ICANN85 Mumbai | CF – Joint Session: ICANN Board and SSAC
Tuesday, March 10, 2026 – 13:30 to 14:30 IST

AARON JIMENEZ

Hello. My name is Aaron Jimenez. I am the participation manager for the session. Welcome to the joint session between the ICANN Board and the Security and Stability Advisory, SSAC. Please note that this session is being recorded and follows the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the Community Participation Code of Conduct concerning Statements of Interest.

Interpretation for the session will include English, French, and Spanish. For our panelists today, we ask that you please state your name for the record and the language you will speak if speaking any language other than English. Please also speak at a reasonable pace.

The discussion today is between the ICANN Board and the SSAC only, therefore we will not be taking questions from the audience. With that, I will now hand the floor over to ICANN Board chair, Tripti Sinha.

TRIPTI SINHA

Thank you, Aaron. Welcome, everyone, to this afternoon's bilateral meeting with the SSAC and the Board. We have lots to discuss. I

don't have much more to say in the opening, so I'll turn it over to Jim Galvin, my colleague, who will facilitate this meeting. Jim?

JIM GALVIN Thank you, Tripti. And welcome, everyone, SSAC members, Board members alike. I think that this is one of my favorite sessions, certainly. I expect and I'm hopeful that we're going to have a really good engagement here today. We have a number of important topics to get through, and hopefully folks will speak.

As I did say in the beginning, I do want to emphasize Board members and SSAC members who are in the audience, even though we don't have room on stage, please do, if you have a contribution that you want to make, please just stand up and come to the front and we have a roving mic that we can arrange, and I'll call on you when opportunity presents. With that, let me hand it over to you, Ram, for some opening remarks and to get us started.

RAM MOHAN Thank you, Jim. I appreciate the opportunity to meet with you, the Board. We always find these sessions interesting, and our focus tends to be on making sure that our time together is spent productively and in an effective manner. We have, really, from the SSAC side, one topic to bring up, and then that actually dovetails into the Board question. And so I think we're going to have plenty to speak about.

I note that we have some SSAC members online as well. So, Kathy, if you just keep track of making sure that when they do want to speak, that we are able to get them going. I appreciate that.

The topic that the SSAC wants to bring up in front of the Board is a focus on Strategic Planning, strategic reliance for the Internet. Internet resilience is no longer a question of whether packets reach their destination. It's a question of whether the system of trust that moves these packets can survive the many storms that are gathering at its borders. So this is not just a technology story, it's a story also about hidden dependencies, power, cloud vendors, global regulations that we rely upon but that we don't control. As we move toward a world that is driven by AI and total connectivity, understanding these vulnerabilities is a difference between a minor inconvenience and a global shutdown.

The SSAC helped organize and run a plenary on this topic yesterday. In the plenary, we really looked at four systemic threats to Internet resilience. We covered quite a lot of ground in that area. Now, one of the things that we did in the plenary was to also have a conversation with the community that was gathered in the room and online and get their sentiment. So I wanted to share with you what we heard from the room, not just what we talked about, but what did the ICANN community gathered? What did they think about this topic of Internet resilience? Next slide, please.

So we asked the question, what will be the largest cause of the next global disruption? And interestingly, there was a significant

response from the community that underfunded preventive measures followed by circular sectoral dependencies, exploring system complexity after that, and then software supply chain risk. So those were of the four things. You get a sense of where the community is thinking about in terms of the largest cause of the next global disruption. Next slide, please.

We then asked a question. This had to do with preparedness. So we said, if your region's primary power grid or cloud provider went entirely dark for three days, how confident are you that your core services would survive? And 36% said they're somewhat confident. 34% said, "We're not confident. We're going to go dark along with them." Only 11% said, "We regularly test 72+ hour islanding and failover." So that was quite telling from everybody who is participating. And you see, 129 people participated in that. Next slide.

We asked, looking at the broader landscape of Internet resilience, what is the ICANN community's most critical blind spot now? The text is intended to test everybody's eyes at the bottom there. But the 38% is cross-sector coordination, for example, communicating with energy, telecom, or finance sectors ranked the highest. The others, the 20% after that is securing underfunded, open-source software supply chains. The 22% was ensuring operational compliance for registries/registrars under extreme global stress. And then the last 20% was understanding the real-world impacts

on end users in emerging economies. So that gives you a sense of what we heard as an outcome from the plenary.

When we asked the community, does ICANN have a role, where we heard back from the community that they believe ICANN does have a role, number one, but also, number two, that maybe there is a gap that does need to be addressed and plugged. So the question then is, where do we start? I want to explore if ICANN has a role in addressing any gaps. Because one of the things that has emerged is that the problem, potentially, is environmental fragility, not protocol fragility. I mean, the DNS BGP still works even under stress. But apps around them, about them, on top of them, etc., that's where a lot of the fragility is coming up. So when applications that depend on DNS and Internet infrastructure fail at scale or across sectors and without warning, the downstream impact ends up being measured in human welfare and economic loss and eroding trust in the Internet itself.

So the thing is, inside of ICANN, no single group, SO/AC organization, etc., has this problem fully in scope. Even the SSAC doesn't have this problem fully in scope. And this is the gap. At this scale, in a system where the Internet is becoming critical infrastructure, it'll either get filled deliberately or it'll get filled badly. That's really where the SSAC's thought process is at this point.

I'm going to pivot just quickly to a few of our SSAC members who have some points of view and some thoughts on this before we get to a Board discussion. So let me start with you, Robert.

ROBERT GUERRA Sure. This is Robert Guerra, SSAC member. I think, to your point, Ram, the issue is whereas in the past exceptions were the exception, now there are much more collateral issues. The power outage in Spain, for example. Other issues that have taken place, the Rogers telecom failure in Canada as well. It will affect providers, it will affect others, and a lot of larger companies involved in ICANN, registries or registrars, may have plans but there's no sharing across. And so identifying the gaps that this is an issue that requires attention, I think, is something that the community and perhaps the Board should be thinking about. And whose role it is, what the scope is, that's something to be determined later, but there is this gap that exists. And ICANN's role of being a coordination, I think, would be most useful.

RAM MOHAN Thank you, Robert. Matthias?

MATTHIAS HUDOBNIK Yes. Matthias Hudobnik speaking for the record. I would like to try to add three points or thoughts we discussed. So the first thing is a bit like when we talked about the framework or playbook, I think the most important thing that we think about what could bring

some added value. So not duplicating some things you already have. And when we even talk more concrete about it, let's say, for example, sharing of information or threats related to security and stability. I mean, there are a lot of things already that's in place, in on operational level, like the Cyber Response Team certs. Also, when, let's say, I'm coming from Europe. So, in Europe you have like the EU cert, you have like Europol, they share a lot of information. And here we could think, is there some gap where we could say we could bring some added value and not simply replicating some playbooks or sharing landscape?

Then also the second thing from a more governance and law perspective, most of these companies, they are critical infrastructure, so they are applicable to some laws, to some standards, ISO, NIST, whatsoever. So they have already some things in place. And here we could think again, is there some framework possibility which is, on the one hand, broader than their scope, but also it should be actionable and meaningful. And this is a bit like the hard thing to do, to find, to balance these kind of things.

And then maybe the third thing is also there would be different ways or formats. So you could say, does it necessarily need to be something written? It could be also some workshop or some information or some awareness campaign or something like that. So that's a bit throwing into the discussion. Thank you.

RAM MOHAN Thanks, Matthias. Danny?

DANNY MCPHERSON Can you hear me okay?

RAM MOHAN Yes.

DANNY MCPHERSON Yeah. I had the opportunity to participate on the panel. I think about this for a bit with Ram and some of the others as we prepare for that. I guess my view is that the various stakeholders, for example, in the root server system, some registry operators spend an inordinate amount of time focusing on the resiliency and robustness of the systems that they operate. Operationally, we've seen multiple terabit level attacks on the root. Within the last year alone, we've seen route hijacks that had active instrumentation of large swaths of the root server system or the root operators within the last year alone. And there was near real-time detection of those and some of the preventative controls and the distributed nature the root helps scope that.

I do think that the cross-sector capabilities of the community—I think all the individual operators do a pretty good job of engaging with their various contracted parties. Not within the ICANN ecosystem, but their carriers, their data center operators, various folks working within their core areas. Many of us participate in government-related incidents. For example, the U.S. government

has something called Cyber Storm. The Information Sharing and Analysis Centers have a number of tabletop exercises and so forth. But I don't think that there's a DNS ecosystem level exercise or contingency planning at that level, and so I think that there may be an opportunity from that perspective for the ICANN Org and the ICANN community to do something unique here.

As we were discussing, it's like, well, what can ICANN do, and what's within the remit? I think various elements of this are already embodied in the Strategic Plan. It's just how do you actualize those and identify anything that we can actually do? So that's kind of one side. And then at the same time, I actually think that something akin to a trends or threats forecast or a strategic outlook that talks about things that could be impactful to the ICANN community or the stakeholders here from geopolitical shifts, emerging technologies, be it quantum, be it AI or agentic AI, various other components, or economic disruptions, other things, supply chain. What are the things that impact the stakeholders within the ICANN community? And what could ICANN do from even their own risk mitigation or risk management perspective to take a take a step back and look at the interdependencies of some of the things that we all rely upon and better inform the stakeholders in the community? I think that's a couple of examples of unique things that ICANN could help better inform folks on.

RAM MOHAN Thanks, Danny. Jeff?

JEFFREY BEDSER

Thanks. Jeff Bedser. I think I'm going to lean in a bit to what Danny's saying, but particularly to the fact that this is not about worrying about what's going to happen in the future, it's what's happening now. There's been a well-documented series of events that were cascading failures of cloud-based infrastructure. One system fails, and there's a cascade of further systems failing down the line. We're looking at the new round, and we're looking at a lot of registries and registrars that are starting out now are building their entire infrastructure cloud-based. So how does that impact us as far as overreliance on single points of failure, when cascading failures are something we're seeing documented time and time again in the media, whereas they affect us.

I actually was on a trip to Toronto, my airline got affected by the CrowdStrike outage, and I ended up taking a bus home for 13 hours because it was the only way to get home. So, real-world impact to these cascading failures and the overreliance on cloud infrastructure within that applying to our industry is a current problem, not a future problem.

RAM MOHAN

Thanks, Jeff. Wes, I'll come to you in just a moment. One of the things that inside the SSAC when we discuss this, we also ask, "Is this in scope, resilience?" When we looked at SSAC's own remit in the Bylaws is to advise ICANN community on matters relating to the security and integrity of the Internet's naming and address

allocation systems. ICANN's core mission in its Bylaws, it says preserving operational stability, reliability, security, and resilience of the DNS and the Internet.

So what you're hearing from us, in kind of a broad sense, is that we see an inflection point. We are moving from stability being looked at as keeping the lights on to stability… We should start to look at stability as recovering from a disruption and being able to recover from it, from that disruption. So we see that there is a gap. We wonder whether you on the Board see the gap that we're describing. And do you see ICANN writ large, as Danny was saying, ICANN the Board, ICANN Org, the community, as having a role in filling it.

Jim, I saw Wes put his hand up, and Tripti has got her hand up as well.

JIM GALVIN Okay. Thank you. Does that complete your introduction?

RAM MOHAN It completes my introduction.

JIM GALVIN Okay. That's great. So now we'll move around and take comments, and I'll manage the queue. So, Wes first, and then Tripti, and then Patricio, and then I see Byron looking for his card. Wes, please.

WES HARDAKER

Thanks, Ram. I did attend the plenary the other day, and it was well put together, so thanks for doing that. It was interesting. And I love the usage of the poll to figure out where the community lay. I will say some of these are hard. Danny did a good job talking about the DNS and mechanisms. We need to think about all the protocols that ICANN is responsible for, both names and numbers.

To a large extent, it's absolutely within ICANN's remit to identify risks. It is, unfortunately, not within ICANN's remit to handle some of those risks, and I think that's where the problem is going to lie. We can identify that an asteroid may hit our building but we can't really protect a building from being hit by an asteroid. And I think that that's the challenge that you're going to face. I think that the notion of the electrical grid being a quintessential point of ICANN's communication framework is well spelled out. However, we can't fix the energy grid so that will be a problem.

I think the other one that was not really covered well during the plenary or discussed here yet today is the tension between centralization, which is problematic technically, versus decentralization, which requires significant more people to understand. And Dan York actually talked a little bit about the need for the human element. But the reality is is that centralization is advantageous economically, and that's where we always come back to get bitten. So as all of the technical communities produce more and more wonderful technologies, it becomes nearly

impossible not to outsource. And I certainly would love to see SSAC consider that along with what is in their remit or not. You have a hard even definition problem ahead of you, I think. And I say you when I also mean me.

JIM GALVIN Thank you, Wes. My takeaway from all of that is, in general, it's important for us to explore understanding this space so that we can begin to think about what's in our remit and what's not, and then what we would do about things that are not in our remit. I hope that that's okay. So two fingers. Go ahead, David.

DAVID MCAULEY Centralization, not just economically, of course, but as a means of control of the system is significant.

JIM GALVIN Okay. Thank you. Patricio, next. Oh, Tripti. I'm sorry.

TRIPTI SINHA Ram, first, thank you very much for the topic. I don't know if there's a question in it per se, but I can wax eloquent on this for hours. This is so broad in scope and very timely, and I think we're trying to scope this to ICANN's remit. But in recent history, I don't think we have entered a phase that is going to be as complex as the next few years will be. I believe everything is so accelerated now because of what's happening with artificial intelligence, because of the

maturity of quantum which is, honestly, as I've been involved in this, a year ago, I said it's about 10 or 15 years away. I don't think so anymore. I think it's closer than that. That's going to be a seismic shift for our ecosystem. So, the threat landscape is so broad, so broad. Look at what's happening with undersea cables and how they are being cut for nefarious reasons. They're being bombed, all kinds of reasons. They're taking out our infrastructure.

So, in terms of our remit—and I'm trying to scope my input on our remit—I think what is on the landscape is agentic AI. We've got to get our arms around it. My fear is we won't. And let me just give you an example. When you look at the early days of the Internet, it started off as a DARPA project, then, of course, came into the National Science Foundation, NSFNET was created, and then the Internet was created, so on and so forth. Typically, those research dollars came oftentimes from the federal government, and I'm talking about the United States right now. Recent numbers say the U.S. spends $1 trillion on R&D, $1 trillion. $300 million of that comes from National Science Foundation, universities and federal government. $700 million comes from the private sector.

In other words, the rate of innovation now is coming from the private sector at a lightning speed that is almost impossible to keep up with. When you look at AI clusters and so forth that are being stood up, and that's where our problem is. The government's input could put $50-$100 million behind this. It's not a drop in the AI bucket. The financial wherewithal lives with the private sector. They can put upwards of a trillion dollars. Look at Nvidia. Nvidia's

market cap now is $3.5 trillion, I believe. Whoever thought that someone would get into that range.

So the point I'm trying to make here is my fear is agentic AI is going to impact the DNS in a very big way, as will quantum. Once Shor's algorithm is able to reapplied and can do useful things for us, we've got a big security issue. So, to scope it to us, I would say, let's focus on agentic AI and, of course, on quantum, which is not too far away. Sorry. It came around to that point in a long-winded way.

JIM GALVIN No, thank you, Tripti. I agree with you that those two topics are significant in part of this, and those are the two topics that we should find a way to investigate and dig into in some way in this ICANN arena. So with that, let me turn to Patricio.

PATRICIO POBLETE Thanks. It should be a little to the point I'm going to make. But this past week, some of the companies owning big data centers in the Gulf found out, to their surprise, that these data centers were targets of war. So that's actually strategic change for an industry that considered that being there was being in a safe place. And the thing is, once that Pandora's box is open, it's very hard to lock down. So, I don't know how relevant it is to us as ICANN but to the whole Internet industry, I think there's something that we have to consider from now on.

JIM GALVIN

I think what I would point out and tie this to is the resiliency discussion yesterday. One of the other things that came out in the panel session was the complexity of the supply chain, the dependencies that we don't know about. It's easy to talk about the energy sector as a significant dependency. Everything is dependent on that. But as you go downstream and things start to fall apart, what do we really know or not know? And in many cases, you don't know until it happens, and I think that's an important part of all of this too. Byron?

BYRON HOLLAND

Thanks. Byron Holland, Board, but day job is as a ccTLD operator for Canada, for .ca. And as such, while not under legislation per se, but generally considered critical infrastructure for the country and a supplier of anycast services to many TLDs around the world, that really informs some of my perspective on it from an operator perspective.

I think there's a great opportunity to focus in this community on DNS resilience in particular. I think it's squarely within the remit of the Strategic Plan that we have all had input into and approved. I'm just going to pick up on the comments that Tripti has made. I think AI and quantum are very real spaces from the operator community that we're worried about, and most operators don't have the sophistication or the talent to really wrestle with what does quantum mean. As we as I think about it, quantum was something, a 10-, 15-year problem. Maybe I won't even have to worry about it,

and that is quickly coming at us much more quickly, I think, than most expected. And how do we wrestle with that? What do we do with that? And is there an opportunity for minds that are focused on it to provide that insight and guidance to those of us who have to operate and may not have that expertise in-house. I think there's something there. Certainly resilience writ large with IANA, that's its own topic, but I think that's an important one too.

In the ccNSO, where Patricio and I spent some time as a community, we've done a lot of work through the TLD Ops Working Group around disaster recovery and business continuity, again, not necessarily what you're speaking about here, but when I see what came out of the plenary yesterday, there's an opportunity this community can help develop processes and elevate the bar for us all. So on the broader topic that you're raising here, I think there's opportunity in this community that's already been proved in certain spaces that can assist in resiliency overall. And again, not necessarily the remit per se of SSAC, but I think there are a number of topics that I've just raised where SSAC would be immensely beneficial to the community and certainly from a selfish perspective, the operator community.

JIM GALVIN Thank you, Byron, for expressing so carefully a real need that we have for information and suggestions for action from there. So we'll have to look more carefully about at all of that afterwards. Raul, please.

RAUL ECHEBERRIA

Thank you, Jim. Raul Echeberria from ICANN Board. First of all, thank you for the session yesterday. It was very interesting. It was fascinating. For sure, this is an important topic, and I think something to keep in mind and probably deserves to bring to the discussion some colleagues that are more focused on those areas of security on different fields.

I have two takeaways from yesterday's discussion for me. So it's not only those two, but is that somebody said that in countries where blackouts are normal or happen, so the infrastructure is prepared to deal with that. The other point is that the problem is when blackouts happen in countries where it is not expected to happen, like it happened in Spain last year. My impression is that Internet was very resilient in Spain during the blackout, and the biggest problem in Spain was the battery of the devices. But while people had battery that they remain connected, most of them. For sure, there are stories that's there.

I think it's an important thing to continue exploring, in having discussions, probably organizing panels like yesterday one. I concede with my colleagues, Tripti, Patricio, Byron, that there are other things that look more challenging in the short term like quantum computing, artificial intelligence. Yesterday, during the RSSAC meeting, somebody said that, for sure, we will see much more sophisticated attacks in the near future. So those things that today we consider that are stable and secure or reasonably secure,

probably that is something that we should not take for granted because the things are evolving very fast. Thank you.

RAM MOHAN Thanks, Raul. SSAC members, any reactions, comments to what you heard, including SSAC members who are on the floor here. Warren?

WARREN KUMARI My concern is there are already a lot of groups who are focusing on this sort of stuff, and much of it feels quite far outside of ICANN's remit and areas of expertise. And I'm concerned that we're not necessarily taking into account all of the existing work, all of the existing organizations that are doing this, and thinking that we are going to be the people to solve problems that other groups are already doing, or at least discuss them. We can note that we have dependencies on other systems, but I think there's a risk that we're going to move out of the ICANN scope and expand things.

JIM GALVIN Tripti, do you want to respond?

TRIPTI SINHA Warren, it sounds like we're putting the weight of the world's shoulder on us in the way it was framed, but I think we're all trying to scope it within our remit. But I think we can't have this conversation without thinking of all the interdependencies. I mean,

like the power grid goes down, well, we're all impacted. If names and numbers doesn't work, the whole world is impacted. So, yes, there's so many interdependencies here. So I think—correct me if I'm wrong—you framed it broadly, but we were trying to scope it to our remit.

WARREN KUMARI: Yeah. There's also all the second order effects, like having gone through a bunch of places where there have been power issues. It's not just power, it's you also need the working road infrastructure because you need trucks to be able to deliver you diesel to get to it, and very quickly turns into a huge project. My concern is that potentially we end up taking focus away from other things that are more urgent and more important.

TRIPTI SINHA: I mean, look, we're talking a lot about power, I think our focus… My fundamental problem with how the AI industry is emerging is that it's like this rush to build another data center. Let's power it with megawatts of power. And I think the power industry needs to look at innovation, at power itself. We should be looking at the semiconductor industry to see photonic chips which are known to use less power. That's where the innovation needs to be. I think we're going about this the wrong way. But anyway, this is again out-of-scope discussion.

WARREN KUMARI That was kind of my point. The power industry needs to look at this.

RAM MOHAN One of the things I wanted to really ask—and this is why we're having this as a discussion—we're not proposing a solution. We're not proposing you must do this or you must not. What we're really saying is this is an important topic, and we see this problem happening at scale. As Jeff was saying, this is a today problem. This is not something hypothetically coming in the future.

In yesterday's plenary, one of the questions and one of the suggestions that was made by several of the commenters was—and you heard Danny say—there are some things perhaps that are usefully doable inside of the ICANN context that are scoped within that remit. And there was a comment that also came up and said, is there a role for ICANN in developing a resilience playbook or a survivability framework that may leverage pre-existing resources, but still is something that we say, you know that… So those are questions that we have.

Maarten, you have a comment from the floor.

MAARTEN AERTSEN Thank you, Ram. This is Maarten Aertsen for the record, also a member of SSAC. If people want to discuss this topic of resilience but maybe not tie it too much to the power grid or to AI, I say another topic in this realm is the topic of open-source software.

And we have published a report, SAC132 last year. It was covered in the plenary.

And I think there's some work in that sense, because even if you look at the responses of the panelists, Paul Vixie had a pretty different view than the gentleman from auDA, even though both are very knowledgeable on the subject. So just saying we don't need necessarily to just talk about power and still advance a conversation on resilience.

JIM GALVIN Thank you, Maarten. Let me turn to Suzanne.

SUZANNE WOOLF Thanks, Jim. I'm Suzanne Woolf and a member of SSAC. When trying to scope an issue like this, one of the ways to approach it is, all right, what is it that needs to be done that only ICANN can do as opposed to what other players in the ecosystem can do? And one thing that ICANN could be looking at—ICANN is uniquely responsible for IANA, and maybe that's a place to start. Where are these larger scale issues possibly going to impact the ability to maintain stewardship of the IANA functions? Because that's the core and that's unique to ICANN. Nobody else can do that.

JIM GALVIN Thank you for that very specific suggestion in all this and that. And I think you're right. I agree with you, and that's important.

The one thing I want to put out there, and maybe just to confirm here, Ram, with you is I had always seen this, the plenary session from yesterday, as SSAC encouraging the community. You asked the community for whether or not to have this plenary, and all of that was accepted, and it happened. The idea here was to raise awareness and encourage the community to be interested and willing to do all of that. And I think the takeaways from the meeting are that there is community interest in understanding this problem space. And then I think part of the discussion that we're having here is what does that really turn into in terms of an action? I think there's still space for understanding the problem, so we do have to do that.

Then I agree with Warren, who is pushing back on we can't do everything, but we do need to examine enough of the space, to understand what's in our remit, and then begin to think about what we can do within the space that belongs to us.

Suzanne had an excellent suggestion there in the end. I'm sure there are other things if we take the time to understand the space.

And so we'll go to John.

JOHN LEVINE

John Levine, SSAC. Listening to this, I've been thinking that something we need to pay attention to is sequencing, and some things are considerably more urgent than others. I mean, for example, we keep hearing about quantum. These days, anybody

who says you need to do quantum right now is trying to sell you something. I can go into more detail, but I can say ICANN needs to deal with quantum at some point but not instantly. There are organizations that have things that need to stay secret for 30 years, but we are not one of them. Our secrets are typically measured in months, and we can roll stuff in that timeframe. On the other hand, Maarten's comment about open-source software, we've been seeing open source failures right now. I think there might be concrete things we could do, for example, to the extent that open-source software is bad because people can't afford to fix it. I hear we have some money, there's some possibilities there.

I think there are other problems so we can identify. And even though I totally agree that we need to keep stuff in scope, and that mission creep is a bad idea, and that we need to resist the urge that people look to ICANN to fix the world's computer problems, but within a narrow thing and keeping an idea that there's things we can work on right now, I think there's some useful work to be done, simultaneously saying there's useful work to say this is important but not now. So we're going to work on A now and B later.

JIM GALVIN Thank you, John. Yeah, I think that's exactly the point that I'm getting to here too. And you're saying things consistent with what Warren was saying. A lot of concern about trying to do too much, but we should figure out what we can do and take the time to do that and look at what this problem space really looks like.

I am not seeing any other hands or questions from anyone. Ram, do you want to give some closing comments here?

RAM MOHAN

Thanks. One of the things that did come up in several conversations was—and again, I don't know if this is workable, but it's something for us to think about, and for you on the Board to consider separately—one of the concepts that came up yesterday was the potential for some kind of—and I don't know how to do this—but some kind of a cross-community, cross-sectoral forum on Internet resilience. But again, that was an idea, and these things have to get scoped out.

So I leave that, really, as a topic of joint work between the Board and the SSAC. We're going to continue to think about what, if anything, could/should be done in the area of Internet resilience inside of the ICANN community, but we'd exhort you to do the same and to have a serious conversation and contemplation about that. Because there are problems happening right now. Again, it's not that ICANN is the place to solve these problems, but maybe there is a place to map these problems and to understand what the problem sets are, because we're hearing that even mapping it is not properly understood.

So let me go to the topic two then, Jim, because it's a good lead up. If you could please go to the next slide. We had a question on emerging trends in a potential FY26-30 Strategic Plan updates, and you're asking, what's the top emerging trend that may impact

ICANN that you think the Board should consider? There are two topics that we'd like to bring to your attention. One, of course, is what we just talked about, the widening systemic resilience gap. We think that's really important.

You have an Annual Strategy Review Program. And in your strategic objective 4 which says, "Strengthen the stability and security of the Internet's unique identifier system," you link to it, but we think that the resilience is implicit in that document or in that plan, and we suggest that you make it explicit. So you include the term resilience in there and add a new strategic goal 4.3 that is related to strategic cross-sectoral resilience. So that's a specific piece of feedback on that.

The second thing that we want to bring in front of you is the namespace is evolving and the pace of that evolution is accelerating. So we think technology evolutions begin as separate and distinct from ICANN's remit, then seek to integrate or intersect with the DNS resolution space. I mean, this is not a new story. We saw this for more than a decade. New technologies emerged, blockchain identifiers, and then there's an intent of how do you integrate that with this space?

So we want to make sure. And we've written about some of this. We wrote about dotless domains back in the day. Then we talked about users of the shared global domain namespace, stability of the domain namespace, use of emoji in domain names, evolution of DNS resolution. So we've been paying attention to this topic, but

we think that the emerging trend of AI agents, as these agents evolve towards becoming autonomous and have agent-to-agent operations at scale, we anticipate an increasing reliance on the DNS as the underlying infrastructure for identification, for discovery, and for secure communications.

So, in that area, it's not that we have a specific recommendation, because you have in your strategic objective 3, you have a mandate for proactive screening of technologies that are coming up. But we think that when you do the Annual Strategy Review process, namespace evolution and its implications on the single global Internet should be part of the scope of what gets assessed. And you should also update the Strategic Plan to reflect the urgency and the pace at which these trends are emerging. It's entirely possible that an annual review is too slow because of the pace at which these changes are happening. So those are two specific pieces of feedback for you.

JIM GALVIN I want to thank you, Ram, and thank SSAC for the resiliency session yesterday, and resiliency discussion here that we had today, and your particular suggestions for this. I can say that the Board had its own Strategic Annual Review discussion during this workshop this past weekend. I think that these topics and the discussion we had today will certainly make some interesting opportunities to expand the Board discussion. Give us something else, some additional information to think about.

I think, most importantly, we should look forward to additional dialogues between SSAC and the Board, additional opportunities to talk to each other about where we are, what we're doing, what we could do. I think you've certainly brought to us a lot of important and significant ideas and suggestions, and I don't want to lose them. So I look forward to further dialogue on these points.

Would anyone else from the Board or any the SSAC member want to add anything overall? Our timing is actually pretty good here. Okay. You have another topic can I get to?

RAM MOHAN

Yeah. What I said about the two inputs on the Strategic Plan, Jim has a copy of that and he'll pass it in to the right places for that. But resilience is important. Please provide some focus on it.

Your Board Question 2 on the next slide was on Review of Reviews. I won't read the questions that are on the screen, but I want to turn to our SSAC colleagues who are knowledgeable on this topic to provide their perspective. Robert?

ROBERT GUERRA

Sure. I'm Robert Guerra again, and I'm here with Suzanne Woolf, and both of us are the SSAC members of the Review of Reviews for the Board. What we'll let you know is that we've been informing the SSAC because the process has been going forward. We provided a considerable update on one of our monthly meetings. And yesterday we had a very comprehensive one-hour meeting with the

SSAC that are here, giving them the update on the latest proposed plan by the Review of Reviews. We explained the different kind of components as well, talked about our views on the progress and some of the different challenges.

What I will share with you now is kind of some high-level thoughts, and I'll give Suzanne an opportunity as well to comment, is that we think that the instinct behind the new framework is right. The old system was not working, necessarily, properly. Reviews ran, as everyone knows, well overtime, overbudget, and produced a series of recommendations that sometimes just got parked and never really got looked at. And it's right that the Board started the process to revisit this.

The proposed structure is a meaningful simplification. We hope the SSAC did have some comments and I hope the community is providing comments here as well. I think the session is later this week. We are close to a workable proposal. There has been progress. We have some additional thoughts. But the timeline is very ambitious, and so likely the pace of the Review of Reviews will accelerate as we go forward.

One of the issues that we talked about that is mentioned in the Review of Reviews is the Continuous Improvement Program, and one of the issues that we identified is that if different SO/ACs will have to go through this, then it's really important that there be some way to compare or have some sort of framework so they can be compared, because if each SO/AC has a different process, you

can't compare them, and then we'll be stuck in the same problem, not really being able to track issues going forward.

If I missed anything, Suzanne, please.

SUZANNE WOOLF

No. There were a couple of other comments we wanted to share. There's a large number of changes, actually, as far as the new framework. And one of the things that it does do is shift away from independent, external reviewers. There was a real problem where external reviewers often lack the context to make useful, coherent recommendations that would work within our community. But if you're only evaluating yourself, you will always be doing a great job. So there need to be safeguards around the self-evaluation processes.

Two other things that came out in the discussion we've had with SSAC. People were concerned about conflicts of interest and whether something needed to be more specified about that since the other function, the other reason for having independent reviewers, was exactly to remove vested interest from performance assessment. So any community-conducted review process needs explicit conflict of interest provisions or we're just recreating the credibility problems we already had.

The other thing that SSAC raised, as you might expect, there's provision in the draft framework for adding experts to review teams, but they did want to talk specifically about how to assure

that appropriate technical expertise was brought into the process, as appropriate, were needed. I think we would be happy to work on some guidelines or guardrails for that.

The other question that's come up that SSAC will need to discuss, or at least consider, SSAC decided not to be part of the decisional Empowered Community, and depending on what decision mechanisms the Review of Reviews CCG comes up with to propose, SSAC might have to revisit that decision. So far, SSAC wants to remain in a strictly advisory capacity, but if it needs to be reconsidered, we'll do that and proceed from there.

JIM GALVIN Thank you, Robert and Suzanne. Let me just first say as the one of the two Board members to the Review of Reviews group, along with Leon Sanchez who's out here in the audience, first and foremost, on behalf of the Board, thank you for your detailed and deep engagement, and keeping SSAC engaged, and working with the Membership to get a position and have all those discussions. As you well know, being part of the group, the Board in particular is very interested in community engagement, and it is really important to all of this.

I know that I stay in close alignment and agreement with you two, and that's working out very well. And I think it's a good thing what you're doing within SSAC and for the reviews and for the

community at large, making sure that everyone gets an opportunity to have a voice.

I don't want to comment specifically on the issues that you bring up, those are open questions. I agree with those questions, of course, and they are topics of conversation in the Review Cross-Community Working Group. So I just want to thank you again and encourage you to continue these discussions inside of SSAC, to get some positions on some of these topics as they develop and they come about. So thank you very much.

Any comments from anyone else on SSAC's answer to the review question? I'm not seeing anything. Okay. I believe that is the end of your agenda, correct?

RAM MOHAN

That is the end of our agenda. We intentionally kept our scope of our conversation with you quite tight because we didn't want to give you the usual "Here is a status update on all the work that we're doing." But we are doing a lot of work, and it's going quite well, I think. But we really want to continue the conversation with you in some appropriate way to continue that conversation on resilience and to actually see is there something to be done? And if so, how to go about doing it? So how to keep that properly scoped. But we believe there is work to be done. We see there's a gap, at least, that exists. So that's one thing.

And the other is, I think, from the Board's perspective on the Strategic Plan Review, the evolution of the namespace is an urgent issue, and something that needs quite a bit more work. We're happy to engage with you offline to dig deeper into that. But thank you for your time and attention on all of this.

JIM GALVIN Thank you, Ram. I very much appreciate that. Thank you to all SSAC for being here. I think with that—oh, did you want to comment? I was about to hand it to you to close it out and final comment. Thank you.

TRIPTI SINHA To close it out? We're having a protocol issue here. Okay, no problems. You're done.

I just wanted to say in response to what you said, Ram. The Board did have a in-depth discussion on agentic AI and post quantum cryptography. You said, "What should our focus be on?" I would say focus on that.

And just one more comment, which I shared with you, but I'd like everyone else here to think about it as well, is the threat landscape when it comes to agentic AI has changed quite a bit now because of LLMs. So you're creating threats that now learn how to be better threats. You've got systems that are teaching them how to get better. So if the SSAC could whenever, during your copious free

time, look at agentic AI, PQC, and the threats that come in with that environment. Thank you.

RAM MOHAN Thanks, Tripti. We have a work party that is just starting up on AI and abuse, and we're still in the process of figuring out scope. But we don't have something started up on the post quantum piece yet.

TRIPTI SINHA Thank you very much for this conversation. It was a great discussion. Broad in scope, but I think we just narrowed it down to what's within our control and remit. Thank you, everyone. This meeting is adjourned.

[END OF TRANSCRIPTION]