ICANN75 | AGM – RSSAC Discussion: Recent Legislative and Regulatory Activities
Monday, September 19, 2022 – 15:00 to 16:00 KUL

OZAN SAHIN: Hello, and welcome to the RSSAC discussion on recent legislative and regulatory activities. My name is Ozan, and I am the remote participation manager for the session. Please note that the session is being recorded and is governed by the ICANN expected standards of behavior. During this session questions or comments submitted chat will only be read aloud if put in the proper form, as noted in chat. I will read your questions and comments aloud during the time set by the chair or moderator of the session. If you would like to ask your question or make your comment verbally, please raise your hand. When called upon, kindly unmute your microphone and take the floor. Please state your name for the record and speak clearly at a reasonable pace. Mute your microphone when you are done speaking.

This session includes automated real time transcription. Please note this transcription is not official or authoritative. To view the real time transcription, click on the closed caption button in the Zoom toolbar. To ensure transparency of participation in ICANN's multistakeholder model, we ask that you sign into Zoom sessions using your full name. For example, a first name and last name or surname. You may be removed from the session if you do not sign in using your full name.

With that, I will hand the floor over to Fred Baker, RSSAC chair.

FRED BAKER: Thank you, Ozan. Have we got everybody in the room that we expect to have?

OZAN SAHIN: Yes, we have guests today, Elena Plexida and Jamie Hedlund in the room.

FRED BAKER: Cool. Let me extend that welcome to them. To give you a little bit of background, we're aware that ICANN has been talking with various regulatory authorities in Europe and in other places, and we're interested. We tend to think that we might have something to offer in terms of answering questions or advice, and we'd like to be on the same page with ICANN, not that we expect that there's any significant debate. If we have something to offer, then we'd like to be able to offer that.

With that, let me turn it over to our speakers.

ELENA PLEXIDA: Thank you, Fred. Hello everyone, thank you for having us. If you allow me, I will start with spending a few minutes reflecting on the bigger picture, the political climate we find ourselves in. If I were to put a title to describe it, it would be politicization. The DNS is getting politicized. There are deliberations on international fora, brining into the discussion the identifiers. Most prominently, next week the ITU Plenipotentiary Conference is starting, and the ITU member countries will elect a new Secretary General. They have to choose between a candidate that is pro the multistakeholder governance, and a

candidate that openly supports moving the management of the identifiers to the government led ITU.

On the legislative front there is a noticeable shift, at least at our level, with regard to the DNS. Proliferation of Internet-related regulations worldwide is not something new. In fact, a large part of what we in government engagement has been doing so far has been to help clarify, for example, that platforms are not the Internet, they reside on the Internet, so that legislators avoid unintended consequences to the technical functionalities of the Internet.

Here is what is new, the shift that I mentioned. So far, we've had legislative initiatives that would unintentionally, indirectly touch on the DNS and the function of the Internet. Now we have initiatives specifically intentionally targeting the DNS, with the most prominent initiative in that regard being the NIS2 Directive of course from the EU. Yes, that's right. Particularly the part proposing to regulate the roots. That is proposing that one jurisdiction in the world would regulate unilaterally core functions that have been entrusted to the global technical community.

It's not just these two. There are non-legislative initiatives, too, moving in the same direction of controlling the DNS, securing, controlling our part of the DNS, if that thing even exists, our part. In a world that is becoming increasingly more tense, there is less and less trust between international actors, countries in different regions want to be sovereign, including in the digital sphere. Sovereign, unfortunately not in the sense of autonomy, but in the sense of control. When it comes to the identifiers, of course, it's true, there are countries that have always

been advocating for more control. The coming ITU elections will be very interesting in that regard, as I mentioned just before, as this is the first time that moving the management of the identifiers to the ITU is publicly, formally part of the election platform of one of the candidates.

Yes, control by governments is not a new idea, but that idea was, if I can put it that way, a fringe idea. It's not anymore. Now we have similar ideas oriented at control in a different way from parts of the world that have been, so far, traditional champions of the open Internet and the multistakeholder governance. What is happening is, as I said at the beginning, the DNS is getting dragged into the geopolitical agenda. It's getting dragged into politics, and in other instances different, not legislative initiatives. The thing that proves the strength is the word Ukraine, that very unfortunate thing, where there was consideration of possibility leveraging the DNS as a major political pressure. This politicization of the DNS is very, very, very concerning, of the identifiers, not only DNS, from our perspective. That's a personal opinion. To my mind, such politicization can be existential, even, in the sense that the outcome of dragging the identifiers into geopolitics can even be a fragmented Internet.

The world is very different, governments' stance toward identifiers. Let's not say it's changed, but it's definitely not a given anymore, and that affects or will affect everyone involved in the ecosystem, not least the RSS, considering its criticality and the fact that policy makers are increasingly conscious of it. That was the bigger picture. I think it's important to connect dots, that's why I thought it was worth spending

some time. Let's get to specifics. NIS2 would be the first. Next slide, please.

Now, as a brief reminder, NIS2 was a proposal published in December 2020 by the European Commission. It's an update to an existing directive that already included the DNS, and either imposes cybersecurity measures and incident reporting obligations to essential and important entities. As originally proposed by the European commission in December 2020 it would explicitly apply to RSOs. They would have to implement specific cybersecurity measures, reporting obligations. They would have fines in case they failed to fulfill their obligations. On that slide you see the relevant recital in the article as it was originally proposed, you see in red, and that's my red. It's very explicit that they were in scope.

In the next lines you see the relevant text as adopted. Following a negotiation between the so-called co-legislators, council environment, it is now crystal clear that the RSOs are exempt. We have the exemption there specifically in the article and also even in the annex. That did not happen, of course, just like that. It involved a lot of engagement in Brussels and outside to make people aware of what is at stake. In the context of engagement activities, just for example, we organized a webinar together with [inaudible] in Brussels, virtually in Brussels, that was specifically for the representatives of the EU countries that were part of the negotiations. I have to say this was very helpful, to explain to them how it works, the instances, the redundancy that there is ongoing work on the governance of the RSOs, et cetera. It was really a tipping point in the negotiations.

That a number of RSOs contributed with comments to the public consultation in NIS2 was very important. If I'm allowed going forward, that's what RSOs would have to do. RSOs have to be present at such consultation when it comes to issues that concern the roots, and also take or make opportunities to explain things outside of formal consultation, as such, if need be. This text is getting formally adopted next month. It's just a formality though, it's a done deal.

Now, the root services are out of scope of NIS2, that's done. I cannot promise, though, that the idea will not resurrect in some other scope or form, and that's because the perceived idea that political invigoration could cut Europe out of the Internet is there, and it's probably stronger than ever. The constant message we have been relaying to policy makers is if you have any concern with relation to the RSS you come to the technical community. You bring it to the attention of the RSOs. That's the way to address it, not legislate.

In relation to that, there is yet another initiative in the next slide, please. A non-legislative one coming from the European Commission, again, regarding the root. In the context of the cybersecurity strategy there are a number of initiatives put forward that have to do with the DNS. There was one particularly speaking about the need to develop a contingency plan for the root. Last time we spoke I had mentioned the Commission had not put more meat to it yet. I'll say the same now. We don't have updates. We have not put more meat yet, other than this is out there. This is, by the way, the same strategy that put forward the DNS for EU, which is now almost already a reality.

Again, our input here was one, what is the problem we are trying to address, and two, if there is a real problem that's something to be addressed by the multistakeholder structures in charge of the root operations, so bring it here. Overall, the best thing we can do, I think, to tackle possible legislative intervention, is to be able to demonstrate that we've got it, security-wise, governance-wise. It may be well, of course, that we've got it. The service has never been interrupted, but it gets to being a little bit like Caesar's wife, if I can put it that way. Thankfully there are organizations that we've got it, and I refer to the OECD in the next slide, please.

OECD conducted work, a paper, a report about the security of the DNS, and a second one about the security of routing. Realizing that these issues are attracting policy interest, OECD started to work on this, relating it to the security of the DNS, as I said, for an audience of policy makers. We, and by we, I mean our Octo colleagues who know this stuff, of course, participated in that work. The OECD Secretariat conducted a series of meetings with technical experts. Maybe some of you might have been contacted as well. I'm pretty sure some of you were contacted. Generally, they're very open to input. They are neutral, and OECD is a very reputable organization. A paper by OECD telling policy makers what is an issue, and what is not an issue with regard to security can be an asset going forward when we get in such discussions. It is well invested time from the community to contribute to this kind of work.

The conclusion that the OECD gives in this report is what you see in red. Root servers should therefore not be considered as key security vulnerability for the DNS. Full stop. That was the draft report. Then it

was opened for comments to the OECD members. I will read to you some of the comments that were received so that you see where the concern is raised.

The comments were that aside from everything else that is described in the paper the governance system should be included, and that it is an important aspect. It was also raised that recent RSSAC ICANN documents on possible gaps in the governance system should be included. Further, that the signature of the root zone file itself and possible issues resulting from this process should be considered. In light of those considerations the suggestion was you should continue this last sentence to say yes, it's not a key vulnerability, but constant technical and governance improvements have to be put there.

Now, OECD took that input and continued the phrase, and OECD made sure to write, in red in the second bullet, that the multistakeholder community in charge of the root server operations is the one that has to constantly do that. Thank you, OECD, in that regard. That's it for me. I will hand it to Jamie for more pressing matters and much better English.

JAMIE HEDLUND: Thank you, Elena. I'm Jamie Hedlund. I'm in charge of contractual compliance, but I also head up ICANN's US Government Engagement function. As in Europe, the United States government has taken a much bigger interest in cybersecurity and mitigating cybersecurity risk. There has been a lot of legislative and executive branch focus on moving away from voluntary measures which, following the Colonial Pipeline and

other incidents, a lot of policy makers have lost patients with relying on things like the NIS, the cybersecurity best practices or whatever it's called and moving much more towards regulation. The one area where we saw this last year is in cybersecurity incident reporting requirements, which were adopted as part of last year's omnibus spending bill. The next slide, please.

These are excerpts from the bill. At a high level it requires critical infrastructure owners, providers, to report within 72 hours any cybersecurity incident. It is not self-executing. There's a rulemaking, which I'll talk about next, which is required to implement this, but industry eventually went along with this piece of legislation, which also touches on ransomware, which I'm not going to talk about here. We were very concerned about it because at one level it represented what could like an attempt for the US government to get back into the business of regulating ICANN and the IANA functions and root server functions at a time when other governments are also looking at this and may not have as benign interest as cyber-incident reporting but may want to do other things. Also taking into account the ongoing election at the ITU and the divergent views between the two candidates on the future of the DNS and the multistakeholder versus multilateral approach to governance.

We were successful in getting Congress to adopt a carve-out to this requirement, and you see it up on the screen there. The reporting requirements shall not apply to a covered entity or the functions of a covered entity that the director determines constitute critical infrastructure owned/operated/governed by multistakeholder

organizations that develop, implement, and enforce policies concerning the DNS, such as ICANN or the IANA. That's the law. Next slide, please.

As I said, it also requires a rulemaking within two years of the passing of the law. It was passed back in March. Within two years they have to launch a notice of proposed rulemaking, and then there has to be a final rule within 18 months of that. Basically, three and a half years from now. There are links to all these documents in the slide deck. Among other things, the rulemaking has to identify critical infrastructure, has to identify what an incident is, or a second incidence is. It has to put down what are the requirements for reporting, and consequences for not complying.

Where we are right now, they have just launched a pre-rulemaking listening session and request for information. This is not the beginning of the rulemaking, but it is their beginning to collect information from the private sector particularly on the questions, or on the issues implicit in the legislation. They'll have 11 listening sessions around the US between now or the end of the month and November. There's also a request for information, with comments due on November 15. As I said, they're going to look for what's a covered entity, what's an incident, what's a substantial cyber-incident, what should the report require and what content should be in the report. Then they specifically call out the criteria for determining if an entity is a multistakeholder organization, develops, implements, enforces policies concerning the DNS.

What's left out of the exception is an explicit carveout for root server operators. We think it's included, and we will certainly push that point

at the appropriate time, particularly if it looks like there's opposition to that. We could make the argument that IMRS is part of ICANN and that's explicitly covered. That does not necessarily extend to all the others, but the logic would seem to be the same.

One of the key things we were asked when we were on the Hill talking about this legislation, and we weren't lobbying against it, it was really clear. When we engage with Congress or other legislative, executive bodies, it's not to lobby for or against something, it's to raise education awareness and point out any potential unintended consequences for the Internet, for the multistakeholder approach. One of the questions we got was, "What are you doing now? How do we know that you're paying attention? How do we know that if there's a problem, that it's going to be addressed and that people who should know about it will know about it?" We were able to say that we do reporting, incident reporting, the monthly reporting for the IANA functions and for IMRS.

What we don't have is, unlike some sector-specific regulation, a binding obligation to report to somebody else. We do it because we think it's the right thing to do. We believe in transparency. The reason I say this is not that a hard, regulatory approach needs to be put in place, but the more credible whatever the model is that shows that there is reporting, accountability and attention paid to these incidents, the stronger the argument for the carveout.

The last thing I'll say as this moves forward, we are hopeful, but we're not technical. Elena is technical, I'm not technical. What I know from previous engagements with Congress is when you bring in technical people who know what they're talking about, despite all the caricatures

of Congress not knowing what's going on, which is true, the staff often get it. Engagement by technical experts is critical, whether it's with Congress, DHS, CSERV or anywhere else. I would really encourage engagement, and also engagement with one voice to the extent that that's possible. On behalf of all root server operators, with a unified message, as well as bringing the expertise and the technical knowledge.

With that, I'll shut up and am happy to take any questions.

[KAVEH RANJBAR]: Thank you very much. I have two points. The first one is maybe a simple one. To your last point, Jamie, first of all, thank you for presenting and bringing this up, and also all the great work, Elena. What you showed, I know how much engagement was done behind the scenes to get to those red lines, make those changes and add those exceptions, and I think the most fascinating thing was ICANN did a lot, and in collaboration with other bodies. I can speak for RIPE NCC, and I know the RIPE community as well engaged a lot and many other communities. It was a great effort and showed a great example of how we can actually cause change in legislation.

About the assurances, basically, Jamie, as you mentioned, that would help, of course I'm sure you know that there is a process for RSSAC37 and then GWG work. When that is in place, and that will take time and nobody wants to rush with that, of course, I think all of this will be answered. In the meantime, I can speak for RIPE NCC and K-root. We would be more than happy to make ad hoc statements basically, as long as they are in line with the principles which we have mentioned in

RSSAC37 and then 58 with detail. If you think that's helpful, I think that's something that individually RSOs need to decide on, but I can speak for RIPE NCC, and we would be more than happy to stand behind what we have stated in 37 as final goals of the governance rules. I think that would be an approach for that.

I have a second point, but if you…

JAMIE HEDLUND: I was just going to say that would be incredibly helpful, and we will obviously keep you, everyone posted on things as they move along.

[KAVEH RANJBAR]: For the second one, Elena, I really like the work which was done. I think that's great, as I mentioned. I have one worry about this, and this is based on my limited experience working with these legislators. I have a fraction of the experience that you and your team have dealing with this, and zero with the US legislators, but my understanding is organizations don't learn like that. Correct? We can propose changes and help, adding exceptions and things like that, but they are not going to be institutionalized. They will be in, maybe three years, five years, 10 years. Actually, that creates a gap, an opportunity, whenever there are exceptions, for an upcoming star or someone who wants to rise and say there is something that we can actually change. This is not something that really stays in the long run. Actually, these things solve a problem, buy us time, but in the time, we will need to do something essential. Otherwise, there are actually opportunities to reverse them and make

even stronger statements against what we want. At least, that's what I've seen.

Again, in my limited experience, the best way for any of these organizations to learn is to try and fail. Of course, in this scale you cannot, because it's global and it's one instance, so we don't want them to see the root fail. Correct? Other than that, I don't have the answer. That's basically my question, how we can make sure that a body like the EU in this case, but there are many others, really understands that this is something that we should not touch, this is out of discussion. Technically a root is a mathematical tree. You cannot have alternates and you cannot increase resiliency by reducing the number of participants as this thing suggests. How can we make sure they fundamentally understand this, and basically put this in a box that's, "Hey, do whatever you want, this is something that's not doable," let's say? I don't know the answer, but I know that exceptions are opportunities for people who want to actually rise and then say, "I can make a change and we can make something."

ELENA PLEXIDA: Thank you. It's a great comment, great observation. It doesn't mean that you cemented something and in the future it cannot happen again. I would say it is exactly the same, be it you have an exception, or you don't have an exception. I can reverse the idea and say that if you have a very strong particular exemption, that this one says, "There are out," it is a very strong message for the rest to come. It's really difficult to reverse. Now, you're right, that was a negotiation in the context of one legislative initiative. Some people learn, the ones that were around the

negotiation, but that's just it. They're going to change; they're going to somewhere else at some point in time. More important, as I was saying at the beginning, and sorry if I spent too much time on that, the political ideas are there and those are strong. Political ideas, although technically they might not be possible, might be counterproductive completely, they can mess things up.

The best thing we can do is what Jamie was saying. It is really strong when you have technical people talking about those things. Really, really strong. That's what we should aim to do more and more. Now, the catch unfortunately is that people like the negotiators in Brussels, or I guess in DC, the same thing in other organizations, they care to listen about those kinds of things when there is a folder on their desk that is relative. Otherwise, they have so many other things that they will not sit in a training or in a webinar that will talk about how the root server system works and what happens if it fails. Of course, we will try. We keep trying, we all do. At the same time, I would make the comment that NIS2, the process was educational for a lot of the environment, at least is Brussels. We know that for quite some time, a few years, we are safe. I don't know about the next. Again, it's the political ideas that I'm afraid of.

JAMIE HEDLUND: A great example of all of that in play is with, I don't know if people around here remember an attempt by US Congress to introduce new legislation protecting intellectual property online, SOPA and PIPA, and one of the reasons that bill failed was because of the provisions requiring DNS filtering and DNS blocking. There were a number of

technical experts who engaged with relevant offices and said why this was a bad idea, and ultimately it failed, but that idea has not gone away. It's been introduced in other jurisdictions. There is always the threat it will come back. With engagement from the technical community there is a chance that we can thwart that.

FRED BAKER: I have a couple of questions. On slide five the last word, is that adapted or adopted?

ELENA PLEXIDA: I copy/pasted that from the report, so it was definitely adapted. Now, if it was a mistake in the report itself, I don't know.

FRED BAKER: I would expect the word adopted there. Adapted doesn't make sense to me. Second, I would assume that on a lot of your questions you defer to, or you go to your own technical experts, which is to say the IMRS. You've mentioned that twice in the remarks so far. There are actually 12 different root operators and it might be worth your while to pose those questions to the RSSAC or to root ops in order to get the kinds of responses that you're looking for.

Liman?

LARS-JOHAN LIMAN: Thank you, Lars-Johan Liman from Netnod Sweden here. First, just a quick clarifying question to Jamie. You mentioned this second ruling. Who makes that ruling? Is that also the Congress?

JAMIE HEDLUND: Sorry, yes. Congress told the Department of Homeland Security, CSA, to do the rulemaking. They were authorized by Congress to do the implementation. It's typical. Congress or a commission adopts a high-level thing, and then the implementing agency develops and takes comment on, and finally adopts final rules.

LARS-JOHAN LIMAN: Thank you. That was my second alternative thinking about this. To both of you, thank you very much for doing this and thank you very much for the hard work that you put in behind. I have seen fragments of that, and I'm astonished. I really know how much and how hard work it is to make these changes go into these documents. It's a long path from the idea of knowing that we need to change this until it has gone through the right process, the political process of ending up in these documents. It is hard work, and I respect you every much and thank you very much for doing that.

You mentioned that input from technical experts is valuable and from Netnod's side, we are a very small company, but we try to contribute where we can. The problem we sometimes have is to know where and when to contribute. If you can help us with that part, we can try to help from our side with whatever expertise we can contribute. That's in our

interests, very much so, so we can probably set aside some resources fo that.

I had one more thing on my mind, which I will try to remember quickly. I'll save that for later. Thanks.

JAMIE HEDLUND: Just on the last point, after this meeting, the RFI and listening session announcement just came out the week before we came here. When we get back, internally we're going to consider how we engage. Do we engage at this point? Do we wait for the rulemaking? Obviously, we will share that with the RSSAC, but hope that you all will also consider, because it is a request for comment from anyone. You don't have to be a US citizen, and the more expertise you bring, obviously the more valuable the comments.

LARS-JOHAN LIMAN: The last thing came to me, and that's regarding incident reporting. I can understand a which for reports regarding incidents. I don't have a problem with that. The problem that, at least we as a root server operator have, is to report specifically to one, and it won't be one instance if every government in the world needs their own specified report. We'd have 250 reports that we need to issue within 72 hours or whatever time frame it is. Reporting is fine, but it would have to be something general that we can report to everyone, and preferably even be public about. That would be the easiest way. If that's a message that you can carry forward, that would work for us, at least.

JAMIE HEDLUND: Not only simplicity but also uniformity, that's the whole thing, getting away from policy fragmentation, making sure there's just one global policy, one global reporting function as opposed to this government wants this thing, this other government wants something else.

LARS-JOHAN LIMAN: That is also part of the Root Server System Governance working group and their goals, that there will be provisions for such reporting. It's in the plan. Thanks.

ELENA PLEXIDA: Thanks, Liman. If I can come in, I was about to say exactly that. It's much better and preferable, and I hope that's what we will end up with, is that you put in place your reporting system and we don't need to respond to anyone else. The same question, I have to say, that Jamie said, that was raised in DC, "Where do we find reporting if we want to see," was also raised in Brussels of course, in the context of the NIS2 discussions. From my perspective at least, and I'm not that technical, it was, if I may say so, the only rational argument that I heard in that discussion. "We just want to have some information. Where do we find it?"

Then if I may make another comment, thank you very much for your good words and the appreciation. We appreciate that, and of course you were part of some of those activities. I really have to say, going down what I have said before, it was a collective work. Many

organizations helped in that, and if they hadn't, we wouldn't have had this outcome. Thank you.

TERRY MANDERSON: Terry Manderson for the record, ICANN Org, IMRS operator, a technical person and a neophyte when it comes to jurisdictional issues, to say the least. A whole lot of work went into this with basically two pieces of legislation, NIS2 and the US version. Sorry, three, there was the OECD as well. Are we in a game of whack-a-mole, investing a lot of time for every jurisdiction coming up with a piece of legislation? How can we stop that? Can we stop that? Is there a pre-emptive retaliatory strike against this?

ELENA PLEXIDA: Your governance structure, I would say.

JAMIE HEDLUND: We're going to roll out the ICANN tanks.

TERRY MANDERSON: I can buy one.

[KAVEH RANJBAR]: Actually, to build a bit on top of that, no value judgement, I'm just saying that we know that the EU and US are supporters of the multistakeholder models. Correct? If we need to put so much energy to make sure friends don't get it wrong, and it's not friends and enemies,

it's friends and people who don't believe in this model. Again, they might be right, I'm not judging, but I know I'm working for this model. How much input will it take to deal with economies or jurisdictions that don't even support the whole idea, fundamentally? I think that's a bit scary.

JAMIE HEDLUND: This isn't limited to this issue. This is the Internet in general, and the downside of the success of the Internet is that governments have become much more interested and willing to intervene. I don't know that there is a global pre-emption. I think the better the model we come up with and the better we're able to sell it, to put it crassly, the less likelihood there will be fragmentation. As the Internet continues to be such a big part of the economy and people's lives, governments are going to be interested.

ELENA PLEXIDA: Completely agree. It's about being able to demonstrate how effective we are. That's the strongest argument, not that we will stop the train, but it's a convincing argument and a good one. Just parenthetically to say, yes, that's the concern. Even champions of the multistakeholder approach, I want to believe, do not realize that. We have to engage and explain, explain, explain. In the context of NIS2 not everything ended merrily and nicely. Article 23, which is about registration data, none of your concern as such, although it might have some merit, we'll see, for the WHOIS Disclosure System, it does clearly intervene, take over part of the GNSO policy making already.

FRED BAKER: Russ, you have your hand up?

RUSS MUNDY: Yes, thanks very much Jamie and Elena for the presentation. I had seen at least one of these earlier. I think it was for the general meeting at an ICANN meeting, and as the SSAC liaison to the RSSAC, I think that there might be a similar amount, although from a different perspective, a similar amount of interest from the SSAC, whether it would be as the SSAC trying to say something as an SSAC document, or if it would be individuals that are participants in SSAC that would be also willing to engage.

One of the things that I've noted is that at least from my view there has not been a great deal of information from the government policy activity in ICANN to, at least members of the SSAC and the RSSAC, for what is going on. What are the current hot buttons if you will? What are the current things that need support and attention from the technical community? I was wondering if there had been any thought given to trying to have at least an ongoing method of communicating what might be upcoming, what attention might be required to make responses to the legislation that passed, as Jamie pointed out, in March. I did personally just see the rulemaking announcements. It's an interesting read, whether you're a US citizen or not, for the kinds of things they're looking for.

I didn't know if there was thought given to trying to structure something, I'll say within our community, to convey this information

beyond the government policy group at ICANN, both for, not only what they're up to, but what kind of help might be needed, both currently and in upcoming things. Thank you.

JAMIE HEDLUND: Thanks, Russ. I completely agree with the premise of your question, which is that the more great minds that are focused on this, the more successful all of us will be. Mandy Carver, who heads up government engagement, has for the past several ICANN meetings had a session, a general session in each of the ICANN meetings on regulatory and legislative developments around the world. We published a lot of documents, and all that is well and good, but I think the suggestion of more focused or structured meetings with groups like SSAC and RSSAC I think makes a lot of sense. Since the transition and up until this, there have been fewer of these things percolating, but there's going to be more. We would certainly be happy to and would really enjoy the opportunity to engage more regularly with SSAC and RSSAC.

ELENA PLEXIDA: If I can just add to what Jamie just said, in addition to the plenary session that is taking place for, I don't know how many past meetings, the government engagement part of the ICANN website is a part where we publish various papers that we draft now and then for issues that we find from a government engagement perspective that will affect the community. They are not issues that necessarily have to do with the root as such, or one constituency or the other constituency. We just try to highlight and bring to the attention of the community issues. There's

also a page where we are publicizing upcoming opportunities for the community to give input. I will send the links to that. Thank you.

KEN RENARD: Ken Renard, with the US Army Research Lab. Again, want to reiterate, or thanks for what you do, and offer our support to do what we can. You mentioned education, how the system works. Root server systems are a very technical piece. I just wanted to point out, there is a session tomorrow morning, that's Tuesday, yes, at 9:00. It's an RSS information session. If anybody that's online or here wants to join and dive into some of the technical aspects of how the root server system works, it's an opportunity to dive in and get some of the background. Thanks.

FRED BAKER: Jeff?

JEFF OSBORN: Thanks, Jeff Osborn, ISC. I really want to add to what everybody else said. This is really terrific work you're doing, and we appreciate it very much. What I wanted to ask was, it looks like on Thursday there's a session called Update on Geopolitical Legislation Regulatory Developments. Is that a rehash of this, or is this additional information? This is making me feel like I have a lot more I need to catch up on. Would that be valuable?

ELENA PLEXIDA: Yes, that's exactly the plenary that Jamie was referring to. It's a plenary that we have in every ICANN meeting. It's much more general, so there we'll refer to legislative initiatives globally, and not specifically maybe those that are of interest to root server operators. This is much more targeted. You will hear many more initiatives if you follow the Thursday session. Still, I would suggest you did follow it. It give you, if you will, in idea what's going on around the world and where policy makers are going with it.

FRED BAKER: Erum?

ERUM WELLING: Thank you, this is Erum Welling from [inaudible] G-root. I have a question, please, about your reference on slide four, if we can go back to that, please. Could you elaborate a little bit about the EU funding that's referenced there? Is that a formalized process that's already been established?

ELENA PLEXIDA: Let me just make a differentiation here. NIS2 is a legislative initiative, which takes negotiations between Council, Parliament, et cetera. This strategy and the bullet within it is a number of initiatives that the European Commission is putting on itself to carry out. The European Commission has EU funding, has a very big budget, that has a mandate from the other institutions of the EU to spend as it thinks is more useful to the EU citizens. Therefore, they do have the funding to do this

activity. There's not more meat into it, as I said before, in what exact way they intend to do the funding, what is the precise idea behind the contingency plan. In the same strategy, as I said before, you have the DNS for EU initiative. Again, there, they were talking about EU funding. What they do now for the DNS for EU initiative is that they opened up a call for tender, to invite people to give proposals. The idea is that the EU budget, the EU funding is going to pay for the DNS for EU initiative.

Something equivalent is the thinking behind this one, but again, there is no meat to this and I really wonder a lot myself what is the exact problem we're trying to tackle and the rest.

FRED BAKER: Terry?

TERRY MANDERSON: I can only speak for the IMRS, but I think I would really like a briefing like this at every ICANN meeting if that's possible and if you folks are willing to do that. I'll leave it up to… I'm seeing nods of heads around the room from the other root operators, so maybe we can table that in RSSAC as a standing agenda item and we'll get clarification in RSSAC if it's okay with both of you.

ELENA PLEXIDA: Absolutely. We're more than happy. It's just that sometimes because legislative initiatives are going slowly we might bore you, or we might exchange and say nothing significant has changed so far, but yes. Absolutely.

TERRY MANDERSON: I'm happy to hear if there's nothing significant.

FRED BAKER: Erum has a hand up.

ERUM WELLING: Yes, sorry. I have another question please. You had made a reference about the Plenipot coming up, and one of the candidate's platforms includes identifiers, a focus on identifiers. How can we learn more about that, please?

ELENA PLEXIDA: In the link I shared with the publications from the government engagement team there are specific papers that are referring to specific countries and their strategy. Now, we don't need to hide, the two candidates that are now for ITU going forward are the US candidate, who is supporting this approach, the multistakeholder one, and the Russian candidate that is, as I said, very openly saying this should be moved to government led organizations. I will send you the specific link to the paper about Russia, where you can read more specific quotes that Russian officials have made, or the candidate himself, where you can see the line.

FRED BAKER: We're three minutes to the end of the session. I'm going to need to close the queue pretty soon. Do we have other people who want to dive in

before I do that? Failing that, I guess we're coming to the end of the session. Let's go ahead and close the session.

OZAN SAHIN: Thanks everyone for joining. Please stop the recording.

UNIDENTIFIED FEMALE: Recording stopped.

OZAN SAHIN: So, just a quick announcement, the next RSSAC session, which is with—

[END OF TRANSCRIPTION]