
ICANN75 | AGM – Joint Session: ICANN Board and SSAC
Tuesday, September 20, 2022 – 16:30 to 17:30 KUL

SPEAKER: To help us fulfill our mission. For this session, no surprise, we will have the SSAC leaders to moderate.

SPEAKER: Thank you for my SSAC colleagues to be in this place. We certainly always do appreciate on behalf of SSAC to engage quite directly. We have a new agenda here. Three items on the agenda.

JAMES GALVIN: But what I will do is give Rod an opportunity for some opening comments and let you walk us through the three topics that you have.

ROD RASMUSSEN: Great. Thank you, Jim. Can we advance to the next slide please. Thank you all as usual for having us with you to meet. This particular question that came out from the Board around what we can do to coordinate across the community was really a good one and it got us thinking about a lot of things. And that's what we want to concentrate on today. If you're looking at the original

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.*

deck that got sent around, we switched the order around. We have our briefing on routing security that went a little long in the GNSO the other day so we shortened it up and moved that to the end so we can save the cool technical bits for the second half of our talk here. But there is really good stuff in there so we look forward to sharing that. But we want to start with a topic that was inspired by your question, but we put it under our topic, and the Board topic about the collaborative actions and we want to focus on DNS abuse across the community. We will get into that in a minute. That was the agenda that we had and we would like and I was told you would like to make this as interactive as possible which we really appreciate. Part of what we were trying to do was ask questions, we're not trying to come here with solutions to anything today. Well, we have some things on routing, but that's a different part. In the first half of this, we want to concentrate on starting some dialogue around some of the things we have seen and see where that goes. Can I have the next slide please. So, this first topic we were looking at gaps and if I could have the next slide, we will talk about what those look like. So in taking a look at who all has an important voice in security and stability operations etc. issues in the DNS but who often is not at or involved with ICANN policymaking, we thought it would be good to bring up this gap that is been off and on for years, in the case of security practitioners and we will talk about DNS operators in the next one. But as a community, a profession etc., there is some

involvement by security practitioners, some members of the SSAC are security practitioners, but the SSAC is set up to bring together people with security backgrounds, operational backgrounds, infrastructure backgrounds to create a group that looks at things from a lot of different angles and provides direct advice to the Board, and to some extent to the community and others, but it is really trying to synthesize and look at ideas and issues as standalone things and bring that in rather than represent a community in the policymaking. Security practitioners have shown up over the years, often without much knowledge of what goes on at ICANN and it has never been—it's oil and water to a certain extent. I know Maarten, you live in those circles as I do, and we have two different worlds that we live in to some extent. And that is all fine and good. There is plenty of that. but there is this overlap where we're talking about things like DNS abuse, access to registration data where there has been a lot of assumptions and things made without direct representation of those communities. And not, lack of representation, but really a home for them. I and we and many other people who I've talked to over the past couple of days after we presented this to the GNSO, and we shared this with the SO/AC chairs at the roundtable, have said yes, this is a gap, what do we do about it? I've heard a lot of interesting ideas where we might address that, but we wanted to bring this as a topic for potential discussion in how the community looks at this. One of the really interesting

ideas that came out of our meeting with the GNSO Council was to look at this as potentially part of the holistic review when you're looking for things like gaps and what the ICANN community is doing and who is involved, and how we go about doing things and this one and potentially the next topic area as well might be something that might fit into that. That one was an intriguing thought in my mind. I know you guys have had these questions for a bit, because I've gotten a few Board members who've said a few things to me about this already, so I do not know if there were thoughts that you guys had, either individually or gotten together to talk about on this topic, and then we'll talk about, I think, the DNS providers separately, but I wanted to throw that open. You see this slide here that we have the points on, but I think it is something to think about and try to address going forward to have that community better represented and involved and interested in what goes on here so we can get better outcomes and maybe it helps us get through things a little quicker in some of those areas there. I will turn that back to Jim for moderation.

JAMES GALVIN:

I was going to ask, you seem to want to separate these two., but I'm thinking, aren't they sort of in the same space of the question about wanting a voice in the community?

ROD RASMUSSEN:

And that is a fair point. And go ahead and advance to the next slide. So DNS operators. This includes both the authoritative side and recursive side. And when ICANN formed in 2000 or so, over 20 years ago, the landscape looked a lot different from what it does today. ISPs handled most DNS resolution. And hosting companies and ISPs handled most authoritative site. Things have changed a lot in the industry whether it is the rise of large public recursive resolvers, or security focused resolvers. Okay—hey, we have scribing. You have seen a big change in the recursive side at least in some territories, it is not universal, there are many places that still have a more traditional, if you will, model, and on the authoritative side, you have managed DNS services that many of them started with registries and registrars but have moved on to be independent services and a lot of things going on at the big content delivery networks, Amazon, etc. where they are providing huge amounts of authoritative DNS infrastructure. The issue there being that while some people from those companies may be showing up, they're showing up for other reasons. Like the registry at Amazon or Google or however is showing up, but not necessarily the people running those infrastructures. And we've seen there has been an impact from the things that they have been doing to make DNS operations more efficient. It is a business and they want to do things to make money, which is all fine and good. But sometimes those things have impacts on the way that affects the rest of the DNS ecosystem which is definitely

within ICANN's purview. We've actually done work that SSAC has published as an example, others have too, around DoH and DoT as an example of protocol changes, you have QUIC and some other things going on at a technical level that impact how we see things at the very least and to be able to measure and understand when there's maybe issues going on. So, what can we do for both of these communities to try and get them more involved, etc.? And I will put one last thing on this last point on the DNS operators. I was just informed and I had not had a chance to sit down yet and have a chat, that the ISPCP is actually looking at how they might be able to expand their [bit of it.] So that might be a home. That's a potential. But these are the kinds of discussion points we thought might be interesting to have and not necessarily to solve problems in the next 10 minutes, but we have a conversation and think about where we might be able to as a broader community to bring those folks in.

JAMES GALVIN:

Thank you, Rod. I do want to say, on behalf of Board, this is an excellent two things to bring forward as strategic things that SSAC is thinking about as a way to constructively enhance the community and improve security efforts in general. When you touched on a topic of holistic review and having heard that, there's one Board member here that I was thinking I was going to

tag to, add a few comments to the discussion, and again, a reminder to everyone, this is an open discussion so please, anyone who wants to add some thoughts or comments, raise your hand, we're watching the Zoom room if you want to put your hand up there, or I will try to see you waving in the distance and keep the queue going. Let me reach over to Avri first to comment. Thank you.

AVRI DORIA:

This isn't the first time that groups that have not been—or have not felt adequately homed—I was going to say not represented, but homed. Because certainly, functioning within the open community is available to them and always available to all. But in terms—because there's been conversations, many over the years. Now, coincidentally and at this point, you know, we are getting ready to sort of put together a holistic review of ICANN. As you probably know, the terms of reference for that are in discussion, are in public comment now. While this is certainly not something that I see the Board doing anything about, because that would be very top-down as far as like, “Oh, okay, you guys can find a home here, and you guys can find a home there,” though certainly, imagination would allow me to do that. But to basically try and get that discussion, included within the whole bailiwick of what is holistic review of ICANN—because among the things they're

talking about or possibly talking about are the structures, are how it is set up and how it works. So it would fit very well in there. Perhaps it would be good to read the terms of reference and sort of say, gee, you know, let's put a comment in saying in this particular paragraph, it would be really good if you looked at groups like the following. I would really recommend that as a path while continuing to participate in any other groups because there have been several over time that have looked for a home and said we can't find a home. ISPCP often ends up being the home they think about, but somehow or other, that does not necessarily happen. That would be the first approach that I would take and try to bring into sort of that structured conversation. That will be happening. And hopefully we will be starting early next year at some point. But, first we had to get the term of reference established. So it is a perfect time to get it into the terms of reference somehow. Thank you.

JAMES GALVIN:

To make that specifically actionable for SSAC, is what that sounds like Rod is producing a comment to the terms of reference that are out for comment. I do not know how long there is to do that, do you Avri?

AVRI DORIA: Until late October, I'm not sure the exact date, but we just started them, so there's at least two or three weeks left, if not more. I can check. But yes.

JULIE HAMMER: It's actually the 20th of October, and this was our intention, Avri, to do a comment in the public comment that brings up this and a number of other points. And we actually had a discussion on this last Saturday in the SO/AC chair meeting and all the chairs and vice chairs are aware of this, as in the need and wish to comment on those terms of reference, so that will certainly be our intention. Just one other point, maybe I am jumping in where Rod was about to say the same thing. One of the points I know Rod has made visible is that it's not necessarily people clamoring to become involved in ICANN. Some of the practitioners that Rod has identified aren't necessarily even aware that there are issues going on in ICANN that they ought to be involved in. And it's not that they can't find a home, it's that they do not know that ICANN is relevant to them.

JAMES GALVIN: Thank you. I think that's an important question as well. put Harald, you have a comment for that. Please.

HARALD ALVESTRAND: I can easily see the value of these people showing up for ICANN. but Can you describe briefly why you think it is valuable for them to show up here?

ROD ROSMASSUN: Yes, having been one of those people in the past, I started to show up, so I think I am a good case study. I get addicted. The most obvious examples is what happened with access to WHOIS data. Even though ICANN was saying this would happen, and other people were saying this will happen, it was a massive shock to the system in the cybersecurity field. And there are plenty of people that knew in the field it would happen, but in general, people with heads down on keyboards and going after bad guys and doing things like that were like where did my stuff go? Who moved my cheese? There've been plenty of meetings since then where people were like, ICANN should fix this. Well, if you want ICANN to fix something, which, it doesn't really work that way, you need to show up. Right. There are things like that that have happened and other policy things, and we know ICANN is doing a tremendous job at tracking all the new legislation going on around the world. These things will have an impact, we deal with it here, and it has other impacts that go throughout the ecosystem. I think there is an abject lesson that has been learned recently where people are

saying okay, how do we participate in this process, where do we go to do that?

JAMES GALVIN: Kaveh, please.

KAVEH RANJBAR: I agree with what was said, and I want to point out some positive examples of where this happened. One example is for example OCTO is involved in RIPE community from time to time, whenever there's an issue coming up, or sometimes you present about ongoing status, mostly technical, sometimes policy stuff, and for example in RIPE which is operator community for Europe, Middle East and Central Asia, there is a very active DNS working group, where many operators, software vendors and other participants play a big role. There is an effective link although it is not formal, but ICANN and OCTO send people there and present there, I have seen similar to NANOG. None of these are formal, but there are also some positive examples. That does not mean we are fully covering all of the relevant stakeholders there, but I think that is one effective way we have utilized in the past.

JAMES GALVIN: I'm looking around to see other hands. Rod.

ROD RASMUSSEN: That was an excellent point. ICANN does a fabulous job of doing outreach. The OCTO team has been doing a great job of late of publishing things. There's a lot of stuff going on that's getting good uptake. I think the gap we're trying to identify here is around the ability to come in and help affect the policy so there's more than communications, although that is important, it is also about how can those folks have a voice in how things get done.

GÖRAN MABRY: I want to build on what Harald said. That what's in it for them? For instance, if someone comes to ICANN and thinks we can fix GDPR, they will probably be slightly disappointed not because of ICANN can't do it but because they should probably go and use their potential to do elections because that was a law, not something ICANN can do but it is important, I am very much in favor of having a conversation. And in my goals from last year and also this year we are talking about how we can have better interactions with manufacturers, software providers and also ISPs, telcos, whatever you want to call them, because in the end, we sort of depend on them. They are the ones who actually provide us with the Internet. And I think that over time, we have lost a bit. So I think this is timely and really good. But I also think what Harald

says because it could also be the other way around. One of the things we sort of often talk about bringing people into ICANN but maybe we should go out and. Speak to them so they don't have to come here, even if it's nice to be in Malaysia. And I can see Harald now almost laughing at me, so I'm going to not say anything more.

JAMES GALVIN:

Thank you Göran. I want to thank you, Rod, for bringing this forward. I think it is fair to say it is very constructive contribution from SSAC to be thinking about the issue of these two communities and I would say we also have a constructive response to that, so that's a good thing. So unless I see any other last comments or hands, I think Rod, we will turn it back to you for your next topic.

ROD RASMUSSEN:

Great, thanks Jim, can I have the next slide please. This is a Board topic around collaboration across the community. And further progress in achieving strategic priorities. So, this one, we love this question. And we dove into this. And, where we came out with what we wanted to bring to the Board's attention and community's attention and coordinating is around DNS abuse which has been a top topic obviously for several years in the community. So let me run through a couple of things in the

background. Really quickly. Next slide please. So DNS abuse, lots of work going on all over the community, tons of work. In the community and outside. With groups related. Lots of people doing good things. Organization, ICANN org has done lots of things with the DAAR, a bunch of other initiatives looking at this stuff, so there's a lot of work going on. But we thought to ourselves, what is the plan, what is the overall arch here. So we took a look at the strategic plan. There are many things in there that mention DNS abuse. Or at least touch on it. And here are some of the ones directly from the strategic plan around security of the domain name system etc. Can I have the next slide please. And then there's this strategic goal as well, in strengthening DNS coordination, partnerships etc. That speaks directly towards mitigating DNS security threats and DNS abuse. These things are already in the strategic plan. And there are efforts going on. Can I have the next slide please. So we have these high-level strategic goals, and lots of work going on in the community. What we saw as a gap is kind of that bridge, the strategic plan, the roadmap, an overview etc. of how we bring these things together especially now that we've been working on them for a long time and looking at different parts of the problem etc. Can we create a bridge between what's in the strategic plan and all the efforts going on now and into the future. So we can—well for lots of reasons, there are a lot of good reasons to do that. And I know there has been discussions going on about this already, and we've gotten plenty

of feedback on that, and we just had the small team from the GNSO giving a report. The GAC and the ALAC have been doing work and putting out recommendations as well, and the contracted parties have been doing work on abuse, lots of work going on here. We're not suggesting come in here and saying to do it this way or that way. What we are suggesting is let's all get together and have a conversation about how to coordinate and move this forward. Next slide please. So, in thinking about this, the strategic plan, we are engineers at heart, so what does the plan look like, what's the product we want to build. What are the requirements for it? What's the timetable, deliverables, how will we measure it? All those things, how we approach the problem. We put a few thoughts here. They're not comprehensive, they are exemplary, but if you're going to create an overall plan, here's some of the aspects you'd want to include, everything from looking at how we can look at what people are doing out there from their practices and preventing registrations up front to—malicious registrations, we don't want to prevent registrations. Let me make that clear here. But make sure the folks that are getting domains are at least not trying to use them to harm other people. That is a goal. And two, what information can be shared? All these kinds of things you think about with any kind of security problem. Just another one of those. And then creating a consistent baseline so expectations can be measured across the ecosystem. What does that look like, what can we agree to as to

what that looks like. Almost just as importantly, what can we communicate out to the world that is not doing the infrastructure and putting the domains out there and all of that to have them be effective at getting the information, and there is lots of work going on in this space. There is good progress here. And the story here is not just can we get the folks doing the domains and putting them into production working on this stuff. It is also those finding things that are not kosher so to speak. How do we get them working better with the community. And then again, as I think I mentioned earlier, create a timeline and goals and expectations around that. So we are throwing this out there as a hey, we are coming to the same place at the same time. Maybe we should get together. I know there is a special Board caucus on this, or Board group, I got that right on that. What's been going on in GNSO, efforts in the ALAC, and the GAC, etc. Can we somehow get together and work on a plan that we can execute against? And one of the other reasons—it's not stated in the slides—for doing this is to be able to show to the outside world that is looking to blame ICANN for not getting things done. We have a plan. Here are goals, we execute against them, if we do not meet the goals, we are transparent about why and what the challenges are. But being able to share with the broader community. We know there's various pressures for various reasons. That no, we work together as a community, we have a plan, that we will execute against. I think that would be a valuable exercise for this if nothing else. I

will throw that out there, and I know you have been talking about it, so I would love to hear what you thought about already on this.

JAMES GALVIN:

What I will say, is in principle, we all share this as a goal. The Board and the DNS abuse caucus would appreciate this sort of strategy moving forward. But let me ask a question of you for just a bit of clarity, and I believe there's a couple people already ready to comment. Are you sharing this as, to inform the Board about something SSAC will do? As in you really want to reach out and do outreach with the community to see if you can pull this together? Or, is this going to be an ask of some form from SSAC to the Board and community in general at some point in the future?

ROD RASMUSSEN:

Let me pick a different answer than the two you gave me. Well, this is a conversation starter, I think number one, right? With some thoughts around how to have that conversation. I think to the extent where we have the time, expertise, capability to do so, we participate in efforts to make this happen, the SSAC is not volunteering to lead such an effort. We're just not set up for that, right, and that's not the desire here, the desire here is we are seeing efforts going on, we have that engineer's desire to bring things together and have a conversation. Not for us to decide, it's

for all of us as a community to decide what to do, but that said we would certainly be I think important participants in whatever that effort looks like. I don't have any prescriptive ideas for what that might look like or anything like that. Sure, we will all sit around and blue sky some ideas and bring something to the table, but I don't think this is the appropriate venue for getting into that solutioneering. But, I think what we want to do is raise the awareness that we need from our perspective, there should be a plan, and that we are willing to put our time and effort to help make that happen. Does that answer your question?

JAMES GALVIN:

It does, thank you. And that moves us in a direction of thinking about whether this is a strategic objective or a path that should come out of our strategic objective, and I think I'm going to look to Matthew from the Board to offer up the first set of comments and of course the floor is open for others.

GÖRAN MABRY:

We talk about DNS abuse, and I want to make a couple of comments. If you want really good comments by the way, look at the transcripts for what Jim said in the GAC an hour ago, it was sort of a summary, because I know that you don't mean this, Rod, it's like we don't have anything, we might have a plan, but if you look back, ICANN I don't know how many years ago, five or six

years ago, we put in the Spec 11(3)(b), we renegotiated the .com agreement, so they're on the same provisions, we did the same thing with .biz, .org and .info, we added the DAAR system, we added DNSTICR, and if you look at the amount of DNS abuse, you can see it's gone down dramatically. Using the same data [sets of the] European Commissions, they just looked at three months, we looked at five years. With that said, I can also say if you missed it, the Contracted Parties House right now are sitting and talking about entering negotiations in their contract, of more things to come into the actual contract, we might as well look at that as well. Thank you.

MATTHEW SHEARS:

Rod, this is great. You are absolutely right, the Board does have a strategic planning committee, and I chair it. So thank you for this. This is where we're probably going. I will put that out as a general statement. The strategic plan as it stands today is very much a set of goals and priorities and we put it out there and we've encouraged the community to look at it and place its work around there, but we've never provided a framework if you will for the specific areas of the strategic plan. And that is the next logical step that we will go through because what we want is greater alignment across the community—org, Board and the community, stakeholders, in terms of how we deliver on those

priorities and goals. And what you are doing here in my mind at least I think it's what you're getting at, is how do you structure a framework around which we would then address DNS abuse for example. In many ways we will need this kind of approach for other strategic priorities as well, frameworks within which the work can be undertaken, different parts of the community hopefully coordinate and aligning in terms of how they will adjust their priorities. This I think is a great first step for thinking about how we can address DNS in a more holistic way, so thanks very much for that.

ROD RASMUSSEN:

For those of you who are not in the room and didn't see it, I gave a big thumbs-up to exactly what that is. That's exactly where we see that gap. And I'm not saying [inaudible] done their job here, it's a natural progression, as you said. And we are saying this is a good place for us to have this conversation and because the whole community is looking at it, it's a good use case for how we move that strategic plan into these frameworks that you are talking about.

JAMES GALVIN:

I would think there are two actions at least that come out of this that are worth considering. One of course in line with what

Matthew was saying, there's an opportunity for SSAC to look at the next cycle of strategic planning that goes on and see what it wants, if it could consider making some kind of constructive contribution to all of that and be a part of that process from the community. The community is involved in the development of the strategic plan, so there will be opportunities coming up along the way for SSAC to be a part of that and contribute even if it is just a review of what ends up there, but I would hope giving some thought to what might change there, so look at what's there and consider that, so that is one and the second thing is I do think that SSAC should continue down the path as you have been doing already with other groups talking about this and seeking to create a conversation with the other constituencies in ICANN and seek to and see if we can get some traction with a group of people who want to do something and then figure out together what it is we can do together and how to go forward with that. I'm interested in comments about that. Other thoughts about it from anybody. Rod, you should have an opportunity to speak first. But please SSAC members, other Board members, anyone who has any thoughts., we'd welcome some other comments.

ROD RASMUSSEN:

I think the discreet action that you mentioned, that's an easy step for us. And we would do that regardless. But I think maybe in a

little more active rather than reactive role that we took to the first stab at the strategic plan a few years ago, and this particular area is within our skill set and remit to at least have some thought leadership on because obviously, the strategic plan will be adopted by the whole community but we could really contribute a lot to that by giving input upfront. So I think that's one thing On the second part yes, this is something where the SO/AC chairs, we converse regularly, there's a lot of desire to amongst the leadership at least to try and coordinate efforts which is not always easy to do practically, and I think that's one of the challenges and I think the Board can help facilitate the community coming together. That's one of the reasons we wanted to bring this up with the Board as well. As a community, we were having these discussions already around how we coordinate better, this is a great example of where we might be able to come up with a process or whatever, hopefully lightweight, because one thing that has been said, is don't create a new bureaucracy [LAUGHTER] That's not what we want to do at all. We want to get on the same page and how do we do that? There may be facilitation that the Board can help with.

MAARTEN BOTTERMAN: [inaudible] is not bureaucracy we need, but a process to make sure all voices are heard. One remark here is I fully appreciate that

the strategic plan is an important place to lend this. But let's look at two time horizons. Let's look at what we need to look forward to to be able to address this in the five years to come, knowing some of the problems we have today will not be there, and other problems will be there, and knowing that some [of these,] we don't know. but at least the measuring and things may happen, help there. the other thing is to progress the DNS abuse discussion we have today to more practical action together. So let's keep the two timelines very clearly in mind when we work on this.

JAMES GALVIN:

I think emphasizing SSAC continuing to be proactive in reaching out to other groups and looking for other partners to continue this discussion and to you know, as you say, SSAC doesn't want to lead this, but I do think that SSAC has a critical role in participating in this process. We have a certain special expertise to bring to those discussions and we can help the community as it moves forward in the space. We should not lose sight of that. So we would welcome that discussion and then we'll look for an opportunity where the board can be particularly supportive to the effort and certainly take that onboard. Go ahead.

ROD RASMUSSEN: We'd normally do this offline, but I'd say some sort of setting up a discussion with the DNS abuse Caucus with the SSAC. I wanted to say that publicly because it's good to let people know we are thinking about these things, to do that and be able to give more depth on what we are talking about.

JAMES GALVIN: I appreciate that. Any last comments or thoughts from anyone? Not seeing any hands and nothing in the Zoom, okay, then thank you for that, and let me suggest we move onto the last topic.

ROD RASMUSSEN: And I will turn the presentation over to Russ who I saw just joined us, and thank you for getting up, he's 12 hours different so you do the math. So thank you very much Russ. You have about a little over 15 minutes to run through the slides on our routing security work, turning it over to you Russ.

JAMES GALVIN: Before you start, can you put this in a context, as to this is informative or there's an action in here for us? What is the context for the presentation?

RUSS MUNDY:

Thank you Jim, I was going to actually include that as part of the opening parts here. This piece of work by SSAC which is published as SAC 121 is an initiative that was undertaken by the SSAC. A number of the members of SSAC have seen this as a challenging area. Security in particular with impacts that it has on the DNS, so it is something to be thought of as an initiative by the SSAC itself. The results—and you will notice the title is somewhat unusual of a title for an SSAC document. It is SSAC briefing on routing security. And it is indeed just that. It is a briefing. It is a set of information that is intended to help inform as well as educate the community. There are no recommendations for the Board in this publication. There are a number of suggestions in the document for various parts of the community. So, it is our hope that this will be a useful set of material to provide for a wide range of people around the community with the primary emphasis being on the impact of routing security can have upon the DNS community. But, it does impact many other aspects. And let me just ask for the next slide please. Oh my. Okay. Is there a problem with my audio? I don't know if it is me.

JAMES GALVIN: You are fine Russ.

RUSS MUNDY: Okay good, thank you. The briefing slides truly are an extract from the content of the publication itself. It's not an incredibly long publication. But it does also contain a very lengthy set of reference material that at least in my opinion is one of the most comprehensive sets of reference material about routing security that I have ever seen published in a single document. There is a lot of additional things for people to go look at and read if there is further interest to explore that. So the impact specifically of routing security upon the DNS servers just as many people realize that DNS is used and it is critical for the function of the various and most applications that are used on the Internet. Routing is very important to not only the applications but also to DNS, and to the functions of DNS. And so this you can think of in some ways, if you think about things as protocol stack, the importance of DNS to the applications above is similar to the importance of the routing system and the stability of the routing system in the lower levels of protocol stack. And so just to identify the set of things in DNS that make a higher connection between routing and that DNS services that exist on the Internet, is that there are a lot of structural things that impact results in these dependencies. The list on the left is an indication of the things that are done, or not

done by various parts of the DNS. And on the right you can see how an attack is very practical or feasible to be put in place, against the normal and regular ongoing DNS service. I'm going to skip through these, because there is not a whole lot of time, and not cover any of them directly, so can we just have the next slide please. So the example—there are a couple examples in the document, but the example that's received a lot of attention over time is what is referred to as the MyEtherWallet Route 53 hijack. And what this was, was an attack that was based on an attack on the routing system itself. And in conjunction with that, a fake malicious DNS server was used as part of it, but the actual attack itself was on the routing system. The results of the attack are twofold. The first one which is what has gotten the most publicity, is that the attackers stole \$150,000 in two hours. That's a lot of money in a short length of time. But, the other, and in some ways as important aspect is for the users of the Route 53 DNS service, they were essentially totally out of service, for two hours until the problem was identified and corrected and cleaned up. So not only were those people that were using the Route 53 service that were part of the ether wallet attack, not only were they impacted but all the other users of that Route 53 service, so next slide please. In the document we describe in further depth how the pieces meld together and how there is a number of different activities that are really needed to improve and enhance the security of the routing system. On the left side of the slide you will see GGP security and

there are a couple of different aspects there. These are generally what you would hear a lot about, if you look at the literature and how you can improve the technical pieces. If you look in the center of the accuracy of the routing policy, it is aimed at operational aspects, whether it is operations of DNS activities or operations of direct routing activities that you need to have a policy that meets your objectives and goals, and you need to be consistent and you need to have it stay accurate. And on the right you will see a direct operational [inaudible] and a set of things that are listed there for activities that need to be done monitoring the routing of your system internally. Monitoring how the routing of the system external to the parts that you directly control as an operator. Those are both important. And yet distinct activities in most cases. And then the MANRS project, that has laid out a set of things that apply to the routing world itself. So, can we have the next slide please. The key takeaways from this are several. The first being that the routing system as it exists today is very much subject to ongoing attacks. There are hundreds of thousands of attacks that happen every day. We have not in the document used the word attack talking in terms of routing anomalies because the reality of things is it's generally believed by security and networking professionals that most of the things that occur that look like an attack are really just a mistake. Oops, fat fingered that, I need to fix that. But the end result in the routing system itself is largely the same. So routing anomalies is a terminology

we chose to use rather than attacks because you just simply can't tell the difference between them in sort of a real world sense. They happen all of the time. And sometimes result in significant DNS outages. Now how do we improve that, the next takeaway is it's a combination of a set of things that involve operators involved in all the aspects. If you are operating a DNS centric activity, you will have some routing in support of that directly related to that. And even if you are very DNS focus, you need to have expertise either on your staff or available to interact and understand what's happening with the routing system. Now, the third point we want to make is monitoring to detect anomalies is incredibly important. That's the internal and external monitoring of how your network and your IP routes are being handled on the broader Internet. The fourth point is that routing security is a very important aspect, but it does not substitute for other critical aspects of security using the DNS and the Internet. Such as it does not and will not replace DNSSEC, it is a different set of activities that are crucial in a different plane of activities. And sometimes, security technologies in one plane can help or prevent the successful execution of security anomalies or attacks in another plane, and sometimes they will just help you be aware of it. As is usually the case with security aspects, there is not a single silver bullet, one thing that solves all of the problems. There are things that you have to do on a broader spectrum that involve multiple technologies and so the routing security is important and touches

many other aspects but it does not replace security that you need to apply to these other areas. So, I want to leave a few minutes for questions, and I see Yoshiro has asked about KINDNS. And yes, Rod's answer is good. And I think that is the first question, and I'm certainly open to take questions here. We have a couple minutes if there are any.

JAMES GALVIN:

What I want to do is comment to my Board colleagues as a reminder, when this document was first distributed to the Board for our usual 48-hour prepublication, I had pointed out at that time that this document is a nice tutorial style discussion of routing security and although it is very much focused on security and stability implications for DNS, this matters in an ICANN context because we have several entities, registries and registrars that have very large DNS infrastructures. Probably the larger ones do a pretty good job with this. But as those who are in a medium or smaller state, having this kind of information accessible so that they can inform their own operations is a good thing. I would say that this document in general is one of SSAC's better documents in terms of a survey of this kind of information, similar to what we did with DoH and DoT years ago, and IoT discussions, it's just a good informational document that should in general help the industry and help folks here. If you haven't had a chance to look

at it, I hope this presentation piqued your interest and curiosity further. And certainly feel free to spread it around, it's intended to be accessible to a non-technical audience. Policymakers and legal experts. I'm still not seeing any hands or questions from anybody.

MAARTEN BOTTERMAN: Just from my side, and indeed this touches well on the operations, because things are happening out there, and as Jim said, it's a different mix of people who are actually operating. MANRS has shown to be very useful. This is a step that really helps to firm it up. So I really appreciate the work.

JAMES GALVIN: Avri go ahead.

AVRI DORIA: I did not get it read in the 48 hours, but I got it read since then. It is a very good read. And what Russ said about the appendix, the list of references, it is an amazing appendix. I will congratulate you on the document. As I said, it is a good read.

JAMES GALVIN: Not seeing anything else so thank you Russ for the presentation, over to Rod for any other closing comments or any other business here.

ROD RASMUSSEN: Thank you Jim. I just want to express thanks again for a good discussion today. I think we got really good feedback on what we would propose and I really appreciate and it is quite clear that the Board took very seriously the input we provided to you and thought about it and came back with some really good thoughts on all the topics we brought up, that is much appreciated. And I really mean that. We get so busy with these things and it's hard to keep up and the fact that folks spend a lot of time and clearly thought about it and were thoughtful about it, I really appreciate that and I hope to return the favor.

JAMES GALVIN: Thank you Rod and thank you to the SSAC. And it goes to Maarten for final close.

MAARTEN BOTTERMAN: I would only repeat what Rod and Jim said, thank you very much, we appreciate this, and it's great to be updated about this. SSAC

is not always on top of the agenda, but what you do is crucial for ICANN and to have the opportunity to listen to you and interact with you up and beyond reading the reports and having the benefit of your liaison is truly of high value for me. So thank you very much and have a great evening.

[END OF TRANSCRIPTION]