ICANN85 Mumbai | CF – Joint Session: NCSG and SSAC
Saturday, March 7, 2026 – 15:00 to 16:00 IST

ANDREA GLANDON

Hello, and welcome to the joint session, NCSG and SSAC. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct concerning statements of interest. Please observe the following guidelines to participate in this session. I will also post them in the chat shortly for your reference.

Only questions posted in the Zoom chat identified as a question will be read aloud during this session as time permits and when directed by the chair of this session. If you wish to speak, please raise your hand in Zoom or otherwise as directed. When speaking, please state your name for the record and speak clearly at a moderate pace. And I will now hand the floor over to Ram and Rafik. You may begin.

RAM MOHAN

Thank you so much. Welcome everyone to this session. Rafik, it's good to have you here again and for us to meet one more time. We're starting to build a habit, and these are good things to do.

In our preparation for this session between the two of us, we thought about some topics. If you could go to the next slide, that shows the topics that we had thought of as useful to discuss. So

without further ado, let me just hand the microphone to you, Rafik, for some welcome remarks, and then we can go to Maarten.

RAFIK DAMMAK Thanks, Ram. Yes. Really the intent here is to have this discussion on a regular basis so we can talk about several topics of interest where we can find common ground. And as you can see, we are talking about follow-up of previous action items.

RAM MOHAN Speak closer to the mic.

RAFIK DAMMAK Yeah. Okay. And to really follow up on previous discussion topics, because we want to act and to work together on those issues, not just discussion for the sake of discussion.

So, we selected a few topics. We had that going back and forth. We wanted to hear about one of your latest papers because we have interest to know what SSAC is working on. But also we want to know more about how you work. We heard about a new working party on AI, if I'm not mistaken. We wanted to know what you are planning there, what you want to do, and also what you have in your pipeline.

Yes, we have those topics like DNS abuse, et cetera, that we will try to go through within this session. So thanks again for this opportunity and looking for fruitful dialogue today.

RAM MOHAN

Thanks, Rafik. Look forward to a fruitful discussion. To start with, we're going to go to Maarten Aertsen, who was the work party co-chair on the free and open source work party from last year. We published a report, SAC-132, and we want to brief the NCSG on what our findings were and some implications for the future. Over to you, Maarten.

MAARTEN AERTSEN

Thank you, Rafik. Thank you, Ram. Next slide, please. Today I'll give you an overview of our latest publication, SAC-132. Just to set the stage, we usually write rather technical documents. This is not one of them.

For this document, the ICANN board was not our primary audience. We wrote this document for an audience of policymakers and regulators around the world, but also those that interact with them. So it's a document for the internet community, in particular, the subset of the internet community that talks to their local policymakers. That, in particular, I think makes this document relevant today and for a session that is focused on our cooperation between NCSG and SSAC.

Personally, I work for a nonprofit, so I also feel a connection with this community. Let's start and dive in. The conclusion of the report is that the DNS is built and sustained on free and open source software. This is not advocacy. It's not us saying that this is

somehow better. It's a statement about how the domain name system infrastructure is actually built. To understand why this is so important for policy, we need to be very precise about what free and open source software is and, just as importantly, what it is not. It's not just free software as in beer. It's a completely different model for building and maintaining critical infrastructure.

Next slide, please. Free and open source software refers to freedom as in speech and not in price, so not free beer after this session. It's defined by four freedoms: the freedom to use a software for any purpose, study how the software works without restrictions, to share and redistribute copies, or to change the software to fit your needs. These freedoms are legally granted by software licenses, and if any of these freedoms are restricted, it's not open source.

These freedoms create a fundamentally different ecosystem, and that's what we'll focus on today. Not just for software development, but also for distribution and maintenance compared to proprietary software. While there are philosophical differences between so-called free software and open source, in the report, we use FOSS to encompass both concepts that is focused on these freedoms. If you're interested in the philosophical differences, there are good books written on the subject.

Next slide, please. The FOSS model has a different risk profile compared to proprietary software. For example, a distinct and inherent risk of FOSS is maintainer burnout. Most FOSS relies on

single and unpaid volunteers. If you're a volunteer, you can burn out, and that leads to abandoned projects.

Another inherent risk is that this software does not come with warranty by default. There's no guaranteed support. Licenses usually explicitly state that software is provided as is, and no one by default is legally required to fix bugs. If you're an operator and you use free and open source software, it is your responsibility to retain development expertise in-house, or you purchase a separate support contract if that's available.

Another inherent risk is the financial aspect. If FOSS is maintained not by volunteers but by an organization, there is this aspect that funding is decoupled from use, so you can just download something and use it. There is no requirement for payment. When there are small initiatives or organizations that pay maintainers, these are vulnerable to funding shocks, for example, from new regulatory burdens where an existing funding model is threatened.

Let's move on. If you zoom into DNS in particular, we previously looked at inherent strengths of FOSS in general. Now we'll look at strengths of FOSS specifically in DNS. There are also some strengths here. The first is transparency and collaborative security, where the DNS operator community has for decades maintained a strong active culture of openly scrutinizing FOSS DNS software, in particular if you look at the academic community. Flaws are openly discussed and quickly fixed, and operators appreciate the ability to verify software components and expedite patching.

There's also the stability of projects. The most popular DNS projects are supported by long-lived and stable organizations, and these have maintained the software for twenty-plus years. Examples are ISC in the US or CZ.NIC in the Czech Republic. These organizations have provided this support for years, which has given them a proven track record that operators have learned to trust.

The advantage of having multiple implementations in open source gives operational resilience through diversity. There are multiple implementations, and this allows operators to run different software at the same time, which reduces single points of failure. It also lowers the barrier for organizations to run their own infrastructure, preventing concentration risks.

Next slide. What we get asked a lot is whether it is more or less secure. In the report, we concluded that this is essentially the wrong question because security is not determined by a license or the visibility of source code. It's determined by the quality of development and maintenance, and perhaps the processes around this. The key takeaway here is that the FOSS development model has a different risk profile as compared to proprietary software, not that it's more or less secure. This matters for lawmakers, which is what we'll see next.

Next slide, please. We made a bold claim in the beginning of this slide deck that the DNS is overwhelmingly built on FOSS. Let's review some data and look at the root server system. In our research, we surveyed twelve root server operators to identify the

software they use, and nine out of twelve use FOSS exclusively. Even those that run proprietary software often run FOSS alongside it for diversity and redundancy. FOSS is the undisputed dominant technology at the root.

Next slide, please. If you look at the TLD level, the story is mostly identical. We analyzed the largest operators that provide authoritative DNS services for top-level domains, and nine out of twelve TLD service providers use FOSS for their DNS infrastructure. For ccTLD specifically, twenty out of twenty-five use FOSS DNS software. This is where we zoom in on country infrastructure. These are not small or experimental TLDs. These are major service providers responsible for millions of domains. Some examples: Nominet operates the UK TLD, one of the largest ccTLDs, and they use FOSS nameserver components. CNNIC operates .cn, one of the largest TLDs in the world. PIR operates .org.

Next slide. We also look behind public-facing servers at the registry databases and their operators. Again, here we find FOSS being dominant. We find two models here. Model one is where the entire registry is FOSS, like for example, CZ.NIC's FRED system. This is an example of a complete registry platform that is FOSS, and it shows that FOSS is a viable and complete solution, not just a minor component.

In all honesty, the second model is much more common, where the registry platform is a proprietary platform. But we found that these platforms are built on FOSS foundations. That's why the stat says

ten out of ten major registry platforms incorporate FOSS components.

Next slide, please. If you look at the resolvers or the query side of DNS, we again find a substantial presence. This is the bit of the report and the research that was actually hardest to get numbers on because the resolver ecosystem is vast and diverse, and there are millions of resolvers that are hard to measure. Here we distinguish local, cloud, and public resolvers. What we did is looked at what's available, what you can buy, and what you can use, and focused the research from that angle.

No matter where you look in the resolver ecosystem, FOSS is present and usually dominant. If you look at, for example, the local space, which is roughly eighty percent of users worldwide, it's predominantly FOSS. There is Bind 9, Unbound, PowerDNS Recursor, Knot Resolver, et cetera. For cloud platforms, we found that at least four of the major hyperscalers also rely on FOSS for their DNS resolving. The others use FOSS libraries as components within proprietary resolvers.

When you look at public resolvers, this is a mix. There are a couple of public resolvers like Quad9 that are using FOSS, but there are also very large ones like Cloudflare that are proprietary but built on FOSS foundations. Finally, there are also fully proprietary ones. The conclusion here again is a substantial presence.

Next slide, please. In summary, FOSS is the foundation across the entire DNS ecosystem. To quote the report, "In the most critical

parts of DNS infrastructure, FOSS is the norm, and proprietary software is the exception." Again, it's not exaggeration or advocacy; it's a rigorous finding from our research.

Next slide. What are the implications of our finding? This brings us to the second part of the report, which is directed at policymakers. The primary motivation for the report was to avoid a collision course between the reality of FOSS and emerging software and critical infrastructure regulation. The conflict is where you have a traditional approach in law or regulation where you require vendors to meet security standards and you impose these on operators of critical infrastructure or their customers. You hold them liable for failure via contracts and you enforce rules through procurement or market access.

Why this fails for FOSS is because FOSS is usually provided for download at a zero cost. There is no supplier relationship in a traditional sense. There is no operator-vendor contract, or there is maybe not even a vendor to regulate, just a volunteer. Traditional supply chain regulation is designed for a customer-vendor model that assumes financial transactions. But software does not have an inherent material cost per copy. You can provide it at near zero cost, and the financial transactions or contracts are not guaranteed to exist.

If you impose compliance burdens on volunteer maintainers, you can cause them to abandon projects, switch to proprietary licenses, or avoid jurisdictions to avoid regulatory risk. The result is

that the software we found everyone to be depending on becomes less available and less secure, which is exactly the opposite of what these software or critical infrastructure regulations are intended to achieve.

Next slide, please. We formulated five actionable guidelines for policymakers. As SSAC, we are indifferent about whether they regulate. But if regulations exist, we would prefer them not to get it wrong. We say acknowledge the critical role of FOSS. Explicitly recognize that critical infrastructure relies on FOSS, and that is a strength to be preserved.

Consult the open source community. Engage maintainers, foundations, and operators in policy development to avoid unintended consequences. We invite them to make use of contemporary cases. The report has a couple of case studies. Regulators can learn from these models that are emerging. There is no need to start from scratch.

We recommend policymakers to incentivize sustainability. Encourage contributions as an investment in public infrastructure, perhaps through grants, tax incentives, procurement policies, et cetera. Systemic risks should be addressed collectively. For example, funding ecosystem-wide solutions for shared dependencies or in tooling, rather than placing burdens on individual maintainers.

Next slide. What can we do? Everyone in this community has a role to play. We went to the GAC and had a presentation and a good

discussion. From the GAC side, they can share our research with their colleagues working on cybersecurity regulation. They can advocate for FOSS consultation during policy development, and they can use the guidelines to review proposed regulation.

The registry and registrar community can support FOSS projects they depend on financially or with development time. They can establish policies and share their operational expertise. The technical community can document its dependencies, contribute back through code, bug reports, or funding, and they can educate others on their operational best practices. The wider community, including you here today, is to recognize FOSS as a critical infrastructure that requires investment and, most importantly, to bridge that gap between the policymaker and technology in this area. As a community, we are uniquely positioned to influence this issue globally. If we speak clearly to the importance of open source, policymakers will listen.

Next slide, please. We covered a lot of ground, from technical details of the DNS to the prevalence of FOSS and actionable guidelines. As we wrap up and move to questions, I want to leave you with the three most important takeaways. The DNS runs on FOSS. The overwhelming majority does. It's a research finding, not an opinion. Policy must start from this fact. FOSS is different, and policies must adapt. The FOSS model has different strengths and risks. Regulation designed for traditional supply chains doesn't fit and can cause harm.

But we can get this right. There are several jurisdictions that are developing FOSS-aware policies. There are emerging models, and we have formulated five actionable guidelines to follow. The final thought I want to leave with you is that the security and stability of our DNS depends on understanding and supporting the FOSS ecosystem that underpins it. Thank you for your attention.

RAFIK DAMMAK

Thanks, Maarten, for this presentation. I think you highlight the most important point: that a lot of work is on top of FOSS and open source, and we need to ensure the sustainability of this ecosystem. From an NCSG standpoint, what we can do is maybe to build more awareness about this work made by SSAC. People know, and we suspect in general when we talk about internet infrastructure, it is the same case, but we can also highlight DNS. We can use that famous joke that if there is a problem, it's usually DNS. It's always DNS.

We can try to distribute and build more awareness. My question is: are there next steps for you? Is there anything else you will elaborate after this, or some areas you will work on in more detail at the SSAC level?

MAARTEN AERTSEN

Thank you. The next steps we took after publishing were trying to get the research in front of a broader audience. Our end goal is for this type of research to be available whenever policy is made. We

got a good response. When we went to the GAC, multiple regions showed an interest. There were follow-up presentations where we were invited to speak specifically to policymakers. For example, in early December, I spoke in a session organized by the European Commission for country member experts that were interested specifically in this issue.

I think that's where there's strength in cooperation with you and with the broader community. As a small group within ICANN, we can't be everywhere policy is being made. But when you live in a country and you know that there is a certain regulation being worked on, that is where an individual can make a difference by sending the research or making an appointment and asking if they considered this angle. We are happy to engage. We don't write these documents to end up in a drawer; we write them to follow up on them. If there is any reach out from your community, we are happy to connect.

RAFIK DAMMAK I believe we can help spread more information about this. Another point, just brainstorming here, you mentioned open source is quite covered, with different models and issues related to maintainer burnout and sustainability. But we are here to talk about DNS and ICANN. Maybe it's not in our scope how to keep that functioning and ensure it, but is there a possibility within the community for some working party to think about possible business models or how we can use ICANN resources or capabilities?

This should include the whole ecosystem of DNS and not just talk about registries. As you mentioned, there are DNS providers, but also everyone, even the hyperscalers for cloud services. We should think about what creates a pool of resources and how we can sustain it. Should we think of a model like a consortium or a foundation, similar to what exists for Python or cloud-native foundations like CNCF or Apache? There is something in that model that we can work with to support and sustain. This community has a strong interest, along with others outside operating DNS who are impacted by it, to come up with something concrete, including governments for funding. Something new can come from us instead of waiting to fix all open source issues. I am just brainstorming on the fly.

MAARTEN AERTSEN

It is very much appreciated. Even before we started this research, members in this community were thinking about this. For example, if you look at the group of people that set the ideas for the ICANN Community Fund, the document they delivered considered open source as an area that would perhaps be valuable to consider grant proposals for. It is not like we start from scratch. There have been individuals in the ICANN community that have had this on their radar for a while.

By discussing research like this, it can be tabled in broader discussions. On Monday, there will be a plenary session about resilience. It is also on the agenda for this session a little bit later.

The FOSS aspect we documented in SAC-132 is a part of that more proactive thinking about resilience instead of responding when something breaks. It is also about business models. I think that's a little bit further from what we do in SSAC. In the end, that is one of the factors that determines whether we'll have the same status quo in ten, twenty, or thirty years, or whether it will change. But this report was primarily about changes in the regulatory environment. In that sense, it was a little bit less about money and more about awareness amongst policymakers.

RAFIK DAMMAK Thank you. I think the merit and intent here is to kickstart discussion and awareness, and we are achieving that. I abused my quality as chair to ask several questions, but let's go with the queue. First Pedro and then Farzaneh.

PEDRO LANA Thanks, Rafik. Thanks, Maarten. First of all, I would like to congratulate the SSAC for the last few publications you are making, SAC-127 on DNS blocking, for example, and now the FOSS open source one.

MAARTEN AERTSEN Can you speak louder?

PEDRO LANA

I will speak closer to the microphone. They are deeply aligned with NCSG concerns, and we have some historical advocates for open source in our community. Even though you mentioned that it's not an advocacy document, it's really useful, especially regarding the narrative that exists nowadays that equals proprietary technology to innovation. My question was actually if there was something that happened recently that led to this concern on publishing this document. Did you notice some kind of worsening traditional regulations regarding software, or was it part of a larger perception that this needed to be pushed so people would care about FOSS and open source again?

MAARTEN AERTSEN

I can answer that. My personal motivation to bring this work to SSAC was based on experiences from my day job. I work at one of these foundations that make open source software based in Amsterdam. In Europe, about three and a half years ago, the European Commission decided to start regulating hardware and software to make product security regulation for digital products.

In their original proposal, you could see that they had considered open source software, but the nuance was not right. As a broader community, the open source community engaged with policymakers, and the law changed substantially. It had to, because if it hadn't, it would not have matched with the reality where most digital products sold today are actually open source inside. The policymakers didn't know this. We talked to quite a lot

of people in the Parliament, the Council, and the Commission, and we got questions like, "Why should we care about this?" The headline of the report is that the DNS is built on open source software. It's titled that way because this was not a fact that was easily documented for a policymaker audience. That was my personal motivation to bring the content. The SSAC found it interesting, and so we started a work party. Thank you for the question. I appreciate it.

RAM MOHAN

Being mindful of time, we'll go with Farzaneh and then move to the next topic. Farzaneh, please go ahead.

FARZANEH BADII

Thank you, Rafik. Hi, everyone. Farzaneh Badii speaking. You might want to think about my question a little before responding, so I don't expect an immediate response. We keep talking in our conversations at ICANN about associated domain checks and mitigating DNS abuse, noting that some registrars don't have the technical feasibility or knowledge to do those things. I think there might be a role for FOSS here that we could explore.

I have to emphasize that as it is open and free software, the processes that happen when they use these tools should also be transparent. For example, when we provide filtering or listings that registrars, registries, and DNS resolvers can use, that can all be done with open source software. But of course, there have to be

mechanisms for transparency. I wonder if there can be a role for FOSS in providing that basic technical capacity for registrars to do some of these mitigations of DNS abuse. Of course, we need to emphasize transparency, due process, and accountability. Thank you.

RAM MOHAN I am not sure where we take that, Farzaneh, in terms of next steps for the SSAC. Do you have some suggestions there?

FARZANEH BADII It just came to my mind because this morning we were having a conversation and some small registrars were saying that for associated domain checks, they don't have the tools. I know that for filtering and things like that, there are some resources outside of ICANN. I was thinking this is a topic we can discuss. It doesn't even have to be discussed at ICANN, but we need to think about how we can help with DNS abuse and mitigation by providing tools and processes that smaller registrars can use to comply with various requirements.

MAARTEN AERTSEN Thanks. Just off the top of my head, that feels a little bit...

RAM MOHAN Further afield from the kinds of things that the SSAC would engage on, because we rarely get involved in the specific operational

pieces of it. We can point to where open source resources might exist, perhaps. But thank you for that input. I see Peter's hand up.

TAIWO PETER AKINREMI: Thanks, Ram, and thanks for sharing this detailed finding with us. My question relates to the methodology that was applied in this study. I see that was not touched on as an academic, so I am always interested in hearing about the methodology that underpins the research. Second, as SSAC, where do you see this research evolving, and what is the next plan? Looking at the fact that the DNS actually runs on open source and we are concerned about the resilience of critical infrastructure, what is the next step in ensuring SSAC makes sure this is further investigated? I typed a lot of questions in the chat, which I don't need to restate on the mic. Thank you.

RAM MOHAN: Yeah.

MAARTEN AERTSEN: Thank you, Peter. With respect to the methodology, the report contains an appendix, Appendix B, that documents for each of the findings what method was used to get to the facts we present. It differs for the various slides that you saw. For example, there is a different way of determining popularity amongst TLDs than for resolvers.

A lot of it was survey-based because you cannot remotely measure reliably what implementations people used. We are actually quite happy with the level of cooperation we got from operators of various services. We focused on larger operators to make sure that we create data that is actually representative of what is big. Please have a look at the appendix and feel free to reach out if you have any questions.

With respect to next steps, currently we are mostly focusing on outreach based on these findings. We have had discussions in the past about repeating this for routing security, but we have not started that work or continued the discussion. I am quite sure you could do something similar on the routing side of the internet pillar technologies to give it a name. I hope that helps with respect to next steps.

RAM MOHAN Thanks, Maarten. In the interest of time, I would like to suggest that we wrap on this topic and move to the next one. Does that work for you, Rafik?

FARZANEH BADII Yes.

RAM MOHAN All right. I just wanted to provide a preview of the plenary session that the SSAC is helping put together on Monday here at this ICANN meeting. The topic of the plenary session is From Stability to

Survivability: ICANN's Role in the Future of Internet Resilience. There are really two reasons why we wanted to bring this up here in our discussion with the NCSG.

The first is that we believe we may well be at an inflection point in terms of where our community and the internet itself is progressing. Looking back in history at how the SSAC itself was founded, some of you may remember the 9/11 attacks that happened in 2001. When that happened, a bunch of us got together and asked what would happen if the internet infrastructure had an impact and who was looking at the security and stability of that. That is what led to the SSAC being formed.

We think we are at a place now where we are moving to an expectation that the internet and the network that so many services depend upon is just available at all times, as a utility. It is not a feature or a luxury; it is a core utility. The other part of it is the realization for everyone watching developments over the last year or so that pieces of the internet or parts of network availability will be disrupted. There is going to be a rupture in the availability of the network. The rupture could happen at a localized, regional, or even larger level. That is the present and likely the future we are marching towards.

Therefore, we believe we have to start thinking about the role of ICANN itself, and stability not just in terms of it staying up, but in terms of when pieces of it go down, can you bounce back? Can you bounce back in a reliable way? Do organizations have clear

frameworks and plans to understand significant disruption and know what to do when it happens? Who do you contact? How do you get back to accessibility, availability, and interoperability? We are at that inflection point, and that was the core cause for helping pull this plenary on moving from stability to survivability.

This is the first piece of it. Our intent at this first plenary session is to provide basic information on the technological pieces behind the internet and its stability, survivability, and resilience. As we continue this conversation, we will go to other parts concerning accessibility and interoperability. I bring this up to the NCSG for two reasons. One, we really want your input and engagement. This topic is important not just for a stable ecosystem but for how individuals operate and interact with each other.

The other part is a realization that if you want to have a cross-community forum on internet resilience, there is no easy way to make that happen unless there is support from various parts of our community acknowledging that internet resilience is a serious strategic topic deserving of discussion and potentially the creation of a cross-community forum. We can initially begin by convening voices and eventually lead to actionable things or usable tools that organizations and individuals can use when there are threats to the accessibility, interoperability, and availability of the internet.

Those are the two primary goals. We invite you to be present at the plenary and engage in the discussions. As we move forward, we expect there will be other public sessions. We would like to do a

future session alongside the NCSG to look at not just the technical aspects but the human aspects of resilience and the disruption to this interoperable network we have all taken for granted. The ask for the Rafik and the team is twofold: one, engage in the plenary, and two, start to think about the NCSG's and ICANN's roles in ensuring survivability when the network we depend upon is disrupted. Back to you, Rafik.

RAFIK DAMMAK Thanks, Ram. First, the NCSG supported having this plenary session because we believe it is an important topic for the community to know more about and to have a forum for discussion. We understand that in the beginning, we need more familiarity with the technical aspects. We are happy to go to the next step or other plenaries to go further into human rights or human aspects, and we are happy to collaborate and provide that perspective. In the end, the whole internet has value because there are users. If there are no users, why would we talk about this technology, even if it is wonderful? We will be happy to participate and work to bring more perspective.

One of the risks we try to explain is the regulatory point. It brings risk when different states try to regulate or come up with a new law or requirement that impacts the operation of the internet. We would be happy to share our point of view and bring expertise from those involved in those issues for some time. I can say we will be

happy to help and participate, and we are looking forward to engaging. The plenary will be on Monday.

RAM MOHAN 10:45 AM.

RAFIK DAMMAK We will be present there and try to engage and share our input. I don't want to monopolize here, so let's see if there is anyone else from the NCSG. We can go with Robert because he is one of our members.

ROBERT GUERRA This is Robert Guerra. I just want to echo what Ram was mentioning and say that we live in very interesting times. Just like 9/11, when there was a reevaluation of the security situation and what different actors need to do, the pace of change is greatly accelerated. Assessing how things are working and adding resiliency and other factors are needed more than ever as the internet and ICANN's role underpin so many things. We need to see standards and planning added. I also want to comment that there has been some discussion about this in the chat as well that you should take a look at. Thanks.

RAM MOHAN Thank you. I am just taking a quick look at the chat. Peter, you are saying you are part of a team working on complex systems,

anonymity, and resilience of critical infrastructure at the University of Cincinnati. That is great to hear. Pedro, you are saying the perspective of access to the internet as an enabler of human rights would fit well into this discussion. I agree with that. In fact, Rafik and I have had fruitful interactions saying this first plenary is to level set and raise awareness. Once we have a common nomenclature and understanding, we can dig deeper into this topic. Thank you for your support; I look forward to collaborating on that. With that, let's go to the next set of topics. Next slide. Rafik, many of these fall more in your area. Why don't we go to the things where you have inputs to provide, and then we can have a discussion?

RAFIK DAMMAK

Thanks, Ram. I think there are at least three topics from our previous discussion that we put as action items, like the safer cyber collaboration, educational progress, and data accuracy. We suggested an interest to collaborate and work with the SSAC on those, particularly the educational program. We said we need to follow up, so if we can agree on next steps, that will help us implement those action items.

Regarding the DNS abuse discussion, since the working group is starting today, we want to work with you and share our point of view. I believe the SSAC is represented in that working group. For the human rights impact assessment, we know you are having all your reports, and the suggestion was how we can help you include

that in the report. We can clarify those two: the human rights impact assessment and the DNS abuse discussion. For the others, we just need to agree on next steps for implementation.

RAM MOHAN

Thanks. Let's go to the first one, the human rights impact assessment. My recollection from our discussion two meetings ago, ICANN 83 in Prague, was that the NCSG would provide a briefing to the SSAC on what a human rights impact assessment framework might look like. That was prompted by a question when we were presenting on DNS blocking. Someone asked if the SSAC looks at the human rights impact of security or stability. We said, "Educate us on this because we are not the experts in this area. Tell us more so we can see if this is meaningful to integrate." We encourage you, if you have a framework or pointers, to talk to us about it. Perhaps at our next meeting, that becomes a presentation from the NCSG to us.

On the DNS abuse discussion, I don't know that we actually got to a constructive endpoint. I recall the SSAC speaking about DNS abuse and DNS blocking. Speaking broadly, the SSAC point of view was that if you are doing blocking, recognize that the cure is often worse than the problem itself because of collateral damage and the ripple effect. At that time, I remember a spirited conversation about the human rights part of it. We ended up saying that we generally stick to the technical aspects and don't comment on policy or human rights components. It doesn't mean we don't want

to be engaged, but it is not our area of expertise where we can speak with authority or put out a recommendation. I don't know where to go forward on the DNS abuse side, but we would like to hear from you on human rights.

RAFIK DAMMAK

Thanks, Ram. To clarify, the last three points were follow-ups on previous discussions. I take your point about the human rights impact assessment. We can work on a briefing. I don't want to use the word educate; it is more like sharing with you and explaining the human rights impact assessment so you can get more familiar with it.

For the DNS abuse discussion, it is not related to what we discussed about DNS blocking. It is for the specific case of the PDP that just started. It is to have a dialogue and a fresh start. We understand your focus, but since you will be present in the working group, we would like to engage with the different parties to hear and work with you and share our perspective.

RAM MOHAN

Thanks for that clarification, Rafik. We are very interested in the PDP on DNS abuse. We have firsthand, deep knowledge about related domain names and the significant abuse that we believe happens and goes unchecked. We think strong efforts have to be taken in the community to address that problem and find a way to stamp it out. The spirit of abuse is being abused by those who go

with just the letter of the law, and it's causing real harm to users all around the world. We have a strong interest in helping move that discussion forward and look forward to collaborating.

On safer cyber, I wanted to share that at this meeting, we are announcing a collaborative effort with the ISPCP. We are doing a year-long series of sessions and webinars on topics related to DNS security and stability. The ISPCP is hosting these; we participated in one last month. The model is that the ISPCP convenes the forum, and we bring the speakers and experts. We have an editorial calendar and an agenda through the end of the year. The forum held in February had over eighty people dialing in from around the world. We had two of our experts speak. One of them, Vasil, is sitting right here in the audience. We are happy to work with you on things applicable to your audience and bring our experts and content to bear on that.

RAFIK DAMMAK

Thanks, Ram. I am happy we can work on those. We are mindful of the time and need to wrap up, but we have a question or comment from Pedro.

PEDRO LANA

Talking about DNS abuse, the NCSG was very interested in the work being developed by the DNS Abuse & AI Work Party. We would like to know the angle you are taking on that and when we can expect the paper to be published.

RAM MOHAN Do we have any work party members here? Jeff is here, Nabil is there, Vasil is there. One of you can speak to the question.

JEFF I cannot say about the exact dates. We are defining our scope, and you can attend one of the work party meetings during this ICANN. We are shrinking our scope because there are a lot of things we would like to explore, and it's a very dynamic system. We will come up with a paper and take part in our working party meeting. Thank you.

NABIL I would just like to add that we started the work party by defining many items related to AI and DNS abuse. We are preparing the first report of a series of reports. Thank you.

ANDREA GLANDON We really need to wrap up, gentlemen. I'm sorry.

RAFIK DAMMAK Thanks, Andrea, for the reminder and keeping us on track. It was a good opportunity to discuss with the SSAC. We have some actions to follow up and work on. Looking forward to the next discussion. We will work on those details with Ram and Nabil, depending on availability. Ram, do you want to add a few words before we close?

RAM MOHAN	Thank you. We really appreciate the opportunity to continue our collaboration and look forward to more. Thank you so much. Back to you.
ANDREA GLANDON	Thank you. Please stop the recording.
TAIWO PETER AKINREMI	Recording stopped.

[END OF TRANSCRIPTION]