'm looking ahead on my own copy.

So we're still on 115. Let's clean that one up, and then we'll run through 114. And, hopefully, Becky, we'll be able to talk to directly what you're talking about there on 114. But let's clean 115 up first and then we'll move on to that one, if that's all right with everybody?

MERIKE KAEO: Yeah. Were there any more comments specifically on the DNS abuse advisory? Akinori, you have your hand up.

AKINORI MAEMURA: Thank you, Merike.

Thank you very much, SSAC people, for bringing up this other advice.

My question is a little bit simplified. Do you expect the board to create this -- the Common Abuse Response Facilitator? Or what do you expect to -- for -- as a reaction to this advice?

ROD RASMUSSEN: Great. And thank you for that. Excellent question.

No to your -- to be specific about -- for the way the recommendation -- we went back and forth on this one quite a bit as well.

Really, what we're recommending is that the board and community participate in this broader discussion. And having a dialogue about how to best do that is really the next step. And that's an area where we'd like to be able to engage with you on that.

Is that -- One model you might think of would be the Universal Acceptance Program, where ICANN has convened and helped get that going but has not, you know, actually been the organization, so to speak, that has contributed to that.

There is participation in other ongoing efforts out there. I mentioned the INJ stuff. There are other efforts that are going on amongst some of the contracted parties who have done -- have gotten together on things. There's -- I think we've mentioned several examples in the document of efforts that are out there.

But to focus the -- some of the energy that has been bubbling up here the past year and a half within the ICANN community and focus that on having a broader dialogue and encourage -- and probably some outreach to other organizations that are looking at these issues to see if there might be a convening of some sort of broader dialogue that could then work towards this idea of interoperability within handling the -- the ongoing operational handling of abuse and making that efficient and seeing where then the role of ICANN can help fit into that.

But that's not any specific -- we tried not to be too proscriptive here, and, rather, to use this document as a kickoff towards having a conversation about how to best approach that. But to also break us out of kind of our internal -- I won't call it navel-gazing -- but kind of in a silo of looking how can we do this within the world of registries/registrars, and the name space without -- but at the same time, people, very rightly so, say, hey, this is a much bigger problem. This is not our job to solve all abuse issues. There are some abuse issues that fall into our area because they were -- of the way they were crafted. However, it's a much bigger problem.

So let's actually do that; right? And bring those -- that -- see if we can reach out and bring together a broader set of stakeholders to try and take on this -- this interoperability issue.

Hopefully, that solves that.

AKINORI MAEMURA: Thank you very much, Rod. That actually addresses my question. Thank you very much for -- again for this innovative idea. And this kind of innovative idea need an innovative solution. And that's for us all to think about that. Thank you very much.

MERIKE KAEO: Great, thank you. Are there any more questions or comments from my Board colleagues?

Okay. I don't see any.

So, Rod, why don't we go ahead with SAC114, and maybe if you can answer some of Becky's questions that she had posed prior to going through this.

I guess, let's continue to go through the slides first.

ROD RASMUSSEN: That sounds great, yes, Merike. I will definitely try to address some of what Becky brought up. And then we can probably -- because there was a lot in those questions.

[Laughter]

It's a good setup for walking through this, too.

So SAC114 is our extended response to the final subsequent procedures report. And just to give you some background about this, as we're going through the final report -- by the way, excellent job and work that was done by that subsequent procedures team. There was a lot of really thoughtful things put together there. Very thoroughly researched and well-presented. So please don't take -- for those who worked on that so hard, don't take our comments here as criticism of that work. We thought it was, in general, a very good piece of work that would really be helpful.

But as we were going through that, we looked and some questions had come up. It was clear from discussions that some of the topics that we had concerns around weren't really within the charter of that PDP to look at. So we had some of these, what we called, metaissues which we addressed in the first three recommendations that kind of went beyond the scope of what the sub pro team was tasked with. So that's important context for that -- for our report here.

And there were some that we actually had some dialogue that the sub pro team was gracious enough to set up a session where we had an interaction and talked through kind of some of the specifics within the paper. We bring some of those up here within this document.

But this is one of the reasons we've directed this at the Board is because we have these meta issues and where else are we going to address this to because it's not -- there are some fundamental questions. And this is an area where I think it's good for us in our ongoing dialogues about how we address some of these issues, were they most appropriately done and how is the community going to deal with those overall going forward. There's been a lot of discussions amongst us and the SO/AC chairs, et cetera, around these responsibilities. I think this is a good example of one of those areas where we are going to bring these things up for discussion and they should be -- they should be hopefully listened to. But the question is how do you deal with them.

Another thing, too, is that we looked at this strictly from a SSR perspective. There are many other considerations, economic, cultural, et cetera, et cetera, that we are not making any comments on here. But we did have concerns that we wanted to think about strictly from an SSR perspective and the expansion of the usage of the namespace. There are some fundamental

questions that do get brought up about, okay, how big and to what extent.

And another important distinction is the second bullet point here. That's the word "delegation." At the end of the day, the concerns are -- that we have expressed don't manifest until you actually put things into the zone and they start resolving.

So up until then, everything is more operational and there are other considerations to be brought to bear around how to deal with some of these issues. But up and until you actually delegate something is when problems that we're concerned about may actually manifest, right? So that's an important context to have for this.

Can I have the next slide, please.

We have a few slides here, talking about the main recommendations here.

And the first one is around this idea of looking at the overall expansion. And this is the meta-meta issue, I guess you could call that, and having this as part -- I think the timing is actually quite good because I know we're going to have a session to talk about updating the strategic plan and thinking about is this meeting

strategic goals and is expansion an appropriate way of meeting the overall goals.

The answer could very well be yes. In fact, probably depending on how you weigh things, it will be. We wanted to bring up some of these things from the SSR perspective. And just the very basic thing, the more complexity you add to a system, the more likelihood that you might have something go wrong. You're just having complexity, and that's just kind of a generic truth, so to speak, is that you -- as you create more and more component parts and it expands, there may be capacity issues you're just not aware of because you're now crossing orders of magnitude beyond where you were before. What are those impacts? And do we understand them? And are we willing to accept those risks? So you can see those bullet points there on some of the areas that we wanted to make sure we address.

One of the things in particular -- and if I could have the next slide because this goes with Recommendation 2 as well, in particular -- is thinking about things from beyond just the root system itself and kind of the base-level TLDs and thinking about impacts throughout the DNS ecosystem, so caching resolvers and applications that use names, et cetera. Are we -- are we taking that into consideration as we're actually pushing these things out?

If you think back to when the TLDs, kind of the first round, when you had TLDs that were longer than expected that broke software in various places, that's just an example from the past where things have impacts that weren't necessarily anticipated. I know there's still some issues out there with Web forums and things like that that don't accept certain kinds of TLDs that may be too long, things like that.

Whether or not that's a particular issue that is, quote-unquote, a showstopper, anything like that, is not what we're trying to say here.

What we're saying is are we looking at the entire ecosystem and what are our measurements for that, for understanding where those things are going to be and do we have a good plan for that.

And then -- a very practical one, because this was -- it was part of the discussion around the -- many people asked the sub pro team about, is on DNS abuse. They rightly said DNS abuse isn't not just about new TLDs, it's about all TLDs. And our response to that is, yep, that's true so let's get that work done and understand those things. Because there were definitely some issues that arose as part of the new TLDs that were done in the last -- in the 2012 round where there were specific issues and do we have those

understood. Do we have best practices put in place to ensure we don't repeat the same kind of failure modes and are those going to be ready to go? And there's several reasons for wanting to do that as part of going -- getting this out there. One of the fundamental things that we have concerns about is the reaction that various other parties in the ecosystem had to specifically high abuse issues which for a lot of TLDs made them literally unroutable, or at least run unresolvable, for many parts of the Internet as people said, Nope, we're not going to interact with things that have that as a TLD and the concern that brush might be -- that people are painting with, therefor, not including those, might lead to a much broader impact on all TLDs that get put out as the technologies and capabilities for people to filter, block, and et cetera, have become more and more sophisticated over the last ten years. So that's a real concern for the success of the program, is understanding this and making sure the reaction from the rest of the ecosystem does not jeopardize putting out additional rounds.

And then we had -- go to the next slide. These are the three metaissues. We had specific things that were tied to the report. First one is kind of a catchall. There's a whole bunch of little stuff in there. This is one of the things to take into consideration, probably more on the implementation side than anything else.

There was a desire, I think, for there to be a better set of educational materials, et cetera, so that new providers can get up and running. Some of the challenges we saw with the adoption of DNSSEC were likely due to people getting it set up but not necessarily having operational experience, for example, and having reference materials and the like and doing things like that would be really useful.

Intended use as a defining characteristic for contention sets, there's a whole section on that and what some of the challenges there are in doing that.

And then the -- we have the ongoing work with the NCAP project where we're getting concerned about delegation of domains before we have -- that work took place so we can have a good set of standards for understanding risks and of potential collisions, et cetera, so that we don't have those being put into the zone without having gone through a process.

I believe that was the last slide in this section. Yep.

Go ahead and go back one.

And I see -- I thought I saw another hand up. I see Göran's up right now.

And, Becky, before I go to Göran, I want to make sure that I at least touched on the many questions you had. But if there's some you feel that you would like to dig into further, I give you first dispensation on that, if that's all right.

BECKY BURR: Thanks. Let's go to other people. I mean, I think my concern is that meta concern that other people have questions about as well.

MERIKE KAEO: Göran, I see your hand is up.

GÖRAN MARBY: Sorry. This is third week of an ICANN meeting, so it might be said my brain cells are more loosely coupled than they usually are.

Just thinking what you're saying about the next round of DNS abuse and what you talked about previously about the more holistic view on abuse, because I got the impression that when you talked about abuse, DNS abuse, the holistic approach -- and you mentioned not everything can happen within ICANN.

On the other hand, you think that ICANN should do more things when it comes to specific DNS abuse. And I have a small problem connecting those things because -- and I'm not taking sides because I do believe that this conversation belongs to the ICANN community.

But if I compare, for instance, numbers of DNS abuse, I often think to myself why are the DAAR numbers so different from other numbers. I bet one of the reasons is definitions. There's a broader definition of "DNS abuse" for someone else which we don't have. And that's fair. The other one is that it could be that you go into the CC specs where ICANN doesn't do policies, they do independent policies themselves.

So if you take those two things, my question would be sort of: Do you think that as a part of this, what you actually want to talk about, if you want to be specific, is the actual definition of the DNS abuse for the next round and broaden it or sharpen it or going around it or something? Is that what you're expecting for the next round?

Because I have a problem. I like the holistic approach really much because we all know that there are spam filters out there. There are different kind of filters you look into things. The telcos around the world have programs looking at child pornography, looking at

the actual traffic, et cetera, et cetera, so there are many parts of this.

So I don't get it, Rod. Can I admit that?

[Laughter]

ROD RASMUSSEN: That's fine.

The -- I think the -- trying to reconcile what we have in the DNS abuse paper versus this particular issue on understanding abuse within TLDs, this was extremely high in the 2012-plus rounds, is -- I see where there's -- you can get confused there.

Think of it this way, though, what we are talking about in this whole holistic approach is around the operationalization of reporting and incident handling. Right? That's a separate topic space than a TLD having a very high rate of registrations where abuse is created within it.

So that's a different set of the -- that's a different problem space within the overall space of abuse and subspace of DNS abuse, where that -- you had measures that some of the new TLDs probably had in place that prevented those domains -- or

prevented their spaces from being abused for malicious registration purposes. That's a different set of questions than how do I -- once I have something that's being abusive, who's the right person to talk to or what are the right evidentiary standards, what are the right communication standards, et cetera, in order for that abuse complaint to be dealt with in an appropriate manner. That's a separate issue. That's an operational, signaling, et cetera, issue.

What we're talking about here is that you had very -- some TLDs with very high rates of abusive registrations actually in them. And there's a different -- likely a different set of tools, some of those probably being operational, some of them being best practices, some of them being potentially policy-related that you can use to address the creation of those -- of those abusive, malicious registrations within that particular set.

Defining abuse more consistently across different communities may be helpful there, from a measurements perspective. But at the end of the day, if you have a TLD where you're getting reports of 50%-plus abusive registrations in it, it's going to cause a certain set of, you know, responsive behaviors by others in the ecosystem, which will probably not be to the -- to the benefit of the TLD.

So that's a different -- it's a different conversation, really, than the notification conversation we were having in 115.

And as far as -- a saw a comment that Becky's question didn't get answered. And I think I know the portion now of -- that didn't touch on there or didn't touch on in depth on the presentation. That's around, you know, what level of T- -- of names can be added into the -- you know, the root zone and it be stable and usable, et cetera.

And the question -- the answer to that question is, we don't know. I don't know that it is knowable. The concern we have is that you may add so many, and it doesn't exhibit behavior that would indicate there would be a problem until it becomes a big problem. So, in other words, you have a fairly stable level of operational capability and then a very sharp decline in the ability to do things. There are many systems that exhibit that behavior. And it's a question of really understanding where those problems may occur. And it may not be in the root zone system or the root zone operations themselves. It may be in recursive operations, for example. So having a better understanding of that is really important.

And, again, that gets into are we talking about adding a similar number of TLDs that we did in the last round or are we talking

about orders of magnitude more? And I don't know that anybody knows the answers to the question of how many more in orders of magnitude are we proposing on doing. And if it's going to be a lot, then that should be something that would probably need to be looked at and understood better.

MERIKE KAEO: Yeah, Rod --

ROD RASMUSSEN: -- with magnitude.

MERIKE KAEO: Rod, I do see that Becky's hand is up. And so, hopefully, she can also clarify.

ROD RASMUSSEN: Yeah. So that was what prompted me to try and answer that question a little better.

MERIKE KAEO: Yeah.

So, Becky.

BECKY BURR: Yeah, I mean -- just to be clear, I mean, I understand the SSAC has had a position over time and pretty consistently regarding the rate of addition of names to the root. And I think while there was a lot of discussion about it, I don't think that the Subsequent Procedures Working Group has come up with a massive change in that.

What we see from the OCTO numbers is that with respect to the -- the security abuse -- and so one of my questions is what if the definition of abuse that SSAC is using. But if you are using the phishing, malware, botnet, spam as a vector -- delivery vector for those kinds of things, but the amount of that seems to be going down. Spam unrelated to those behaviors is going up, but spam is a complicated issue.

So the question around sort of what's the security issue here, what is the security and stability issue really, that's what I want to pin down.

Are we talking about the volume? Because it seems to me that that could be completely independent of the number of top-level domains in here. What is the sort of fundamental security harm that we are seeking to prevent here? And is this -- because that's

what I am just -- I'm really struggling with that. It doesn't come out to me from SAC114.

ROD RASMUSSEN: Okay. So there's one word you used there, I wasn't sure what it was. So....

But there's a -- yeah. So we've got a couple of, I think, intermingled issues here.

So for abuse definitions, at least within -- we didn't actually particularly point to any specific abuse definition for SAC114. That's the Sub Pro document. And I think the assumption -- and I think it would be a fair assumption to use -- would be the ones that's specifically called out in the contracts; right? That's the -- as you mentioned, phishing, malware, et cetera. Spam as a vector thing. There's no particular desire at this point to try to redefine abuse for anybody, just adopt -- I'm just pointing out that these are the ones that the community has adopted. So within that -- so you can use that, I guess, as the baseline for your reading through of our comments there.

The -- and so there's a couple of concerns around that in that -- Well, one thing you brought up is that, at least the numbers that you're looking at, the numbers are going down. And I know I get

reports that some are going up, some are going down. It really is a matter of what you have as measurements. So that's -- in every -- I think Göran mentioned that earlier, different people measure things differently. So there is that challenge.

But a lot of the abuse has been morphing over time, and that you may see absolute numbers go up or down, but the types of things that they're doing having more and more impact. And we've seen that certainly in the last year, with the rise of -- massive rise of malware -- of ransomware, which is a specific form of malware, which is having huge impacts.

So getting into a discussion around, you know, numbers going up or down or what have you is very -- I'd love to do that. But the bottom line is that the impacts of some of these things are going to -- are still with us and are going to be -- be there going forward as the next criminal or abusive behavior becomes in vogue.

So understanding where those impact the systems and processes that we are dealing with is the important part of that. And the concern around particular -- in particular, the DNS abuse, understanding all that for moving things forward, is really just a matter of making sure that we have proper responses in place for when these things come up, whatever the new, latest flavor of abuse is. And if it is prevalent within a particular operator, TLD, et

cetera, do we have measures in place to make sure that that does not become such an issue that it makes the -- universal acceptance is a term for it -- of a TLD or a whole host of TLDs, does that put that in jeopardy? And that is a -- becomes a -- are we consistent? Are things operational? If people start saying, "I'm not going to use this TLD," well, what about other domains that are dependent upon name servers within that TLD? Then you get into a whole bunch of stability questions as well, because you have a kind of cascading effect where people who are responding to an issue that is an acute issue in one area end up creating cascading problems in other areas.

So just trying to look down the road here as to if you don't address these issues or have a way of mitigating these issues up-front that you're going to have to deal with it as a tougher problem in the future. That's certainly one of the areas that we had concern about.

Hopefully, that gives you a -- connects the dots a little bit better for you as to what we're trying to get to here.

MERIKE KAEO: Becky, any other board colleagues have a follow-up to this?

And I can already anticipate that the SSAC public session will be quite a lively one, which I think is going to be a good thing.

ROD RASMUSSEN: Yep.

MERIKE KAEO: So --

ROD RASMUSSEN: Let me just point out here is that we're raising these issues and not -- because we have concerns, not because we're trying to put a kibosh on the name space. We're just asking those questions you've got -- we feel you should have good answers to move forward. That's all. And I know there's been comments in various places, and I'm seeing them fly by.

We're trying to help.

MERIKE KAEO: Yes. As S- -- I just saw KC put something in the chat. And it's something SSAC could and should reiterate. There are a lot of older advisories that pertain to statements we're making today. So these are not necessarily new things that have come up, but some of the things are -- especially when it comes to some

measurements and some more data-driven kind of information, right, the SSAC has always wanted to have more data around certain aspects. So some of the items that we're seeing in these newer advisories are just reiterations of old things that the SSAC has said as well.

ROD RASMUSSEN: Yeah, and a big part of our recommendation space here is about having better data to make better decisions as well.

MERIKE KAEO: Exactly. And I am noting the time. We have about 16 minutes left, and we have two more topics, I believe NCAP and the routing work.

So unless somebody has a burning question that they want to ask on the previous topic, I think let's move on to the collision analysis project.

ROD RASMUSSEN: And I believe, Jim, you're going to give a quick update on where we stand there? I think we've been making some great progress here over the last couple of months.

So I'll turn that over to you, Jim.

JIM GALVIN: Thanks, Rod. Jim Galvin for the record here along with my co-chairs, Patrik Faltstrom and Matt Thomas, who are both here. Thanks to the Board for taking the time to listen to us here and get this quick update.

So on the next slide, this first slide here, just a quick recap. You know, the ICANN Board obviously, as you know, you asked us to conduct a study, two specific resolutions, one regarding .HOME, .CORP, and .MAIL and one asking for general advice about name collisions.

We are up to 25 discussion group members with an additional 23 community observers. It's not a bad size group.

And in all honesty, typically we get around ten to 12 or 13 in any given week in our meetings, active members, which is probably about typical.

Next slide, please.

So the original Name CAP project had three studies that were propose. Study 1 one was really typically a bibliography of published work, whatever we could find out. Obviously, we have been delegating new gTLDs for eight years now in this particular

round. So we wanted to reach out and see what we could have learned over time and what's been done by others. And that's actually been completed and reports out there are published. And you've seen that it was done in June of 2020.

Part of the results of all that was realizing the circumstances have been evolved a bit, not just because people have done some name collision sort of reviews and analysis, little bits of things here and there, but also because the Internet infrastructure has changed. The circumstances under which new TLDs will come into existence is actually different.

So it seemed appropriate to provide a bit of a revision to Study 2 and to do things a little bit differently. So, in fact, we had originally planned to do -- the bulk of the analysis was going to be the study 2, but we've taken on a responsibility to update that project plan a bit. And I'll say more about that in just a moment.

And then Study 3, of course, would have been to look at mitigation strategies, things that are being done now, things that might have been done because there have been some reports, 40 plus reports, that ICANN has received at its portal. And we wanted to look at those, take a look what we could learn from them as well as consider what other mitigation strategies might make sense and, of course, provide some advice on how future

mitigation strategies might be evaluated. The premise being here that name collisions are here to say. They will always exist. They are not going to away. There's no way to prevent them. So it's about what are we going to do about the fact that they exist and how are we going to respond to their presence.

Next slide and this is the last slide.

So what we did in revising Study 2 was to consider -- reconsider some of the basic assumptions because that's evolved a bit in some of the major project elements and our resources needed. Has now been published, it's out in the public. And it has been proposed. And the Board Technical Committee has it in front of it, and it's also in front of the Board.

I know you've been discussing that yourselves in the background. And it's on the agenda for Thursday's public Board meeting. So we'll be looking for hopefully a final resolution on that and hopefully support. But more discussion will be what it's going to be.

We had a time line for our revised project. We provided a technical basis for why it needed to change. I think the important thing about the change is that it end up costing about 30% less based on the things that we've done. And we had imagined an 18-

month time line based on the Board's approval. We had hoped that that would mean, you know, June of 2022 for closure. That was the way it was sort of laid out. But we've been a couple of months getting the final version of that project proposal. It was delayed, and we didn't get it to you in time for your January Board meeting. So that's why you're dealing with it now.

And that's okay. Just for everyone to understand, we actually picked up in January anyway and we've been going forward with our analysis. We've gotten a yeoman's amount of analysis charts, reviews of data from Matt Thomas in particular, one of our co-chairs, who has been presenting that to the discussion group at-large.

And we're now just beginning the process of a detailed review of given all of this data, how can we begin to answer the Board's questions, how do we interpret the data, and what does it look like.

So the project has actually picked up in January. With any luck, our time line will actually still hold out. Fortunately, OCTO has supported us with the technical writer that we were looking for by giving us the research fellow. We've also gotten some advanced help in some secretariat support also from OCTO. So we want to make sure we thank them for that. In fact, of course, also

provided us with some of their staff support while we waited for OCTO to come around with this support. Hopefully that will translate into being more directly supported by Org as opposed to being, you know, resources that are on loan for the moment to help us move forward and keep this project going. We really are trying to stick to our 18-month time line in June of 2022.

I will just close by saying but this is ICANN. We know how these volunteer things go, but at least we're doing our best at the moment.

That's it for me for this. Thanks much. Happy to take any questions, if there are any. Let me catch up on the chat here while you...

MERIKE KAEO: Thank you very much, Jim. And I will also say thank you very much for the NCAP admin team who has been really helpful in also keeping the Board Technical Committee up to date with its work and progress and everything.

So, Akinori, I see your hand is up.

AKINORI MAEMURA: Yeah, thank you very much, Merike. Thank you very much, Jim, for the update. I simply want to express our appreciation for your effort. And then as you said, at tomorrow's public Board meeting, the NCAP Study 1 end and going forward on Study 2 is on the agenda. It is to be formally resolved. Thank you very much for that.

You kindly redesigned Study 2 in response to our request. So I believe that there was a lot of additional effort by that, by you. Again, thank you very much.

And I'm looking forward to -- for us to have Study 2 analysis done. And, again, thank you very much for your great effort for the 18 months. That will be helpful for the community. Thank you very much.

JIM GALVIN: Thank you, Akinori. Appreciate the opportunity.

MERIKE KAEO: Yeah. Thank you. Anybody else have any questions or comments from my Board colleagues? All right.

I see not. We have eight minutes left to talk about our routing security work party. Who is going to be speaking on that?

ROD RASMUSSEN: I think I'm covering that. I'm not sure.

RUSS MUNDY: Tim is going to speak on it.

ROD RASMUSSEN: Okay, good. Go ahead. I won't step on you.

TIM APRIL: Can people hear me?

>> Yes, Tim, we can hear you.

TIM APRIL: Okay, perfect. I will be quick and save time for questions and other discussion.

We started the routing security work party. The charter has been finalized after some delays by the holidays and all that. The scope is basically to create a document to explain the impacts on

routing security to the ICANN community, and we're trying to focus on nontechnical users being able to understand the document as well as anyone who is technical in this space. We are focusing also on the impact to the DNS specifically. It will hopefully be written in a way that will be generalizable to anybody else who is interested in the topic at hand. But there are other publications that people can review for that.

We will cover general background of what routing security is, how it can be implemented, what tools are out there, what gaps there currently are in routing security, and trying to instill some sense of urgency related to how much of this sort of attack type we're seeing in the real world at any given time.

I believe that's all I really had.

Oh, we may publish -- we're at least trying to publish one document. We may try and publish follow-on documents as the work party and community sees fit.

Happy to take any questions.

MERIKE KAEO: Thank you for that, Tim. And I'll also make a comment that, you know, the SSAC, as it delved into the routing space, did let the NRO know and we got some really good feedback. They were really happy to get a heads-up about this work.

So anybody else have a comment on this? Any questions from my Board colleagues? Maarten?

MAARTEN BOTTERMAN: Thanks for this and thanks for all this. I also appreciate the constructive approach that you take in truly advising and recognizing it's not only the ICANN Board that should resolve all this information going forward, but this is a community activity.

And this work is maybe extra difficult to do with the full community if we're not meeting in one location, but it's still key.

One of the things we're currently struggling with is prioritization overall. So as I don't hear any specific questions coming, if I may ask: What from all of this would be the most important thing to focus on above all, if you needed to prioritize? I'm not asking for a perfect answer but just thinking out loud. Comparing DNSSEC impact to the NCAP study impact, my guess, with my limited understanding, is that progress in DNSSEC might be more

important than further research on NCAP as long as we don't get into a crisis situation with new TLDs, for instance.

MERIKE KAEO: So, Rod, if I may, I'll maybe start off answering this question.

As some of you are aware, the SSAC has done an internal environmental scan which was work started to inform the SSAC about gaps in memberships and also looking at how does it prioritize its work in terms of advisories that it should be really concentrating on.

Part of that work will probably answer some of your questions and it wouldn't just be one item, right? It would probably be like, oh, these two or three or four areas of some concern regarding potential exploitation and impact.

But I'll let Rod answer to what we've decided to do with that work. But I think that would probably give out a context.

ROD RASMUSSEN: Thanks, Merike. I was actually thinking of that same thing, is we did do our internal environmental scan. And we've shared that with BTC, or planning on doing that, along -- we did it side by side a little while ago with some of the internal points there.

The various work we do over time is obviously going to be germane to any particular issue. I think that the work that we put together, that the Board will have access to on the threat scan at least gets you to the areas that we think are some of the highest potential risk areas and potential impact areas.

So I always look to that for guidance there. And it's really hard to pick what's your favorite kid, right?

[Laughter]

Yeah, dealing with issues, they're all important to some extent. And it really gets back to risk analysis and trying to weigh those things into impact.

From our perspective, I think we take it more from kind of a generic or technical perspective of where those impacts are going to be throughout the Internet and how that can affect lots and lots of people and end up having stability issues or places where things start fundamentally breaking down. There's lots of ways for that to happen.

As a Board, you need to also consider impacts in the organization as well, which is not really our remit. But certainly those are concerns that our individual members are going to have as well.

If problem A isn't addressed properly, what impact does that have on ICANN Org, the multistakeholder model, et cetera?

As I said, we're focused on more the technical side and the overall impacts to the ecosystem. But it certainly is an area that our members are at least thinking of as we're trying to prioritize some of our own work as well and realizing practically that this is important as well beyond just the technical aspects of things.

Without going through a long and contentious prioritization exercise within the SSAC -- (laughter) -- I'm sure it would be -- we don't have a listed order of address this one first and this one second. But, certainly, we did do an exercise and shared some of those results with the BTC around the things that we -- that bubbled up to the top of us for us to at least address and talk about.

That's one of the reasons we've taken on the routing work, for example, is that there were recent attacks on that space -- using these techniques and they had impacts and we haven't said a lot about it, so hence the paper we're working on for that.

MERIKE KAEO: We are at the top of the hour. I will just make one last statement on that, even -- whatever the topics SSAC is looking at, I also have

strong belief that there's a lot of risk impacts overall that have other aspects, not just technical aspects to it, that also need to be considered.

ROD RASMUSSEN: Yeah.

MERIKE KAEO: Well, I want to thank everybody. We are one minute over time. But this has been a very lively and good discussion. And I thank the Board members for their interest and their questions and comments. And look forward to seeing most everyone at the SSAC open session tomorrow.

MAARTEN BOTTERMAN: Big thanks to SSAC as well, including you, Merike, for an excellent facilitation of this meeting.

MERIKE KAEO: Thank you very much, everybody.

[END OF TRANSCRIPT]