ICANN84 | AGM – Joint Meeting: GAC and SSAC
Tuesday, October 28, 2025 – 15:00 to 16:00 IST

GULTEN TEPE: Welcome to the GAC meeting with the SSAC session on Tuesday, 28 October, at 15:00 UTC.

Please note that this session is being recorded and is governed by the ICANN expected standards of behavior, ICANN community participant code of conduct, and the ICANN community antiharassment policy. During this session, questions or comments will only be read aloud if submitted in the proper form in the Zoom chat pod.

Interpretation for this session will include all six U.N. languages and Portuguese.

If you would like to speak during the session, please raise your hand in the Zoom room, and please remember to state your name for the record and the language you will be speaking in case speaking language other than English. And please speak at a reasonable pace to allow for accurate interpretation.

I will now hand the floor over to GAC chair Nicolas Caballero. Thank you.

NICOLAS CABALLERO: Thank you very much, Gulten. Welcome back, everyone. I really hope you enjoy fantastic Irish coffee. I have the pleasure of

introducing a very good friend and his team Ram Mohan from the SSAC. And we also have Suzanne and Maarten and Tara. Welcome. We're going to have a very interesting, at least in my opinion, session divided into four parts.

The first part and the most important, again according to my opinion, is the Importance of FOSS (Free and Open Source Software) in the DNS Industry. And I would add anywhere else, but that's a different discussion to have. The Impact of String Collision and Similarities on Security and Stability. This is kind of unavoidable at this point. And finally, the Possibilities for Cooperation Between the SSAC and the GAC. And then I'll open the floor for a Q&A session.

So welcome again. I'll give the floor at this point to my very good friend Ram Mohan. All yours.

RAM MOHAN: Nico, thank you. It's a pleasure to be back here with you here in Dublin but also with you in the GAC. We have been really honored that you have now over the course of several meetings continued to invite us and allocate time on your very busy calendar for us. On our part we not only value this time with you but we prepare quite intensively for it because we want to make sure that the information that we provide and the communication and the interactions we have with you are both at the right level but also

are actionable, have things that you can take away and go with. So that's the basis of what we do.

Without further ado, what I would like to do is to focus the first part of our time on the Importance of Free and Open Source Specific in the DNS Industry. To introduce this topic and share the details with you, let me pass the microphone to my colleague Maarten Aertsen who was one of the co-chairs of the work group on this topic. Maarten.

MAARTEN AERTSEN: Thank you, Ram. Thank you, Nico. Today I will talk to you about software. SSAC usually writes rather technical documents. This is not one of them, and the ICANN community itself is not its primary audience. This document is written for policymakers and regulated around the world. So I believe I am in the right place. And if it's not you, then I'm sure you have lovely colleagues who deal with cybersecurity.

Let's talk about software. If you condense our report in a single sentence, we find that the DNS is built on free and open source software. This is not advocacy. It's not us saying that free and open source software is better. It's a statement of fact how the DNS is actually built. Next slide, please.

FOSS stands for free and open source software. Free refers to freedom like freedom of speech and not price like free Guinness after this talk. FOSS is defined by four freedoms. Use—you can use

the software for any purpose. Study—you can study how the software works including its source code. Share—share and redistribute copies of the software. And finally, Change—you can change the software to fit your needs and release the improvements.

These freedoms that are part of the software license create a fundamentally different ecosystem for software development but also for distribution and maintenance compared to the proprietary model. While there are philosophical differences between free software and open source, this report uses FOSS to encompass both concepts centered on the four freedoms. Next slide, please.

The FOSS model has a different risk profile than proprietary software. As most free and open source software is maintained by volunteers, motivation plays a large role. So if people are working on software as a volunteer, they can also burn out. And this leads to abandoned projects.

Another risk of FOSS is that there is no warranty, no guaranteed support by default. So operators need to take responsibility to retain either development expertise in-house, exercise those freedoms and fix the software if it's broken, or they can purchase support contracts.

Where it is not volunteers but professional organizations that take care of open source, there is a free rider issue because the software is freely available. So you can have a situation where the funding is completely decoupled from use and where a maintainer is part of a

small initiative or organization that pay maintainers. These are vulnerable to funding shocks resulting from new regulatory burdens. For example, when an existing funding model is threatened.

So these risks are real and inherent to the FOSS model. Regulation that does not consider these tradeoffs can make these risks worse, not better. Next slide, please.

There are strengths as well. Here we look at the DNS in particular as opposed to the previous slide where we looked at FOSS in general. Looking at the DNS in particular, we see that there is a strong transparency and collaborative security strength. Academic and operator communities maintain a strong and active culture of openly scrutinizing the free and open source DNS software, and they've been at this for decades. You can find papers in the '90s looking at software flaws or ways to improve. So these flaws are openly discussed and fixed.

And operators that we surveyed for this research, we got over 100 operators to contribute, they appreciate the ability to diagnosis, verify, and patch vulnerabilities because the supply chain is open. Because they do not rely on the speed of the vendor but they can be proactive about it.

In the DNS in particular a number of popular DNS projects are not maintained by volunteers but by long-lived and stable organizations. These have been maintaining software

implementations for over 20 years. This longevity provides a track record that operators trust.

Another strength of FOSS in the DNS is that there is operational resilience through diversity. Multiple FOSS implementations allow operators to run different software reducing single point of failure. And it lowers the barrier for organizations to run their own infrastructure preventing concentration risks or as is recently a hot topic dependencies on foreign entities. Let's go to the next slide.

Let's talk about security. SSAC is focused on security, and it's very important to understand what determines security in specific. What doesn't determine security is whether a source code is open or closed. What doesn't determine is whether developers are paid or volunteer. What doesn't determine security is whether it's from a commercial company or a nonprofit.

Now what does determine security is rigorous code review and comprehensive testing, a well exercised vulnerability process, and active long-term maintenance with sustained resources.

To quote the report the security of any software project is determined by the quality of its development and maintenance processes not the visibility of its source code.

We hear a question a lot: Is FOSS more or less secure than proprietary software? The answer is neither. Security is determined by the quality of the development process not by the license model.

The policy challenge is that FOSS has a different risk profile. You cannot copy-paste regulations from the proprietary world and expect them to work in a reality that has FOSS.

I made some strong claims at the beginning. Let's look at some data. Next slide, please. Starting at the root server system level, we surveyed the 12 root server operators and tried to identify the software we use. We see a dominance of free and open source software. At least 9 out of the 12 root server operators use free and open source exclusively. Even operators that use proprietary software to perform this role often run FOSS alongside it for diversity and redundancy. The key takeaway here is that it's not a small percentage. FOSS is the overwhelming majority in the root server system. Next slide, please.

We also looked at the top-level domain operators. Here these entities provide authoritative DNS services. The key finding is that if you look at the operators that serve the largest amounts of TLDs, 9 out of 10 use FOSS for their DNS infrastructure.

Now for this audience it might be even more relevant how it works in the country level top-level domains space. If you just look at countries, we find that 20 out of 25 operators use FOSS. Collectively the ccTLD operators serve 234 unique ccTLDs using this, and that's only at the level that we looked at this data. So in reality this number is even bigger.

These are not small or experimental TLDs. These are major service providers responsible for millions of domains. Some examples,

Nominet in the U.K. runs FOSS, CNNIC in China uses FOSS, just to name a few. Next slide, please.

Let's look at registry systems, the database that stores domains within a TLD. We see two models. The first is a completely FOSS system. These exist. They're not the majority but it shows that it's viable, so it's an important point.

The most popular model is where registries are proprietary. But even here we find that these proprietary systems are not built from scratch. Instead they are proprietary integrations built on top of free and open source software. And of the ten major platforms that we surveyed, all incorporate FOSS components. So even when the top-level business logic is proprietary, the foundation is FOSS. Next slide, please.

The resolver ecosystem is the hardest to measure, but here we again find substantive use, substantive presence of free and open source software. Eighty percent of users worldwide use a local resolver and here FOSS is dominant. Even when you look at the commercial solutions of which there are many, in most cases if you look inside what they sell, it's FOSS. The same goes for public resolvers. A number of them are FOSS.

We made a little case study in the report of Cloudflare who have a proprietary core surrounded by FOSS. At least four of the biggest hyperscalers use FOSS for their DNS solutions. Others use FOSS

libraries as components within proprietary resolvers. Next slide, please.

So to quote the report in the most critical parts of the DNS infrastructure FOSS is the norm and proprietary software is the exception. It's not exaggeration. It's not advocacy. It's just a rigorous finding from the research that we did. The Internet's core naming systems run primarily on software that is collaboratively developed and freely distributed. Next slide, please.

The traditional supply chain regulatory approach requires security standards, possibly by imposing these on operators of critical infrastructure. You hold them liable for failure and they turn to their suppliers and set these requirements via contracts. And you enforce rules through procurements and market access.

Why does that fail for FOSS? FOSS is often provided for download at zero cost. There might not be a supplier relationship in the traditional sense. There is no operator vendor contract or there's even no vendor to regulate, just a volunteer.

So in posing compliance burdens on operators to affect their supply chain could cause them to destabilize the small organizations that maintain this specific. Or if it's volunteers, they could lose their interest, and this causes abandonment of projects due to legal risk, switching to proprietary licenses, or even avoiding jurisdictions. The result is that software that everyone depends on becomes less available and less secure. Next slide, please.

We included case studies because major jurisdictions like the U.S., U.K., and EU have been developing FOSS aware policies. I will not go into these in detail unless there is interest, but this can be done. Next slide, please.

These are the five actionable guidelines we came up with. SSAC is indifferent to if you regulate. It's also not our position to have an opinion. But if regulations in your jurisdiction are being considered, please acknowledge the critical role of FOSS. Recognize that global infrastructure relies on it, and it's a strength to be preserved.

Consult the open source community. Engage maintainers, foundations, and operators in policy development and avoid unintended consequences.

Make use of the contemporary cases that we collected and learn from emerging models.

Incentivize sustainability. Encourage, for example, contributions to free and open source software as an investment in public infrastructure.

And address systemic risks that do exist in the entire software space, not just FOSS, collectively. Fund ecosystem wide solutions for shared dependencies rather than placing the burden on individual maintainers.

I think that gets us to the end of this presentation. I'm really looking forward to your questions.

MARCO HOGEWONING: Thank you, Maarten, for a clear and concise presentation. And of course as I passed on the message from Ram earlier, I recommend everybody to follow the link and read the actual report.

Timewise we have the room for a few questions. The first one on my queue is actually sitting next to me.

NICOLAS CABALLERO: No, no, it's the European Commission.

MARCO HOGEWONING: Okay, we'll go to the European Commission first. Thank you.

GEMMA CAROLILLO: Thank you very much chair and vice chair, but I'm happy to leave the floor to [inaudible] if you prefer going first. Gemma Carolillo, European Commission. We are among those you are addressing I guess also with three out of four of the case studies.

This is a topic really important for us, and I want to stress that we as a regulator also have learned from this process in terms of how to incorporate the different characteristics of open source into digital regulation. And this has been I would say a painful but very useful process and I think we are learning collectively from that and we are achieving good results at the moment.

My question regarding security of supply chain because this remains an issue. Even if we want to try to go around it, this remains an issue. If you have a take regarding initiatives like the software bill of material and how this could help basically address the issue of security of supply chain. Thank you.

MAARTEN AERTSEN: Thank you, Gemma. You ask whether SSAC has an opinion on the software bill of materials. Unfortunately, I'm speaking on behalf of SSAC and we have not looked at this specific measure. I am willing to give you my personal opinion, so that's the disclaimer up front.

So, yes, security is a problem in the software space—proprietary software, free and open source software. I think where the software bill of materials can help is where people buy software, organizations buy software that is proprietary but is mostly FOSS inside. Because then you get into these situations where a component is vulnerable and it's vulnerable for everyone, even for all the products on the market. And if you don't know what's inside as a vendor or even as a purchaser, yeah, how can you start fixing things? So in that sense, it's an interesting instrument. It's also early days.

And I really appreciate your comment about learning collectively while I'm speaking on personal behalf. I found it fascinating to watch the policy development process in the EU and I'm happy that we have a case study that we could include in this report.

MARCO HOGEWONING: Thank you, European Commission, for the question. Thank you, Maarten. I have Bangladesh on the queue and then still the chairman next to me. And then I'll close the queue and we'll move on for the sake of time. So, Bangladesh, you have the floor.

DR. SHAMSUZZOHA: Thank you. This is Shamsuzzoha from Bangladesh. I think this is a very nice and comprehensive presentation. Especially being from Bangladesh and responsible to work with different agencies for the security standards in Bangladesh. They're some of the very [inaudible] that they produced.

Especially interested from two aspects from my side. One if that we are also working with [inaudible] Bangladesh to set their security standards and their [inaudible]. So that also covers the publishing of software in specific [inaudible] as well.

In addition to that, we are also responsible for sitting and collaborating with the national critical infrastructure, especially setting their [CM] and SWOT type of solutions for security operations.

So here is the debate that we have definitely when we try to [inaudible] even in the government procurement system that we are promoting the free and open source software. But one of the arguments that we face is about the inherent capacity within

[inaudible] especially for the [inaudible] and also the issue of quick and [inaudible] requirement.

So if there is not the inherent capacity in [inaudible] so there is a big risk especially when you're dealing with the national critical infrastructure. And also to some extent about the operational cost.

So this may be a question or like your insight about how to address this especially when we're dealing with sensitive critical infrastructure. Thank you.

MAARTEN AERTSEN: Thank you. In that sense I think there is less of a difference between proprietary and FOSS than one might think. Because if you are running critical infrastructure, the operator has a responsibility of keeping things running smoothly. And if you decide to use FOSS, which most do, then you have either expertise in-house which is a cost. You need to have experts. Or you need to find them elsewhere, and in many cases if you look a the most popular software, these organizations are funded through support contracts.

Now if the situation would be different and there would be only proprietary software, then you would pay license costs and presumably also get support. So in that sense, I think there is not that much of a difference with all the strengths that we listed in the presentation being a difference. Like no vendor lock in, etc.

But yes, critical infrastructure is special in that it has these uptime requirements and expertise is necessary to make that happen. And

each operator can make choices depending on how much bandwidth their government provides them to make those choices.

MARCO HOGEWONING: Thank you both. We'll wrap up and give Nico the floor as the very big FOSS supporter he is.

NICOLAS CABALLERO: Thank you. No, I'll be very quick. And thank you, Maarten, for this fantastic presentation. Could you please very briefly comment on how open source avoids lock in situations for government, especially for developing countries not only in terms of cost but in terms of actually…. Let me put it this way, insider security costs.

MAARTEN AERTSEN: Vendor lock in is the situation where you decide to invest in a certain product and you are then not able to migrate away because the investment you did is too large or switching costs are high.

The advantage of FOSS in the situation of vendor lock in, including with cybersecurity, is that you are not actually required to retain your relationship with your original maintainer. Sometimes there are also other organizations that are able to support you in your deployment, including in patching.

Now you will always be dependent on the original developer to develop patches, but it's not the case that like in proprietary software there is only one entity to work with. So I could see maybe

a country with a smaller budget seeing this as an innovation boost to try and build expertise locally instead of paying other entities outside of the country. But that's, I guess, a choice they can make.

But I think that's what I can say about vendor lock in. It's again, I guess, my personal opinion because we don't talk about this in the report as much.

MARCO HOGEWONING: Thank you, Nico, for the question and Maarten for your lovely answer. I think based on time let's move on to the next topic which I invited SSAC to also a bit of capacity building. And to recap, I know that there are many new or newer GAC members in the room for whom this is probably a relatively new topic. But it is important and it's getting even most important as we head up to the next round. So I guess given Suzanne is on the table, I guess I can give you the floor on this one. Thank you.

SUZANNE WOOLF: Okay, thank you, Marco. And thank you, Maarten. Excellent as always. You're a tough act to follow. So yeah, as Marco said, I get to talk about NCAP name collisions because I co-chaired the name collision analysis project which was originally proposed by SSAC but implemented by a discussion group from across the community.

And as Marco said, there are not many of you that have been around long enough to remember, but this is not a new set of

issues. We first ran into name collision challenges in connection with the previous new gTLD round. But we did have to revisit it because a number of things have changed as far as the technology and the expectations in the network ecosystem we have to live with. Next, please. Back up one.

So what is a name collision? It turns out to be really difficult to define except it does turn out to be one of those things you can tell if you see it. One way to think of it is you think of domain names like house addresses. If two houses share the same address, it becomes hard to know which one should get mail or deliveries. There are also security issues if the mail gets delivered to the wrong address. Just think of the privacy implications alone.

In the DNS name collisions occur when a domain used in the global DNS namespace, the public Internet we all think of, and is also used in a different namespace such as a private network operated by your VPN provider where different names are valid and that's okay but where the same name means different things what you're looking for can be misinterpreted. It gets confusing really quick. Next, please.

These next few will go by pretty fast because we're avoiding too much detail and trying to keep to the higher level. But the slide deck will be available, and we're always happy to talk about the technical details.

What is not a name collision? Some of these terms are going to be familiar if you've been looking closely at the Applicant Guidebook

or any of the work being done around new gTLDs. Name collisions are, for instance, not the same as string similarity or confusingly similar strings.

Name collisions are a technical problem causing security and stability issues caused by delegating the exact same TLD already used in a private context. Example.corp in your private network, if it's going to be the same as a name in the public Internet and it means something different, it's asking for trouble. The risk is the queries for private names will leak into the public DNS which also causes technical conflicts and security failures.

String similarity is also a challenge for the new gTLD project and the Applicant Guidebook and so on, but it's more based in user perception. It's a user problem causing confusability issues caused by different public TLDs that look or sound alike to a human. If you've got .example with a lowercase "l" and .exampIe with an uppercase "I," the human can be confused and you end up with a risk of phishing, fraud, loss of user trust and adding impact on users.

The takeaway is there are lots of ways collision issues can arise. The important feature is that when a computer confronts ambiguity, the results can be confusing and dangerous. Next. Thanks.

The high-level take here is the technical details aside, understanding name collisions is important for Internet security and falls directly into ICANN's responsibility for the security and stability of the DNS root. There are risks of unintended

consequences when businesses have used names as internal TLDs that may leak to the global Internet.

Introduction of more new gTLDs increases the probability of these challenges because there are more names that could be already in use in private context but that are also being delegated into the public Internet namespace.

And measuring name collisions is difficult, and we'll get into this a little bit more, due to the evolution of technology and network infrastructure over time particularly since the last time we did new gTLDs. There have been privacy enhancements, for instance, in the DNS that make it harder to measure what's going on. That's part of the point of privacy enhancements. Also, alternative naming systems that have made the DNS landscape more complicated and in general measurements are more difficult. Next.

I wasn't kidding that this set of issues goes back aways. One slide further. Next. There. Thank you.

In 2012 the new gTLD round accelerated the growth of the root zone which caused questions about what happens when new strings are added that may already be in use in a limited context not in the public root zone.

In 2013 SSAC took up the topic and issued an advisory highlighting that significant security and stability problems may occur as a result of name collisions.

The most significant detected string collisions, and again some of you might have heard of these, .home, .corp, and .mail which were being used in so many private contexts that there was a lot of data and there were many risks to identify as far as trying to delegate them in the global root, the public domain name system.

In 2017 the ICANN Board asked SSAC to conduct comprehensive studies to enable all future gTLD delegations to be done in a secure, stable, and predictable manner.

And the NCAP project, I guess there were two separate projects, came out of this tasking from the Board and some follow-on questions.

In the final phase, NCAP Study 2 was published early in 2024 because we wanted to make sure that what findings we were able to put together and our recommendations could inform the next new gTLD round.

Having a team from across the community and not just SSAC members was kind of a new thing for us, and I think it worked out very well. But we did get to take up the previous work and some more recent research and build on it. Next.

The major undertaking of the NCAP projects was to analyze the current situation with respect to finding and mitigating name collisions and to make recommendations to update the handling of name collisions for the upcoming new gTLD round. This is presented as a new risk assessment framework for not only finding

name collisions but assessing how much and what kind of damage could occur and what kinds of mitigations or prevention would be possible.

We do have to point out that assessment has become more difficult for various reasons. We already pointed to that. It turns out that one of the biggest is the fact that a lot of data we used to be able to get about what names people were looking up has been obscured because Janus does a lot more than it used to for the privacy of users. This is good for the Internet and for users but not necessarily good for the effort to understand it all.

So there were some really interesting challenges along the way, but we were able to work with what we could get and we've been able to meet the goals here.

Goal 1: Ensure that name collisions can be assessed. We've got a framework of escalating levels of examination of detail, depending on what risk seems to be present with a specific set of name collisions.

Goal 2: Provide a process for ICANN to evaluate mitigation and remediation plans for identified name collisions. The thing that we discovered even more than in the past all of these cases are going to be at least a little bit different from one another. Next, please.

There will not be a quiz on this, but this is the diagram that was in the report of the framework that came out of NCAP Study 2 taking

in terms of account the risks of name collisions and the evolving challenges of finding and mitigating them.

One of the key features is that we provided for a technical review team to oversee the process and make qualified judgment about what risks might attach to a particular case. We were able to assume that in many cases there doesn't have to be ongoing risk.

Mitigation or prevention is possible but because no two cases are exactly the same, we assume a fair amount of judgment will be required before we can be sure that name collision risks are being properly addressed. So there is some amount of this framework that relies on automated means and some that will go to an expert panel much like what ICANN uses in other contexts where issues can be complicated and some amount of judgment helps inform the process. Next.

So the benefits of the collision risk assessment framework NCAP Study 2 put out for the community features proactive risk management that identifies name collision risks and allows for the development and review of mitigation strategies before they can cause harm.

The framework, we worked very hard to make it consistent and effective. There’s a centralized approach to some of the analysis that ensures thorough risk assessment and mitigation across all new gTLD applications, again because the responsibility for the root zone lies with ICANN.

The framework is data-driven and enables informed decisions for secure expansion of the Internet's namespace.

We were also able to address a great deal of privacy concerns surrounding this area of work. Because while risk is inherent in assessing name collisions, one of the things that we ended up emphasizing, it's a privacy risk of not accurately assessing name collisions and having the wrong data go to the wrong people or the right data go to the wrong people. The privacy risk of not accurately assessing name collisions in our judgment is greater than the risk associated with assessment.

And again, every case is different, but being able to do a comparative analysis of risks of acting as opposed to not acting gives us an additional tool for analyzing these cases. So we conclude with early risk detection and informed mitigation are crucial for the security and stability of the DNS.

That's the high-level take. Happy to take questions if there's time.

MARCO HOGEWONING: Thank you, Suzanne. Much appreciate it. I too stand forever then corrected for colliding between name collisions and string similarities. I will not make that mistake again. And also, very happy to see the institutional [inaudible] that SSAC brings to this topic across the years. I see Nico put his hand up. We have room for one or two questions. I see nobody in the queue so, Nico, go ahead.

NICOLAS CABALLERO: This is a quick comment. If we can go back to the slide on Page 23. There we go. So we have four steps there and my question is regarding the time. What would be on average the time? Are we talking about days, weeks, months? I just wanted to compare these with the 32 steps. You remember yesterday the presentation with the GNSO, right, in terms of efficiency and speed and many other things. So on average, how long would this take?

SUZANNE WOOLF: That was actually a question that we discussed a great deal, and we're not able to come to a final consensus about what to recommend because as you say there are pressures in the direction of making it as quick as possible but we also don't want to miss important risks. So we were thinking in terms of weeks not months or years, but that's actually something that we had to leave for the staff and the community to make final decisions about.

MARCO HOGEWONING: Thank you. We are good on time to take another question, but I see nobody in the room. So then I just thank you, Suzanne, for your elaborate explanation. As you said, the slides will be online.

SUZANNE WOOLF: Yes.

MARCO HOGEWONING: And we can move on the our next topic. That was actually brought forward by the DNS abuse topic leads who were wondering if that we now have an issue paper whether, Ram, you and your SSAC colleagues were able to share any technical recommendations or view of the issue paper as it's been published.

RAM MOHAN: Thank you, Marco. Just before I respond to your question, I also wanted to inform the GAC on the previous slide about some work that we have just begun which is linked to the namespace. We've begun a work party called Responsible Integration into the DNS Ecosystem (RIDE). And what we're focused on is what happens when identifiers in other namespaces, in specific the blockchain naming space, what happens when those identifiers want to link and interact with identifiers, domain names, and other systems that are in the DNS system. We've begun work there, and we expect to provide some commentary and some conclusions on it.

Specifically, we're focused on and we're concerned about issues about the domain name life cycle, user confusion, fraud, things like that as well as security and stability risks that could be introduced to the DNS itself when you have systems in other namespaces that use terms, words that are similar to the namespace that we're used to but are not exactly the same but are linked in some way. So we've just begun the work. We'll keep you informed on that.

On the next slide to your question, Marco, we are very pleased that there is a policy paper that has begun, or at least there's some work

that has begun, on DNS abuse and there's a policy development work that has begun. You could go to the next slide.

In the past what the SSAC has done has been to provide comments and advice after policy recommendations come through. We're changing the model in collaboration with our colleagues in the GNSO. We've been invited to be represented in that PDP process if you will.

Now what we're doing is we're not participating in the discussions on should it be one track or two tracks or three tracks or all combined or anything like that. Those are for the policy development people to contribute to. However we intend to come in and speak about specific issues that deal with abuse, what our observations are, and particularly because we're spending a lot of time looking at the evolution of the abuse and where that is going.

And so we're quite focused in that area. We think it's an important topic in our conversation with the ICANN Board, for example, for the 2026 priorities. We endorse some of the things that the GNSO, the contracted parties have been saying that DNS abuse has to rank high on their list of priorities. There's always a competing list but if we don't get this right and if we mess this up, its not just end users that get affected. It is the reputation of this self-regulated multistakeholder model that we all hold up to be a great example. We have to do the right things, and DNS abuse has to be a big focus.

So we're deeply involved in that, engaged in that, and we intend to participate far more at the design stage than we have in the past.

MARCO HOGEWONING: Thank you, Ram. This is wonderful to hear. As it's such an open discussion I wonder if any of the anti DNS abuse people want to respond to that. Or any further questions to SSAC on this? Or anybody else, of course, who has a question on this particular topic? Janos, European Commission.

JANOS DRIENYOVSZKI: My thanks again for being here today and for your presentations. What we are wondering a bit about with the PDPs it's important to capture the right scope. We're going to put a lot of effort into it. And we're wondering about your views on the bulk registration track, let's call it that, on the bulk registration issue. Because of course, what we want to achieve is in the end of the policy development process we have something that is impactful and really targets what we want it to target.

So we mention APIs, but we were wondering if the approach would really cover fully the majority of technologies or measures that enable large volume registrations. So I would just be very grateful for your views if that is a good approach or the scope should be phrased in a way that it of course ensures sort of a future proof approach in the end. This is my own interest. I don't know what

other technologies might exist that would enable this kind of large volume registrations. Thank you.

RAM MOHAN: Thank you. There's a nuanced answer to that because you have examples where there are legitimate reasons to do a bulk registration. You have a company that wants to protect its new product and it registers a hundred of them across. And it's also do they register across multiple TLDs, inside of a TLD? There are specific things in there.

And I want to note that API access is not always the only way for bulk registrations. We have seen plenty of cases where people with bad intent have registered using a non-API model as a way to kind of hide because they know that API things are being looked at.

Having said that, I think that this is a good area of investigation. Bulk registrations need to be defined. And one of the concerns that we share with some others in the community is if you set a threshold, if you say anything less than and you pick a number is not going to be scrutinized to the same level, then we can expect that to be gamed. So there is some work to be done there.

My hope is that there will be a policy created that provides the broad framework for the kinds of behavior we want to prevent rather than the specific methods by which that behavior is being perpetrated. So I think that's the distinction that we should try to aim at in the policy development process.

MARCO HOGEWONING: Thank you, Ram. I saw the queue is sort of empty, so that kind of gives me the opportunity to then bridge in the next one. And again, much appreciate your input here. And as you said, you're going to be part of the PDP in your opening you mentioned and then we are strengthening the ties between the GAC and the SSAC. So that kind of leads to a more open question on where do we see opportunity to collaborate. We will both GAC and SSAC be part of this PDP. It might not be the only way forward.

If I can get to the next slide. Or is this still about DNS abuse, India, or is this about this particular question? I see your hand up.

[INDIA]: About the DNS abuse in general I think maybe I would like to get the views of Ram there. As to what potential can the reduction of the time 15-day window for the [hold accuracy] can have on the DNS abuse. I think we believe it is one of the simplest steps which can be taken. It can go a long way in actually bringing down and mitigating the DNS abuses.

Maybe authentic validation or verification would have been a challenge maybe ten years back, but presently these things are done. We do it at least three or four times every day. You check in a hotel, you do authentication. You go in an airport lounge, you do authentication verification. But I really wonder as to how can we allow someone to have a domain name even without

authenticating. And mind you, you're not even identifying. It's merely an authentication.

So with that, would like to have your thoughts on this because I really feel you understand the rationale as to why the [inaudible] [should] given at all.

MARCO HOGEWONING: Thank you. So I understand this is about the two weeks that sit between, the two-week leeway there for verification, right? Ram, any views on that timeframe?

RAM MOHAN: Thank you so much. We have opined on urgent requests before and I think the short form of it is that is if it is called urgent, it really ought to mean something. In our view, that is something that requires very rapid response times to it and should not be…it's the equivalent of calling an emergency service in real life. When you call an emergency service, you don't expect to get responses in 15 days or in two business days or something like that. So our approach is that that's important.

To the question on validation and verification, we have from the SSAC I don't know that we have necessarily developed a common SSAC, all of SSAC, point of view on this. But we do note that we've had security researchers and some law enforcement folks say that they feel impeded by the lack of access to some of the registrant information in an easily accessible way. And so we have been

encouraging the development of tiered access systems that can provide disclosure to parties who have legitimate interests in that information.

So that's kind of where we stand. Urgent requests in specific we think, especially when the GAC and the Board work together on this, you should really keep in mind the dictionary definition of "urgent" and not only "commercially reasonable" should not be the baseline for it. Thank you.

[INDIA]: No, my question was not regarding the urgent requests. My question was about the potential of DNS abuse mitigation by reducing the 15-day window period between the verification or validation and the registration of the domain. I think that is something which I really find I think incomprehensible in today's age.

RAM MOHAN: Yeah, thank you for clarifying. Again, I don't know that I can speak for the SSAC as a whole. I think that this is an area that needs to be looked at quite strongly. We should be looking at user harms and measuring them up against other contractual requirements and policy development processes that are here. But we should keep user harms top of mind in this area.

MARCO HOGEWONING: Thank you, India. Thank you, Ram/SSAC. Are there any more burning questions? We have two minutes left. I'm also happy to start wrapping this up then and send you off to your coffee. So let me add as it says here “Possibilities for Future Cooperation.” Nico?

NICOLAS CABALLERO: Thank you, Netherlands. I have one last question regarding cooperation in terms of open source software. Would that be part of the package? And I'm asking this because during the last IGF in Norway the government of Norway has been basically sharing open source solutions. And there are more than 45 countries currently benefiting of that fact. So what would be the way in case we have any distinguished colleague from the GAC, in case they are interested in finding out how to cooperate in that regard? What would be the procedure?

RAM MOHAN: I would suggest that they connect with me as the chair or our excellent SSAC staff. And we will foster a dialogue that can look at the best ways by which we can provide content and other support to you and also collaborate and work alongside you. We’re keenly interested in this area. This is one of the few SSAC reports that’s actually aimed at you, so come work with us. We want to make this work for you. And if you do come and work with us, that actually validates that doing work like this is a useful endeavor for us.

MARCO HOGEWONING: Thank you. On that note, I very much want to thank you, Ram, Suzanne, Maarten, Tara for joining us again. And to the topic of this slide, looking forward to future cooperations. With that, unless you have any final comments, Nico, I think we can have our coffee.

NICOLAS CABALLERO: No, just some housekeeping details. We're going to have a coffee break now. Enjoy your coffee. We'll reconvene at 4:30. Thank you very much. This session is adjourned. Thank you, Ram.

[END OF TRANSCRIPTION]