RECORDED VOICE: This meeting is now being recorded.

[CROSSTALK]

UNKNOWN SPEAKER: Hello. If anyone is on the phone, we're going to take another few minutes to get together and then we'll start.

[CROSSTALK]

DENISE MICHEL: So, it's five past eight here. I think we'll get started with some housekeeping before we dive in. Welcome everyone to the security review team meeting. This is Denise Michel, one of the co-chairs of the team. I have some housekeeping items I've been asked to clear up before we start.

This meeting is being recorded. Before anyone speaks, please give your name for the record. We have, I believe, two review team members who are joining us remotely. Is there anyone on the bridge yet?

Okay. We'll monitor that. We also have observers, both in the room and potentially in Adobe Connect. And we'll keep an eye on the chatroom, if remote participants and our observers have contributions for the meeting.

The next slide… Who is driving the slide deck? Has our agenda. If you could move forward one to the standards of behavior.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

And another one.

And another one. It's in there.

Okay.

Technical difficulties. There are standards of behavior in there somewhere. We'll show them as soon as we find them. Meanwhile, let's go around the room and have everyone introduce themselves. Into the mic, please, for our remote participants. Steve, would you like to kick us off?

STEVE CONTE: Certainly. Good morning. Steve Conte, office of the CTO program sector.

KAVEH RANJBAR: Kaveh Ranjbar, Board delegation SSR 2.

NEGAR FARZINNIA: Negar Farzinnia, MSSI, senior manager.

ZARKO KECIC: Zarko Kecic, dot RS. Tech manage.

CATHY HANDLEY: Cathy Handley, ARIN.

EMILY TAYLOR: Emily Taylor, co-chair.

PATRICK JONES: Patrick Jones, ICANN Global Stakeholder Engagement.

ALAIN PATRICK AINA: Alain Aina, [inaudible] SSR 2.

NOORUL AMEEN: Noorul Ameen, [inaudible] India.

JOHN CRAIN: John Crain, ICANN’s chief SSR officer.

ERIC OSTERWEIL: Eric Osterweil, [inaudible].

DENISE MICHEL: Denise Michel, co-chair.

DAVID CONRAD: David Conrad, ICANN CTO.

ALICE JANSEN: Alice Jansen, ICANN MSSI.

JENNIFER BRYCE: Jennifer Bryce, ICANN MSSI.

BERNARD TURCOTTE: Bernard Turcotte, ICANN MSSI.

KERRY-ANN BARRETT: Kerry-Ann Barrett.

UNKNOWN SPEAKER: [Inaudible].

UNKNOWN SPEAKER: [Inaudible].

DAVID PISCITELLO: David Piscitello, ICANN.

MARGIE MILAM: Margie Milam, ICANN MSSI.

KAREN MULBERRY: Karen Mulberry, MSSI.

DENISE MICHEL: Would the observers like to introduce themselves as well?

[SPEAKER OFF MICROPHONE]

GEORGE SADOWSKY: George Sadowsky, ICANN Board.

RINALIA ABDUL RAHIM: Rinalia Abdul Rahim, ICANN Board.

DENISE MICHEL: Thank you, and welcome everyone. And thank you, especially, for joining us early in the morning. So, yes, I don't think we found the standards of behavior, but yes. But please treat each other with respect, and if you would like the details of that, it's somewhere in this voluminous slide deck.

So, the agenda is also in the slide deck. We'll run through it really quickly so people can get their bearings of what we'll be covering today. We have, of course, our usual statements of interest and roll call. First up, we'll have a brief presentation and general discussion about the [inaudible] landscape, as well as follow-up discussion and questions from the DNS Symposium.

It was a jam-packed, substantive day. I know I have follow-up questions, and I imagine that many of you have as well. So, the first hour is set aside for a broad discussion as well as follow-up questions and discussion with the ICANN staff here. 10 to 12:30, we have a deep dive into the first security review team recommendations and their implementation.

We have a break scheduled for 10:30. Lunch scheduled for 12:30. After lunch, we'll be reflecting on the SSR 1, the security review team implementation briefings, and discussing how we want to tackle our assessment of the implementation and the impact of those recommendations.

Next, and these times are estimated, perhaps hopeful. We'll try and keep the agenda somewhat fluid to accommodate the interests and needs of the team as they progress through this. Next on the schedule, we have the, we have a follow-up discussion on two data driven efforts that ICANN is undertaking, the identifier technology health indicators, referred to as ITHI, and the DNS abuse reporting project, referred to as DART.

After the break, we have time set aside to address additional issues that arise throughout the day, make sure we recap our action items, and review tomorrow's agenda, making adjustments we feel are necessary, before ending around five o'clock. Any questions, comments, suggested edit to that agenda?

Jennifer has sent a link to the slide deck, so you have it on your computer as well as on the Adobe Connect room. Are there any statements of interest updates? James?

JAMES GANNON: So, I just have to do a… Because I didn't get to do this at the first meeting. So, you will see on my SOI, I work for [inaudible]. We're a pharmaceutical company. They do not support me at ICANN. I come here on my own private time. They do not support me in any direct or indirect manner. Any statements I make here are as myself and not on behalf of the company. And also, for the record, I do not work on anything to do with [inaudible] pharmaceuticals or anything like that, but I will excuse myself from any discussions or decisions made around that [inaudible], just because there are conflicts of interest.

DENISE MICHEL: Thank you, James. Any other updates or additions to the statements of interest for team members? Seeing none, we'll move on. Do our esteemed co-chairs have any additional comments or opening remarks they would like to share before we dive in?

EMILY TAYLOR: Just, we're a little bit ahead of the agenda, and there was this sort of section for opening remarks. So, it may be possible to have team members give us a sense of whether you'd like to be by the end of tomorrow in our work. What we would have liked to achieved? And what would get us, sending ourselves on our way with a really good feeling by the end of tomorrow?

DENISE MICHEL: Thank you, Emily. Great suggestion. All right. I'll take volunteers. Our aspirations for what we consider success at the end of two days. We have James and then Cathy.

[SPEAKER OFF MICROPHONE]

CATHY HANDLEY: As far as the end of this, I think it's imperative that we have a work plan, and everything set up. Because I think right now, we're, I think, to me, we're running behind. There is a lot of work that needs to be done. James has done a great start on it, but we need to leave here with some actual direction to do actual work.

DENISE MICHEL: Thank you, Cathy. And we have some agreement around the table. Off to a good start. James.

JAMES GANNON: James Gannon. So, this is why I let Cathy go first, because I think I was going to say the same thing. Yeah, I would like to come out at the end of this with some formal way to start working on substantial issues. We have a very limited timeline ahead of us, and we have a hell of a lot of work to do. So, I would like to come out of this with, okay, what are our topics that we are going to be looking at as the review team?

You know, we've got [inaudible] all of our scope, discussion groups, we've gotten now to a point where I think we need to start working on substance. You know, we'll still be doing admin in parallel with that, but we need to start working on substance, and I like it to start after this meeting.

DENISE MICHEL: Thank you, James. And others? Emily?

EMILY TAYLOR: My personal wish for this meeting is that everybody in the team will play their part, and take the mic, even those that we don't hear from, especially those we don't hear from very often. I really hope that you will feel confident and share your opinions with the rest of the team.

There are a few people who are not backwards about coming forward, but please, everybody is welcome. Everybody's opinion is equally valid. I really encourage everybody to express themselves on the issues.

DENISE MICHEL: Thank you, Emily. Alain?

ALAIN PATRICK AINA: Yes, just to equal what Cathy and [inaudible] said, and add one suggestion. The suggestion is from everything we do, meeting face to face or everything, when we have topics, they may be good that we have topics. For example, after we have listened to this, or after we have done this, what should be the outcome. That we all have a common idea of what we should expect from a session, a presentation.

DENISE MICHEL: Other contributions?

Well, as we proceed today, please give this some more thought. We'll be coming back to it periodically through our sessions, and certainly at the end of today's session. All right. We'll move on to our first agenda item then. That's a presentation, if you will, but certainly a discussion about the threat landscape that ICANN is facing now and expect to face in the future. Followed by a time for team members to ask follow-up questions and have a more extended discussion about some of the issues that were raised in yesterday's DNS Symposium.

Following up on Alain's suggestion, the co-chairs put this on the agenda at the start, to provide a broader set of information about the general environment in which the ICANN SSR related staff and programs are operating, and to fact this into our workplan specifically, and how this might influence the topics we choose to tackle in our work.

That's the [threat?] landscape part, and the DNS Symposium part is the very ambitious and very packed agenda. I know I have follow-up questions on much of the material that was covered, that is very relevant to our work, so I wanted to make sure that we set aside time for our team members to ask follow-up questions and to have a more extended discussion with staff.

With that, I'll turn it over to the staff. I'm not quite sure who is going to kick off our…

UNKNOWN SPEAKER: David, I think you're going to lead?

DAVID CONRAD: Yup. I will attempt to do so.

DENISE MICHEL: And please remember everyone, to introduce yourselves for our remote participants especially. Thanks.

DAVID CONRAD: I'm David Conrad, ICANN CTO. So, I guess we received a request to talk about threat landscape, I guess a week and a half ago, something like that, or I saw it. And things have been a little bit busy with the ICANN DNS Symposium, so I don't really have any prepared slides to speak, you know, directly to the various aspects, but I thought I would do is take a look at the ICANN mission statement, and use that as sort of a way of describing some of the threats that we're seeing in the various areas that ICANN has some responsibility for, at least according to our mission.

And the mission statements, I'm sure many of you have gotten quite tired of actually reading it by this point, says that ICANN does a lot of stuff, but ensures the stable and secure operation of the internet's unique identifier systems, as described in a series of bullet points.

And those bullet points include coordinating the allocation and assignment of names in the root zone, coordinate the development and implementation of policies concerning the registration of second-level domain names that is constrained. Facilitates coordination, operation, evolution of DNS root name server system.

Coordinate the allocation and assignment of the top most level of internet protocol numbers and autonomous system numbers. Collaborates with other bodies, as appropriate, to [inaudible] registries needed for the functioning of the internet, as specified by the IP standards development organizations.

So, with that in mind, looking at the… Ensuring the secure and stable operation of the internet's unique identifier system, the threats that were seen in the context of coordination of allocation assignment of names in the root zone, include a lot of the stuff that many of you are quite familiar with, including the DNS abuse. David Piscitello can talk a bit about the platform that we have developed, known as DART, for Domain name Abuse Reporting Tools.

We, in the context of names as well, there is the security and stability of the root zone in the context of the new gTLD program, how it has added additional names into the root zone, and we'll continue to stretch the DNS infrastructure in ways that was not originally anticipated at the root level.

There is also, in the context of the root servers, as many of you know, right now we're seeing a plague of denial of service attacks. The DYN attack, as I understand it, was about 635 megabytes per second. I'm sorry, gigabytes per second. Megabytes would have been nice.

The last attack that I believe made the press about attacks against the root, I believe was November 2015. That attack, if I remember correctly, was 35 gigabytes per second. So, in order of magnitude, less, and that attack against the root had an impact that was noticeable, at least to monitoring system, in which I believe 11 of the 13 root servers were rendered, if not non-responsive, did not respond to all of the queries that was aimed at them.

The remaining two, which I believe were… Actually, I guess, remaining three, A, J, and L, could easily withstand the additional load, so no one on the internet who didn't have a monitoring system noticed the attack, but the fact that the attacks seem to be growing at a rate that is not easily matched by the ability of root server operator and other infrastructure providers to match, is an area of some concern.

In the context of IP addresses and other numbering systems, the role of ICANN is quite limited. We… I'm not sure what the right word would be, facilitate global policy development associated with global policies for numbering systems, and the IANA functions allocate blocks to the regional internet registries.

There are, with the exhaustion of IPv4, sort of a sea change that's occurring within the addressing world. ICANN's role in that is advisory, at best, because we don't specifically have a direct personal role in the numbering systems, but it is an area that is likely to affect the security, the stable and secure operation of the internet's unique identifier systems.

So, that is an area that we, at least, attempt to work with the regional internet registries to provide data and analysis. With regards to the threat landscapes associated with protocol development, it's not so much a threat landscape, as sort of an evolution in the way the internet is growing. The IETF continues to develop standards that introduce new protocols and new systems, into the internet.

Each one of those provides new opportunities for development, and occasionally, new opportunities for attacks. In addition, as the internet is growing and becoming more a core portion of national infrastructures, there are new players in the standards world. Many of you might have heard of 5G, that's one of the newer technologies that my team is investigating, not so much for threats, as for the, just the evolution of the way things are going on the internet.

Let's see, what other things can I say? The…

DENISE MICHEL: Excuse me. Just before you… This is Denise Michel. Before you move on, could you explain 5G a little bit more?

DAVID CONRAD: Sure. 5G is the 501 from, perhaps surprisingly, 4GLTE, it's a higher bandwidth technology used in mobile networks. There have been suggestions that 5G is a core requirement for deployment of internet of things, but that seems to be, that seems to be a core requirement… Internet of things seems to be a core requirement for almost any protocol these days.

It is currently under development, and there are trials being deployed in various places. I believe the current timeframe is estimated to be 2020 for the deployment of the first production of IG networks, but there will be 4G plus and 4G plus plus, and that sort of thing, as we migrate into 5G.

How will that impact the internet? There are some who believe that the internet architecture will evolve to make use of 5G as the underlining infrastructure, to basically creating clouds of 5G that interconnect clouds of internet related technologies, whether that turns out to be the case is unclear.

The threat complications of 5G are simply a mobile network that has tens to hundreds of gigabytes of capacity, so that your cell phone can turn into next [inaudible] service generator.

DENISE MICHEL: Thank you, David. Emily.

EMILY TAYLOR: Apart from mentioning the DIN attack and the DDOS, did I get it right? That 11 out of the 13 were not able, of the root servers, in the [inaudible] attack were not able to respond to all of the queries aimed at them? What was the follow-up afterwards? Has there been any learning from that? Has there been any work from those root server operators to increase capacity to withstand those DDOS attacks?

DAVID CONRAD: Well, I can't speak for all of the root servers at ICANN since we were on one of the root servers. We did augment our deployments increase, and with capacities and number of [inaudible] deployed a bunch of new nodes. ICANN has now 150 instances of the L root in various places. My understanding is that other root server operators have equally and improve the capacity of their nodes, and how they may be able to speak a bit better to let a K root server, maybe Eric could speak to it, I and J did.

But there is, I think, a general acknowledgement now within the root server system that things need to evolve, that the internet has grown. The RSSAC root service system advisory committee has been working quite diligently on evolving some of the structures within the root server system, and this was an ongoing area of investigation.

EMILY TAYLOR: Could I just as a quick follow-up? Certainly existing in the landscape, DDOS is just, my perception is that it's becoming just this persistent bane, really, of [inaudible] reflected attacks. I just wondered whether there was work within ICANN, or within the community, to see whether anything can be done to [inaudible] doing a DDOS less easy? Or is it something that we all just have to accept?

DAVID CONRAD: So, denial of services, it has become a fairly persistent threat through the internet infrastructure. And the reasons for that threat are sort of endemic. The security systems that the internet evolved have not really been effective in dealing with this kind of an attack. The… I forgot the botnet that did DYN. [Inaudible], thank you. Wow. Too early in the morning. [Inaudible] botnet, leveraged devices that had default passwords and, I'm sorry.

Yeah. [Inaudible] credentials. And allowed for a tremendous amount of bandwidth to be thrown around very easily. The, in the context of the root server system, there have been some proposals, for example, RFC 7706, to allow for, that facilitates the mirroring of the root zone into a more distributed resolvers, which would reduce the threat that a denial of service would be able to take out the root of the DNS, but that doesn't protect, obviously, the ccTLDs or sort of the next level down. There has been a number of discussions about how to have sort of an emergency bandwidth mechanism in case an attack is occurring that the large scale bandwidth providers could step-up and provide additional bandwidth to help mitigate the attacks.

There are a number of services out there that allow for denial of service mitigation, and all of those are being investigated as ways of dealing with specific points, vulnerabilities. But the issue has become more, DDOS has become sort of endemic and there is no really easy way of addressing it.

DENISE MICHEL: Thank you. John? Oh, I'm sorry. We've got David Piscitello and then John Crain.

DAVID PISCITELLO: I wanted to follow-up on what David is talking about, and Emily, you're right that DDOS is very serious. [Inaudible] it's actually a commodity at this point. You can get DDOS as a service from dark net marketplaces. And somebody will just simply, you know, use [inaudible] cloud or some other, you know, very, very powerful platform. And focus in a tax where as long as you pay for it.

The systematic problems that we know, you know, cause the greatest amount of [inaudible] or address spoofing and open resolvers. And we have been talking, as a community, from either SSAC or individual platforms like my own or Paul [inaudible], about these for approximately 13 years. The adoption rate of the solutions is commensurate with the adoption rate of IPv6.

Unfortunately, people are unwilling to put in filters and unwilling to correct their operations, because they don't see that it is their problem, and until we manage to get the edge of the network to stop making it simple for these attacks, there is very little that we can do, because we're basically the punching bag. We're not, we're not responsible for the weapon, we are responsible for deflecting the weapon.

DENISE MICHEL: Thank you, Dave. I have John and then Eric. Others?

JOHN CRAIN: So, the interesting thing about many of these threats, you'll see the threat landscape is extremely broad, but in the context of ICANN, our ability to leverage things and actually affect solutions is actually fairly limited, right? You know, when you look at some of the threats that were brought up, I don't think it was a review. It was another process, they brought up a series of risks, and you look at them, the way I tend to look at these are, as a staff member, as an organization, there are things we can actually do.

We talk about root servers and capacity, now obviously we manage one. So, that's something we can do. We can expand our root. We can investigate technological solutions and management solutions around that. There are things that we can influence almost directly through the policy processes, not us, but ICANN the organization, the community, and contracts. And then the majority of things, actually you have very little direct influence on.

And there, what we spend a lot of our time on is being subject matter experts and helping people, because obviously, we take DDOS as an example, there is a direct threat to the identifier system. I know many TLD end resolver operators will lose sleep over this. But we don't run their systems, we can't tell them how to run their systems, but we can advise and we talk to ISPs and that's, and we can educate.

So, when you look at this large threat landscape, I would ask you to think about, you know, what is actually ICANN's role here? Because we cannot fix the world. I would argue it's not our job. There are things, what we tend to do is, we look at things that are going to affect… Our mindset, we're looking at the negative aspects, but we also look at opportunity, the identifier system.

And DDOS is a really good example when we look at one of the threats, well there are things we can actually do, you know, in our day to day jobs, and then there is a lot of influencing and discussion that we end up having. So, I just want people to realize that although this is in our threat landscape, it's not necessarily something that we can always directly affect, believe me, people like David and myself, and David are always out there saying, BCP 38.

Everybody please just clean up your networks, but ICANN doesn't run the internet, right? We all know that. Right? We all know that in this room, but a lot of people don't.

DENISE MICHEL: Thank you, John. And a good reminder that ICANN has a very specific mission, and although we sprung this topic on the staff, the threat landscape discussion, just last week, and we appreciate you coming and having this discussion with us. The intention here is not, is specifically not to simply focus on the specific activities and role of ICANN staff, but to make sure that security team members have a broad perspective of the threat landscape in which ICANN is doing its specific role.

Thank you very much for that, John. We have Eric next and then Zarko, Noorul, and Kerry-Ann.

Okay, thank you. Noorul, please.

NOORUL AMEEN: So, I'm from [inaudible], India. So, based on the incidents we handled last two, three years, the [inaudible] didn't start with the [inaudible]. It start with the [inaudible] abuse, maybe. [Inaudible] protocol abuse and large data volume traffic, was there is… So, my suggestion is that if you see the chain of DDOS events, protocols getting abused like [NTP?], DNS, or FSTP, and that result or attacks, targeted [inaudible] themselves.

So, it's a global issue. So, as I was telling, the root problem of [inaudible] and [inaudible] IOT devices or web cams that are exposed in the internet. [Inaudible], so the possibility is able to [patent?] the system, or you have to prevent it an attack from the [inaudible] side. So, as far as [inaudible] is concerned, most of the people, ISPs, and they are not other security issues, they are simply [inaudible] type for the [inaudible]. [Inaudible] but most of them are not [inaudible].

So, this is a global issue. I think for editing this, SSR one recommended a DNS cert, computer emergency response team, specifically for DNS operations. So, I just want to know the status for DNS operations, or [inaudible] is performing the functions of DNS SEC.

JOHN CRAIN: Can I talk to this?

DENISE MICHEL: John, please od.

JOHN CRAIN: I will show you the stab wounds and the flailing that staff got when that recommendation was suggested. I think, and I think that's for the review team to look at and decide whether that is a bad idea, or a good idea, or a bad idea. But it was an extreme type of process for staff when [CROSSTALK]…

No, no, not from that. But truly from a political perspective where it was, yeah. Not universally wished for.

DENISE MICHEL: We'll let that topic [inaudible] jump in on this question and then go back to the queue. Other people, certainly feel free to jump in on this if you want to follow-up on this as well. Go ahead, Patrick.

PATRICK JONES: Patrick Jones. Just to clarify this. A concept was not a recommendation of SSR one. This was a proposal that was published under two previous COs ago. And it was put out for community comment discussion, and after substantial community input, the concept was not advanced any further. So, it wasn't something that was part of the first review.

DENISE MICHEL: Thank you, this is Denise. Clive [inaudible] was the CEO under which the idea of an IDN DNS [inaudible] was floated. Norrul, did you have additional comments on this?

[SPEAKER OFF MICROPHONE]

Right, of course, okay. [CROSSTALK]

UNKNOWN SPEAKER: …we have people online, and please use the microphone when you're talking.

DENISE MICHEL: Okay, thank you. And I would note on that, personally I'm curious as to whether the opposition that arose in the community was technical, or political, or perhaps a combination of both. How much of that was influenced by perhaps a distrust of the CEO? And how much was based on a disagreement that DNS search supported by ICANN was needed, warranted, and appropriate within its mission.

DAVID PISCITELLO: This is Dave Piscitello. It actually was a combination. The initial pushback was the perception that ICANN was going to take a much more profound operational role, and the perceptions of what we had intended, did not really come out correctly in the report that was generated. And it seemed like ICANN was going to build this gigantic network operations center across the millions of community dollars.

Unfortunately, I think it's accurate to say that the then CEO took this a little bit personally, and pushed back very hard, and so there was… It devolved into something that became very fractious very quickly. And I think it is unfortunately because it was intended to be more of a distributed effort and a coordination effort, and we never got past the initial fractious behavior to actually sit down and rethink how this might be something that we could actually do well.

DENISE MICHEL: Thank you, Dave. Other comments on this specifically? We have additional questions and other people in the queue. Yes, please.

UNKNOWN SPEAKER: Okay, if I also remember well, the DNS SEC, I also think from the first DNS Symposium we had, 2009 or something, we had two DNS Symposiums before, but it was a difference. So, my question is, the new DNS Symposium is called ICANN, and seems to be ICANN specific model. So, is this going to be like that? Or, we will go back to the previous DNS Symposium, where I think we can still bring the DNS SEC things back, because the community DNS SEC Symposium, I think, allow this kind of discussion.

DAVID PISCITELLO: This is David. So, there were two or three, three DNS SSR Symposiums. Four, and one for five. And you know, I know the ones in Kyoto and in Atlanta, but they were well-received, and focuses specifically on SSR related matters. They did, if I recall correctly, trigger the discussions that led to the DNS proposal that sort of crashed and burned. But the current ICANN DNS Symposium is intended to be sort of more broad and less focused on specific SSR.

We had some very, Matt and I had some very preliminary discussions about, you know, sort of, if this one went reasonably well, what we would want to do for the next one. And the thought of increasing, you know, the amount of time, the topics involving more community as opposed to focus specifically on ICANN's DNS efforts.

You know, are probably areas that we're going to look at more deeply. And as, I think, Matt mentioned yesterday, for those who weren't there, that we are very much interested in community input to help us identify the appropriate path for that meeting. My intent, when I sort of came up with this idea, is that it would be really nice, now that we have a policy forum that focuses on policy stuff, and the GDD summit which focuses on business stuff, that you know, maybe we'd have something that would focus on technical stuff, and that was sort of the genesis of the meeting.

So, it wasn't actually a follow-on from the original SSR Symposium, but including SSR in the future is something we will probably do if it does continue.

DENISE MICHEL: Thank you, David. We'll go back to the queue. We have Eric, Zarko, Kerry-Ann, James, Alan, and then we also have Matogoro with a question in the Adobe Connect. I'll read it now, so staff and team members can be thinking about it. It's not an easy one. And then we'll address this after James on the queue.

The question is, "What are the major four threat landscape that ICANN has experienced for the past two years?" So, that's the question that you want, and we've got Eric in the queue.

ERIC OSTERWEIL: Eric Osterweil. So, we kind of touched a nerve and we've also opened a big kettle of fish. And to think, we're very quickly going to start to talk about what's within scope and what's not, but you know, with regard to DDOS. But I think it's really worth talking about, so I'm glad we're kind of touching on it for however long we do.

Yeah, the DDOS are kind of growing out of control. And we see a lot where we sit, and we see a lot where we don't talk about. We see [inaudible]. We see weapons coming online where they are clearly just being tested. And we see them get used. And we see things that are enormous in scale.

We see, you know, TTPs that are way different from attack to attack. You know, we see different types of botnets, not just [inaudible], some bigger ones later than that, as well. And I think we sort of, we dance around sort of like a finger point game in the DDOS world, and I think that's kind of understandable.

It's unfair, but it's fair at the same time. When a lot of these… When the biggest attacks come from source address spoofing, whether they're NTP or DNS or SMTP, or anything else, the problem is, it's easy to lie, but where you're coming from on the internet, problem with remediation, PCP 38, or PCP 84, is that it's actually technically not possible to deploy these filters in large networks because you don't know who is behind who.

You don't know what customer [inaudible] are, you can't know it. You think, you can know who your adjacencies are, but you can't know who their transiting traffic for, because that changes, and it can be done, you know, for perfectly good reasons, and they give [inaudible].

So, it's not possible to build a filter today because we don't have the tooling necessary to say, "I can discover who is rightfully behind due to source traffic." It's very, very difficult. I could maybe kind of discover who is there to receive traffic, maybe, but even then, that's different than sourcing traffic. So, there is a big problem with [inaudible] and discovering itself.

[Inaudible] telling us all the way back to where we are in the SSRT 2. You know, we could potentially talk about that problem, maybe, if we duck tailed it into an identifier problem, and what we thought maybe we could say about that, I'm not sure. But you know, if we wanted to try and like, you know, ground this conversation, it's a good conversation that happens all over the place.

And I think raising awareness because I think people are starting to understand, source address spoofing, that sounds bad. And honestly, my two cents on that is it's a routing problem. It really is. So, DDOS, like reflective application attacks in the DNS, that's a routing problem. If you fix it with a DNS solution, I'll do NCP. I'll go find some other stateless PDP protocol.

The problem is, I can lie about where I came from, and you can't tell where that is. And so, there are lots of works, some of which people can talk about, some of which people can't talk about, to try and remediate this, but we could potentially see if there is something within the identifier space that we can say something about. If I have an identifier, and I'm allowed to source traffic for it, and you're not allowed to source traffic for my identifier, is there something to say about that?

Maybe, I don't know. So, that's as much as I wanted to say, because I don't really know what the right answer is, but I want to try and sort of like say a couple of things that are important.

DENISE MICHEL: Thank you, Eric. Zarko, you're up next, and then Kerry-Ann.

ZARKO KECIC: Yeah, this is Zarko. I just wanted to comment little what Eric just said. PCP [inaudible] is not recommendation for internet background. It's for internet [inaudible], and if we have spoofing source in the middle of internet, we are in big trouble. So, [inaudible] routers should implement PCP 38, and we are all set. And I wanted to ask David [inaudible] answer, just little bit. And I have question.

How much ICANN can influence root operators? Because my question is, can you ask root operators to have filtering capabilities, like [inaudible] capabilities to certain stand, to fight [inaudible]?

UNKNOWN SPEAKER: So, ICANN is one of the root operators. We obviously have control over what we do, constrained by the need to provide root service as sort of generally defined. ICANN has no mechanism to control what the root server operators do, in general. We can make suggestions, and actually, I should be a little clearer here, at the ICANN organization facilitates the discussion and the contacts of RSSAC.

Where we provide support for RSSAC, and the real influencer is actually RSSAC and SSAC caucus. They, you know, I believe SSAC has made suggestions that have then gone back into RSSAC, which then makes recommendations, suggestions, to the root server operators. The RSSAC caucus works with the RSSAC as sort of core to come up with proposals and recommendations.

The ICANN organization itself doesn't really have any direct influence outside of facilitating this discussions, and the fact that we're one of the root server operators and we can sort of go in and say, hey, here is an idea, let's try this. And see how that works. We have, in the past, attempted to lead by example, publishing, statistics and other things like that.

And yeah, the other root server operators have done similar things, either in response or with… I'll let John speak further.

JOHN CRAIN: Yes. I think David's [inaudible], and it really is the caucus of the RSSAC, where most of the discussion really does and should take place. I'm actually a member of the RSSAC, I wear way too many hats. Core committee. But most of the work happens in two areas. Operational work is what the operators call the, the action operators and those guys [inaudible] ops, but things like for influence and not really policy, but maybe guidelines and things, that one comes out of our RSSAC.

Most of the operators, and I could [inaudible] do some form of lamenting, especially when it comes down to reflection of tax, where the operator actually becomes part of the issue if they're not careful, but that's not standardized, per se. And it's certainly not an ICANN staff thing.

So, you know, there is a question of how, as RSSAC we can be more effective in those discussions, and Kaveh is actually the RSSAC liaison to the Board, so he's a really good person to talk to about that.

DENISE MICHEL: Kaveh, do you have anything you would like to add before we continue with the queue?

KAVEH RANJBAR: Yes. I'm a bit confused, to be honest, because I understand the issue, but [inaudible] have different faces and make it more complex, because this [inaudible] example. The people that will strongly argue that root operators should do any kind of limitation because we also, we have the mandate from the RFC to answer everything in the query.

So, if it starts dropping some queries, which some others [inaudible] acceptable [inaudible], which help with [inaudible], but it will also reduce, in some definitions, the quality of root service. So, these things get very complex. And actually, this was my bigger question for the group, how involve do we want this group, people sitting here, to be in these issues?

Because some of these things are very technical, and [inaudible] at some point, they get most philosophical and how you look at stuff, and much more important round of that. And maybe it's a question for the chairs, how we want to go through with this thing? Do we want to take positions like that? Like [inaudible]… example, face the issue. Because if it's able to [inaudible] because of [inaudible], for example, this might never come into scope.

Then the other viewpoint, we should [inaudible], that would be [inaudible] you will have this issue. In my opinion, this kind of review teams are sufficiently like [inaudible] technical, it should be more like strategic thinkers. And you will have to figure out who will do the actual work, getting to the dirty details, and we just [inaudible] and say, okay, we've got these issues. We need a report from how root servers are involved in facts in which commission research, or whatever, and the results of that, we try to strategically define that and figure out the issues and the [inaudible] recommendations. That was my [inaudible].

If you want to get different issues, there is a lot to discuss. But I don't think any number of meetings would be enough to go through all of them.

DENISE MICHEL: Thank you, Kaveh. And thank you for raising the larger issues of the team's role. We'll just note that it's not the co-chairs job to answer that question specifically, or dictate what the team's role is, but rather there is time on the agenda for the team members to collaborate and discuss and come to a decision on what our role is, and how we want to proceed on which issues.

KAVEH RANJBAR: Just to clarify, I wanted the chairs to please take us there.

DENISE MICHEL: Thank you, well noted. Unless there is a specific follow-up on this topic, I'm going to return to the queue, but I want to give people the chance… Alain.

ALAIN PATRICK AINA: I think Kaveh, but I think, I would focus the issues to understand the role, the RSSAC and SSAC, put into the context of ICANN happen to deal with the threat landscape, which is going into the [inaudible] I think what we should be focusing on. What exactly is the role of the SSAC in the ICANN contest?

But I'm adding extra to RSSAC here, because we need to, maybe is to understand the role of the RSSA and SSAC have been ICANN to manage the threat landscape.

DENISE MICHEL: Thank you, Alain. Did you have a follow-up on this?

ZARKO KECIC: Yes, I wanted to clarify what was my question. It is not to [inaudible]. And also, I didn't think to define, actually to limit answer to the queries from root servers. I wanted to defend root servers from DDOS attack, so it is better to limit some queries, and to not be able to answer any of them. And my question was, to what extent should we look at this issue, and should we put some recommendation to ICANN, to develop policies for root operators?

DENISE MICHEL: Thank you, Zarko. I think David Conrad also wanted to respond to Alain's question, and then just to take a quick, make sure I haven't missed anyone in the queue, we've got Kerry-Ann, James, we have Matogoro's question, Karen has her flag up as does Dave Piscitello. Did I miss anyone in the queue?

And you're still in the queue, Alain, okay.

We'll put that in the queue as well. We've got David Conrad. And then is this a follow-up question, Alain, or do you want me to…? Okay. All right, I'll put you in the queue. David.

DAVID CONRAD: Just a quick response regarding SSAC and RSSAC's role. I just might simply recommend the SSR 2 review team asked for presentations from the chairs of RSSAC and SSAC, perhaps in Johannesburg, if they'll be meeting there. That work can be done. It may be better even be done remotely, I'm sure this could be of help.

DENISE MICHEL: All right. Returning to the queue then, we've got Kerry-Ann.

KERRY-ANN BARRETT: The discussion kind of end up [inaudible] then I had planned it to be originally. I think I wanted to start where Kaveh left off, and the response that Zarko gave. And then I'm going to what my real question was after.

[Laughter]

My real question was a bit different, but then this came before. I think one that, I think… Kerry-Ann speaking. And I think, for me, I was trying to explain it to James beside me, because we're a little bit in disagreement at first. As a policy development person, one of the things that I've done throughout my life is when I have an [inaudible] to address, I go from the root all the way up, because when I get a recommendation, it has to take into consideration everything.

Yesterday, just [inaudible] I said no, but when I have to develop stuff, I speak to all of the technical persons, understand it from the bottom up, and then I can give what you call sensible recommendations. So, [inaudible], Kaveh I disagree with you a little bit. Sometimes the discussions do seem to go into the technical [inaudible] of stuff, but I think as a review team, if we don't understand those nuances, we'll end up giving botched recommendations.

I think the review team, in my perspective, and my team members disagree, my sincerest apologies, but I think as a part of this team, my function will be, I like to understand, because unless I understand, I cannot give sensible recommendations. And as a result, I know, I think the compliment of all of the members that the team explored, because we have someone from [inaudible] in terms of he understands some of the technical issues.

You have you, we have all, then we have persons like me, who are more policy driven, who can actually pull together some of those new instances and then give a decent recommendation as possible, if that is the hope. So, I wanted to just put on the table that, there will be times, I think, that I will need that kind of technical background, because we keep getting [inaudible], what is the role of ICANN?

How far can ICANN expand? I think all of us have been involved in this. I know that ICANN cannot do certain things. But at the end of the day, I think being able to give good recommendations, I think the internet is facing. You described it. [Inaudible] coming up, [inaudible] and unless we give sensible recommendations now to prepare for the future, then I think our role makes no sense then. There is no reason to be here.

With that said, I wanted to put a question to ICANN staff. Given these threats that you have seen, and it goes to [inaudible] question as well. Given that you are seeing, can we then narrow it down to targets? Targets and then pull it out to direct influence in the influence that ICANN can have? Given that ICANN, and I always try to bring the team back to ensure that the differences in the language that each section, the first one says to ensure a stable and secure.

The other says, coordinate, influence, very soft language. The first a, which then, the rest, and I want to give a legal interpretation, only because that's my background. A states the tone to ensure. When you get to the sub-clauses, one, two, three, that is a follow-up to A. So it's not separate from A. Cannot be read outside of A. So, starting off with A, the role of the ways you can do it, is put coordinate, to facilitate, to coordinate, to collaborate.

So, given the context that it's more soft [inaudible], that you have to use to ensure, is there anyway based on the research that we see that the [inaudible] group does and the other research that you have, is there any way for us to identify threats, targets, the targets are the root service operators, fine. We need to then separate direct targets [inaudible], direct targets for training our responsibilities for [inaudible], and then see what we can do directly and indirectly. Is that possible?

It may not be for this team, but is it possible that we can recommend as a way forward in terms of managing this new function or this new role?

DENISE MICHEL: David.

DAVID CONRAD: So, one of the challenges that, you know, particularly when we're looking at the security, stability, resiliency of the identifier system as a whole is that, the threat landscape has become very diffused. There are a myriad of threats, a myriad of targets, basically, in many cases it's whatever the bad guys think they can make money off of, or whatever the bad guys think they can leverage to drive whatever agenda they might have.

In ICANN's context, because we have very limited mechanisms by which to address, to actually implement the mission that we have, we tend to focus on the areas that we do have explicit controls. Things like contractual obligations that we can put in place upon the registries and registrars, infrastructure that we help support including the root servers, but also the registries that are provided through the IANA functions.

Those are the… And since we have control over those, then we identify the targets that are associated with that, and then are able to work on defenses and mitigations associated with those threats. The more general threats, things like abuse, and denouncers, and those sorts of things, we can make recommendations and observations and provide input, but ultimately, we don't have the control to be able to identify anything outside our own remit in terms of targets to be able to do anything about.

KERRY-ANN BARRETT: Let me clarify the question and [inaudible]. Do we have the capacity to identify critical assets? The things that will cause the internet to become instable and insecure? And having identified those critical assets, because we have the threat landscape, and I agree with you, like it's huge. You can't really mitigate everything. You can't be running behind every single root server operator to help them fix themselves.

But we have the threat landscape, the core things that will let the internet… Well, can we identify that? And then the other peripheral stuff, in terms of giving recommendations for policy development, and training, and capacity of all of the root server operators, etc. [Inaudible] remit and direct control of…

Are we able to actually do that kind of [inaudible]? I think that's my direct question, not what you are able to influence, but do we have the capacity to do that map? That's probably the more direct question.

DAVID CONRAD: My team is, you know, relatively small, and there are a large number of avenues in which we could pursue through the various threats. So, what we've tended to do is focus on the things that we think we have some control over. So, could we do it, potentially? Yeah, with community assistance that are working with other entities that are operable in this space, the certs and the first in the world, and those sorts of things.

But historically, we had tended to focus on the things that we felt that we would be able to control directly.

DENISE MICHEL: Kerry-Ann, are you…? Was there an immediate follow-up on this topic? Please, go and make sure everyone…

UNKNOWN SPEAKER: [Inaudible]. There isn't [inaudible]… …information security. [Inaudible]… which focused on critical infrastructure, yeah, and focused on a top, I think, 10, 15 issues. And give [inaudible] of how to, from each perspective, from the registrar, registries perspective, how you can mitigate the risks.

And I can send the link to the document, and I think they're real good. And give you a good idea of how to start with the [inaudible].

DENISE MICHEL: Thank you. Anyone else on this topic? We can always come back to any of these topics. Well, proceed down the queue, we have James next. And then addressing Matogoro's questions and comments. Followed by Dave Piscitello and then Alain.

JAMES GANNON: It's James Gannon. So, this is actually a follow-up that was intended earlier. I'm channeling John here, because he actually took the thought out of my head. For David, John, and probably Dave as well, what keeps you up at night? What should we be thinking about? You know, what's the one thing that is really lodged in your head, we really need to think about this.

UNKNOWN SPEAKER: Looks like Dave has a list.

DENISE MICHEL: In what order shall we take staff's sleeplessness? All right, we've got James, and then Dave, and then David.

UNKNOWN SPEAKER: So, I didn't sleep last night, well not much. You know, there are new threats, or there is a new actuality that's in the press at the moment.

[SPEAKER OFF MICROPHONE]

And this makes me cry, or want to cry. And when things like that happen, there is always a question of, how does this affect the system? Is this something that we're involved? Is this something that we're going to be, as an industry, not ICANN, but as an industry, are we going to be expected to be part of the solution of?

And given the lack of a DNS cert, how are we going to do that? So, you know, we, as staff get dragged into those discussions on the international level with governments and oversight industry. But that was last night, and I think Dave Piscitello over there has a long list. He never sleeps.

DAVID PISCITELLO: How many days do you have? So, one of the things that I would encourage everyone here to do, if you have not already done so is, read the paper that staff generated called the identifier systems attack mitigation methodology and framework. This was published as part of the staff response to SSR one.

It identifies 10 threats. I can tell you that some of these threats have been around for longer than I've been at ICANN, which is 12 years now. And we are not making very much progress. So perhaps, as a way to kind of bring us back to thinking about things that, at least, over the past several years, we perceived as being within ICANN's remit, at least at some respect.

Let me begin with DNS exploited packs. This is a different kind of denial of service, but it one that we actually could perhaps assist with. An exploited pack is basically when an attacker uses a software flaw or bug, in the DNS server software, to render the machine inoperable. And so, it's actually more effective than a denial of service attack because the software stops running and you get no answers.

We'd actually implemented what's called a coordinated vulnerability disclosure process at ICANN, where we will mediate between a reporter of a bug, and the vendor or the open source administrator of that software. It has been successful. We've used this for at least the

Microsoft collisions, name collisions bug, the [JAS] bug. We've used this for two other minor bugs in Bind.

So, that is something that we are doing. And if you're interested, I'll send an email to Denise with some links to some of these things, and also some links to some background articles that I've written over years that explain to some of these attacks. I do have some articles on DDOS. We've already talked about root insertion. There is a whole…

I actually did a classification of 12 different kinds of ways that traffic can be inserted by either hijacking or squatting, or impersonating ASNs, this [inaudible] numbers or IP addresses. Or by simply hijacking the registration, using an expired domain name that was the mail address domain name.

So, if you're interested in understanding all of that, I have that taxonomy written down. But that is, I think that is going to be, continued to be a threat at several levels, especially because IPv4 addresses have enormous black market value. If you can hold of a classy address, you can make a lot of money on the dark web.

Attacks against web services, social media, all of the attacks that are used for pay per click, for redirection, and for redirection especially to malware hosting sites, are becoming really, really enormous pain points. Within our remit, one of the things that we have to pay more attention to is that people will hijack the registration accounts of brands in particular.

So, they will go through a registrar, I'm not singling them out, but they'll go there. They'll either socially engineer the staff, or they'll use some kind of means of acquiring or breeching an email address that's associated with the count, they'll take it over. They can take over the name service. They can use that for defacement. They can use that for a number of different methods. I think that there were some things that could be encouraged in policy, for example, using federated identities for registration accounts that would probably be the kinds of recommendations that we might be able to have the community consider.

There are still attacks, or there is still concerns about parallel roots, where, you know, someone essentially decides that they're not, especially if we are not satisfying everyone's need for a new TLD. And that is, yeah, that is something that we do have to pay attention to. I don't know how much control ICANN can exercise over that, but I think the consequences of that have to be made clear.

There are also things that affect everyone who is using the DNS, especially the surveillance aspects. There is going to be a lot of discussion and controversy in the next several years over whether or not DNS information is private information, whether we should be using encryption on our DNS queries. There are protocols coming out of the IETF previous.

That's going to be a very, very challenging issue because actually monitoring DNS traffic is one of the major ways that we find criminal activity. And so, I think that's going to be a huge political issue that is going to resonate through the ICANN community. And [inaudible] the use DNS as a covert channel is become quite a bit more popular, and this is where you either use a DNS query to convey information to somebody who is running an impersonation server, or you use a server to download malware onto a machine instead of an HTTP or some other protocol. So, those are the ones that make me afraid at night because they're the infrastructure manifestations of most of the attacks.

And of course, we could go into botnets which is really John [inaudible].

DENISE MICHEL: Thank you, Dave. John?

JOHN CRAIN: It might be useful to actually, to answer the question about the four big threats, because that answers some of that, and we had a little chat internally. So, which [inaudible], David, I don't know if you…

DAVID CONRAD: Background chat. The ones that I sort of identified were sort of DDOS, name collusion as a sort of generic concept, the abuse of registration, and you know, to show that it is not always the bad guys that cause the threats. We have the rollover of the root zones DNS SEC key that does occasionally, could potentially cause a sort of a bad day on the internet.

John does have a different view.

JOHN CRAIN: I always agree with you. I think [CROSSTALK]… No, you know, I think those are the [inaudible]… When you look at the abuse of registration, that has many different aspects. One of the issues that I think, and there are people here from registries and registrars, we may be facing going forward is ensuring that the policies and the processes that ICANN has in place facilitates tackling some of these things. For example, botnets domain generation algorithms, DGAs require a lot of work by the registries and the registrars, and every time a new one comes up, there is a lot of different questions about, is this written in policy?

Is this something we should be doing as an industry? I absolutely do not plan to have the answers to all of these questions. But they, you know, there is a policy aspect of the work we do. And a lot of what we do influences policy. And one of the [inaudible] that we have is the policy. So, you know, there is a lot of different areas of how the registration is abused, and that's one, as Dave said, botnets keep me awake at night because I get dragged into all of the discussions, but I worry about the policy implications of some of these activities that are going on.

DENISE MICHEL: Thank you, John. Steve, your nightmares.

STEVE CONTE: [Inaudible] talk a little about the, although the bad guy scenario where people are attacking the network and all of that is classy and exciting, it's [inaudible] put up that next video and it makes the TV in some form of reality. The [inaudible] is a great example, or something like that, where every day technology is evolving. And I ask the review team here to consider the ramifications of the boring everyday evolution of the internet too.

And that has a potential of equal, if not greater, impact if we fail to look at that within ICANN's limited scope and remit.

DENISE MICHEL: Thank you, Steve. Emily, do you have a question?

EMILY TAYLOR: Yeah. Could you elaborate of what you have in mind when you talk about the evolution of the internet?

STEVE CONTE: I'm sorry…

EMILY TAYLOR: Would you mind elaborating a bit when you, what you have in mind when you're talking about the boring everyday evolution of the internet? Was it just a general…?

STEVE CONTE: It's mostly a general, it's mostly taking the bad guy scenario out of the picture. So we have, you know, as of two days ago, one [inaudible] and you know, the ransomware attack. We've got [inaudible], we've got all of these attacks that are large enough to float and make national or international [inaudible], and those are the juicy bits and the ones that people really want to look at.

But there is impact on just the general evolution of the internet. Over the last couple of years, we've had the… [Inaudible] the terminology of IOT coming up, and I say arguably, because I think in some respect, IOT has been around for longer than the terminology of it has, because just other devices in the network.

So, as we [inaudible] of more things being, yeah, more things utilizing the network, be it people, be it devices, be it whatever, it's not being the [inaudible] of you know, of… In network news, fires are always the best thing because it's visually pleasing and everyone wants to watch the fire. And so, as we look at the non-fires, or that's one thing to consider are the things that are just sheer evolutionary that are happening on the internet, and does it have an impact within ICANN's scope?

DENISE MICHEL: Thank you, Steve. This has generated a number of follow-up comments. I've got a new queue [CROSSTALK] which is very productive, which is… I've got a new queue just on this topic with Patrick, James, John, and David. Anyone else? And Emily. All right, Patrick.

PATRICK JONES: All right. I'll build from Steve's comment and actually point to later in the day when Dave talks about the DNS abuse protocol, or DNS abuse project. So, that work is going to provide a lot of understanding of the present day situation in the marketplace of what is happening with registries and registrars, and providing more data about the current situation with abuse in the marketplace, would provide a lot more clarity and understanding of what's happening where.

And should provide some direction to a purchase that compliance and others in the space can take. So, suggest to the review team to look at that.

DENISE MICHEL: Thank you, Patrick. And I would just like to insert before turning it over to James that, and that connects to John's reminder that the ICANN community has a policy making function that can also address these things. But I would note that the domain abuse DART report is nowhere near being available to the public, and the very community in ICANN that is actually charged with creating the policies that potentially could help with this abuse.

So that's the conundrum I would like to tackle during that discussion as well. Moving on to James and then John.

JAMES GANNON: James Gannon. Let me tell you a quick story of why boring is important. So, yesterday we had the [inaudible] ransomware which went around the world, and knocked out hospitals in the UK and everything else, and it was stopped by a researcher, [inaudible] researcher, who registered a domain.

In the little flurry of emails that I was involved in yesterday when he registered that domain, because do you know something really important? The WHOIS information in this is bad. It is registered to [inaudible] dot tech, as the domain registrant, and everything else is pretty much empty or nonsense on this.

The actual string also looks like a generated malware domain, because they used it in different sandboxes [inaudible]. So, there is boring things to do as well. So, when a security researcher finds something like this, how do they make sure that it doesn't get taken down for having inaccurate WHOIS, which is a flipside of a policy that some would say is a good thing and is stopping bad actors on the internet?

So, there is boring things to be looked at as well. There is following the trail of well, what are the implications? [Inaudible] there are implications of well, within the coordination process that ICANN does do, I think you do [inaudible] and everything else, is there something that we can improve on there? For example, to make sure that when a researcher goes off and registers this domain, that number one, they know how to register it correctly, they know how to do it in a way that protects themselves, because they don't want some shadowy group coming after them, because [inaudible] there, you know, potentially very lucrative ransomware.

Impact [inaudible] generated $30,000 as a result of that takedown. There is boring things for us to look at as well in regards to, not the big flashy things that are on the news, but the things that are going on in the background. How do we improve coordination? How do we improve communications within the communities that are involved in using the identifiers for good and bad? You know, how do we make sure those processes are in place?

So, there is more and more for us to do as well. It won't all be [inaudible], and if we focus on a group that starts with cyber, then we'll be going down the wrong road.

DENISE MICHEL: Thank you, James. Before I turn it over to John, I would like to ask the ICANN staff here, if they've contacted ICANN compliance to make sure that they don't enforce on a bad WHOIS record. [Inaudible] off the internet. John.

JOHN CRAIN: So interestingly, we do have some processes that deal with those kind of problems, specifically with registries, and we're missing processes in other places, possibly for registrars. Around when can they break their contracts or break policies, because sometimes they have to for the public good.

And I can't remember if it's ES, RS or ER, [inaudible], yeah. So, there is… For example, when doing a DGA takedowns, sometimes registries want to act as a registrar, but the contract may not allow them to, and this really in the past was the case. And we have the ability to waive clauses within the contracts for specific cases. Sometimes they actually want to put incorrect information into the WHOIS, which is a policy breach, but it could be for safety reasons of the people involved, or it could be to [inaudible] information to the bad guys.

So, you know, what is ICANN's role there? Is ICANN's role to get out of the way? Is ICANN's role to facilitate? I don't know the answer, but there are questions there. Going back to boring and evolution, we've had a number of protocol that have required change over the years, either due to lack of security, actual security issues, or just depletion.

IP version four, autonomous system numbers, whether the actual protocol definitions cause issues, because nobody was meant to be using our internet, and we've got everybody on it. And those are pretty boring, but we need to keep an eye on those. So, one of the things we may [inaudible] SSR and in research is to keep an eye on those evolution protocols, what's happening in the ICANN, etc.

Now, we shouldn't lose, I believe, so I know how important it is to be ahead of the curve of these things. We don't want to be caught out by something, just by doing a little bit of research into how protocols and developing, could have prevented this. And obviously preventing various services and transport layers as well, different layers. Probably across all of the layers.

But, you know, it is important elements is to keep looking at how things have changing, so that we can look for both risk and opportunity though.

DENISE MICHEL: Thank you, John. I have David and then Emily, Kerry-Ann.

JOHN CRAIN: So, one of the fundamental dichromacies that exist within ICANN, is this… ICANN's mission is, states explicitly, that the organization, or ICANN, is supposed to ensure the stable and secure operation of the internet's unique identifier system. The challenge that we get into is that any change that we make to the system risks the stability of the system.

You know, the KSK roll, we are changing the root key. It raises the potential risk of a fundamental instability, and it could break the DNS for anyone who actually does DNSSEC validation. So, there is a challenge that the organization, the community must face, and that is, in order to innovate, in order to improve things, we also risk increasing the stability.

So, going back to the original question of, what are the sort of four threats that we see? What sort of keeps us up at night? You know, for me, at least, is that the concerns that I have derive mostly on the unanticipated consequences of the changes that we're inserting into the system.

So, things like doing the KSK roll, that those, not so much anymore, but did, at one point, cause me some significant angst, because it did not see that the benefit of rolling the key outweighed the risks that were associated with it, given the infrastructure at the time. Similarly, you could look at the new gTLD program as a significant change that introduced a lot of instability across a whole bunch of different areas, but over time, the risks that instability generated, were seen by most folks who were participating to the new gTLD program at least, to have been outweighed by the benefit.

So, in terms of keeping me up at night, the threats that I see, it's the law of unintended consequences that keeps biting me in the rear end every time that I turn around that I worry about.

DENISE MICHEL: Thank you, David. Let me do a little bit of queue adjustment, since I think I'm missed Alain, who is in the queue. So, can we go to Alain? And then Emily, and Kerry-Ann, and…

[SPEAKER OFF MICROPHONE]

Cathy, and then… Yeah, Cathy, and then Karen, did you have something in the chat to interject?

[SPEAKER OFF MICROPHONE]

We have, yeah. Great. Karen, would you like to read the question and comment in the queue to make sure that we capture all of those for the record? And then we'll move onto Alain.

UNKNOWN SPEAKER: You need the mic, Karen.

KAREN MULBERRY: Well, Matogoro had a comment on whenever you ask something, no direct answer, rather given ICANN's limited mission, which sometimes gives me a difficult to go further. So, I believe he's trying to understand what we were talking about there.

He also has a comment. It is high time for the team member to discuss the ICANN limited mission.

And then Ram had a question. And there is another comment from Matogoro.

DENISE MICHEL: Do you want to read Ram's question?

KAREN MULBERRY: I'm trying to find it earlier on in the discussion.

DENISE MICHEL: Here is Ram's question. Is there any IPv6 threat landscape that ICANN has experienced for the past two years? So, we'll put that in the queue. Did you have any other questions or comments?

KAREN MULBERRY: There have been several comments from Matogoro in the chat. So, maybe we could just move those over into the record.

DENISE MICHEL: Thank you. And I would encourage all team members to make sure that you're in the Adobe chatroom as well. Make sure that we, that everyone has an opportunity to see these, and we'll make sure and have an Adobe chat comment archive to review as well.

But thank you, Matogoro and Ram. And please keep the comments and questions coming, and we'll rely on staff's help to make sure that those are interjected into new comments. Thank you very much. So, we're moving on to Alain and then Emily and then Cathy.

ALIAN PATRICK AINA: Yes. This is Alian Aina. So, I wanted to go back to what the CTU sent during his speech on the [inaudible] part of ICANN role. I know that it's in general, in the community, people trying to [inaudible], I'm coming from the RII community, people trying to limit ICANN role in the numbering system, but I think we should remind people that ICANN does have some operational role in the numbering part, because ICANN [inaudible] DNS.

ICANN also manage some [inaudible] and RDAP registry for the numbers, and also, ICANN has a role in RPTI. So, we can't say that ICANN has no operational role in the numbering part. So, can you clarify that one? You seem to know exactly what [inaudible]…

DAVID CONRAD: Sure. Happy to. So, ICANN does have some operational roles. As I'm sure you're aware, there… ICANN actually does not modify the root zone directly. That's actually a function that's performed by the root zone maintainer, who is contracted to be VeriSign right now. But we do have a direct role with modifications to the [inaudible] zone. Some of the [inaudible] zones, sorry.

And we have worked… There is a software system that allows for automated redelegation of the [inaudible] zones. That are used for the reverse look ups of translating numbers back into names, with a future deployment of R-DAP. There is a registry that is operated by IANA that is, that clients, R-DAP clients need to be able to fetch to get, it's called the bootstrap registry for R-DAP.

There are potentially, a role in ICANN in the context of what's called the resource public key infrastructure, that's used as a way, you can think of it in some ways similar to DNSSEC for the address space world. The addressing hierarchy has a root or a set of roots, that at least the IAB has indicated should be located at IANA, but the implementation may be otherwise…

In the context of protocol and parameters, there is a registry that receives probably the largest number of changes, which is the pen registry, the private enterprise numbering registry, that is used in context of network management occasionally fetched on demand. Let's see.

So, there is also the IANA KSK trust anchor, which we discovered very early on. There were devices that were actually fetching it apparently on demand, and those devices were the iPhone, I think. IOS version five. And we found that out when they had a tremendous spike in traffic going against that particular registry, Apple Tune picks that I guess they pass it internally or something, but it was a bit of a surprise.

Those are the only direct operational registries I can think of that are sort of critical to sort of the operation. We do run the IANA WHOIS server, which could be argued to be critical important infrastructure, say critical because that means certain things to certain people. Sort of all I'm thinking of, off the top of my head.

DENISE MICHEL: Thank you, David. All right. We've got… Did you have a follow-up question before we jump? Yeah, please. Sorry, I have James and Kaveh with direct follow-ups. Or, Kaveh and James.

KAVEH RANJBAR: So, David, thank you for the explanation. But I think, David, I need clarification of [inaudible], because many of these functions that you mentioned are IANA functions, [inaudible] PTI, not ICANN, because you said, us. But some of these [inaudible] from IETF to IANA function, and PTI has run them, but ICANN, for example, the [inaudible], the reverse delegation, it's something that IETF basically asks IANA function to do.

I don't know whether ICANN even comes into picture from RFCs or operations or [inaudible]… I understand the whole thing, but and I know you are doing it at the end, but it's, IANA function is PTI, correct?

DAVID CONRAD: Well, ICANN is the IANA function operator.

KAVEH RANJBAR: Okay. So, because I think this is very relevant for this. All of the services that [inaudible] and in that case, ICANN [inaudible] basically. So, that's your ascertain.

DAVID CONRAD: ICANN has been designated by the community as the IANA function operator. We have outsourced some of those functions to affiliate PTI, but we are ultimately responsible for the operation of ICANN the organization is ultimately responsible for the operation of the IANA functions.

KAVEH RANJBAR: Thank you for clarification.

DENISE MICHEL: James, do you still…?

JAMES GANNON: So, your list actually made me think of something that I wanted to ask. With the IANA transition, did IANA give away the [inaudible] to someone else? Or is that still…?

DAVID CONRAD: That remains a rather unusual but IANA function, sort of.

EMILY TAYLOR: Could I ask? It's very excluding.

JAMES GANNON: Two [inaudible] the time zone database.

DENISE MICHEL: We have Emily, Cathy, Kerry-Ann. And I would remind, I think, staff will put you back in the queue to answer Ram's question about, yeah, IPv6 threats. Emily, and we've got a coffee break coming up at 10:30. We could push that up, that would be great.

EMILY TAYLOR: Thank you very much. First of all, I would like to say how much I personally appreciate your engagement in this conversation with staff. I know it was sprung on you when you were busy, but just having you here, and engaging in this quite informal unstructured way, is very, very, personally I'm finding it incredibly useful.

I wanted to ask about the risks of things not happening, because I was a little, you know, I noticed that in your laundry list of things that keep you up at night and threats, there are several things that if they don't happen might well have implications on stability or security, like DNSSEC, you know? Have you given up IPv6, ditto? What are the risks if we continue the status quo there?

But also, forgive me, because this might well seem a completely weird suggestion, but I was talking with somebody from the maritime industry the other day. And there, you know, people involved with that industry deal with just unbelievably scary things all of the time.

And the person I was talking to said people are just un-scare-able now. If you try and sell them a widget, you know, [inaudible] you know, they're like, I've got insurance. One thing that we don't really…

Two things, really. We don't tend to look outside our sector for the practices or ways of dealing with incredibly scary and persistent problems, and two, the role of insurance. I've noticed with working with [inaudible] that as we're exploring issues related to internet of things, that suddenly the insurers are all in the room. And also that, you know, there are some risks of, as this technology becomes more persistent, we rely on it more and more ingrained in our society.

There are going to be some risks that will not go away and are engrained and we cannot really manage away. And that's a rule that insurers can also be a really good way of driving up standards at the edges, which is one of the challenges we've all repeated again and again. So, I thought I would just throw that out there into the conversation.

DENISE MICHEL: Thank you. Does anybody have any follow-up to that? And I know that James wants to jump in on this point as well.

JAMES GANNON: Sure. With regards to the things that not happening. If looking at IPv6 as an example, that's an area that actually has, maybe because of sort of my past history, I have some particular interest in, you know, my belief and it really quickly goes into the realm of opinion that my belief for this IPv6, that we do not somehow migrate to IPv6.

It will mean obviously, that it will remain with IPv4 in order to allow for IPv4 to scale. It will mean increased deployment of carry grade [NAT], which has the unfortunate side effect of adding an additional level of complexity into the underlying addressing infrastructure. That complexity gets reflected sort of most painfully when attempting to manage the network.

And by management, I mean both in the context of the simple network management, just keeping the network up and running, but also in terms of dealing with abusive threats on the network. CGM basically allows for hiding of the source of attacks, and also allows for a much simpler mechanism to concentrate attacks. For example, if you have a CGM sitting in front of a large number of customers, taking out that CGM means that you're able to take out all of those customers.

So, if we don't migrate to IPv6, then I believe there will be increased fragility, increased abuse within the network. So, one of the reasons that I am not one of the IPv6 haters is that that doesn't seem like the best technical solution to move forward. Similarly, with DNSSEC, if it's something that we do not deploy, the underlying infrastructure will continue to function.

There would likely be increased abuse specifically in the area of which DNSSEC was designed to prevent, but given how trivial it is for the bad guys to take advantage of other vulnerabilities in the system, it's unlikely we'll see a whole lot of attacks that are derived specifically on

DNS on [inaudible] or cache points, I mean. The real, for me at least, the real interest in the [inaudible] is not so much what DNSSEC protects, it's more what DNSSEC facilitates, which is an alternative public key infrastructure to replace the increasingly broken X509 infrastructure that is used for TLS.

The HTTPS connections. Also it turns out that DNSSEC, if it was actually deployed, appears to be able to defeat an entire class of denial of service attacks, ones that make use of resolvers to reflect responses from essentially random name lookups. [Inaudible] DNSSEC can actually prevent that, if it was actually deployed and validated as a return.

So, you know, there are obviously other technologies that if we don't deploy them, you know, we face increased risk of badness, for example, RPTI PGP SEC is a technology that, at least conceptually we desperately need. The routing system right now is tremendously vulnerable, RPTI was specifically designed to address some of those vulnerabilities, whether or not it's the best solution or a deployable solution, it's still somewhat up in the air, and there are some limited deployments, some people are actually using it, but it doesn't seem to be taking the world by storm as is necessary to defeat some of these infrastructure issues.

DENISE MICHEL: Thank you, David. I think James wants to get in on this particular topic as does John. Any others? And then we'll move on to the queue. Go ahead.

JAMES GANNON: James Gannon. So, three quick things. Yes, XO509 is really working at this stage. I just want to put [inaudible]. And so to the question that insurance. So, I might be a little bit controversial here, I was hoping that this would come up. And so, at a very high level, if there is anybody who works, please ignore me now.

There is three things that you can do with risk. You can either accept it, you can mitigate it, or you can transfer it. [Inaudible] of insurance is transferring the risk. It is acceptable for an enterprise to do that. I would put it on the table here, I don't feel it would be acceptable for ICANN to transfer risk pretty much to do anything [inaudible].

So, while we may have a conversation about the context of cyber insurance within the ICANN specter in DNS, I don't want us to ever to think that we can insure away any of the risk that we should be looking at. It's just something that I was very worried about coming up with some things.

EMILY TAYLOR: You know, funnily enough, that wasn't why I raised it. Okay? The reason I raised it was not because it represents a magic wand that would suddenly make everything great. But that insurance has a, you know, think about getting your car insured or getting your house insured. If you have this sort of lock, or that sort of alarm system, your premium goes down, and you as a consumer, are incentivized to raise your standards in ways you don't understand and don't care about, accept that it lowers your insurance premium.

One of the things that we are constantly ringing our hands about, from around these tables, is the fact that we can't get these really, really key messages over to [inaudible] affect their behavior, and insurance is something that has worked in other context to get people to change their behavior for the better. It's certainly not a magic wand.

It certainly doesn't take risk away. I think many people around this table understand that.

DENISE MICHEL: Thank you James and Emily. John and David are on this topic, and then we're going to return to our queue with Cathy.

JOHN CRAIN: So, I wasn't going to talk about insurance, and I also [inaudible]. You know, I've had conversations with people from some of the large insurers, and one of the things they do bring to the table is a different insight, and that's always good. So, getting those people to come to the table, not necessarily to insure, because you want to get rid of the risk, you'll just outsource everything, right? So, not our problem.

So, I think it's good to have insurance, people in conversations, because they approach risk differently, I think, then people like I do. So, I think that's good. One these six, and basically DNSSEC, all of the new protocols, and this is part of the, watching the risks and opportunities. As some of these protocols get deployed, they don't get deployed correctly.

It can cause really interesting problems. You know, IPv6, certainly the early days, in the office of management and [inaudible] in the USA, you must have IPv6 to sell things, became a rubber stamping exercise. So, I think things get deployed, just like [inaudible] and other things that may come back to haunt us at one point.

And the other side of these new technologies is that they're not understood by people in the public safety community, etc. So, that causes some interest for us internally. I mean, recently, I've had at least four conversations about [inaudible] networks and what that means with various public safety agencies from around the world, who are chasing people.

To rate those, a translation mechanism so that people would be [inaudible] and get onto v6. And there is an algorithm or a mechanism for using the v4 address of the client to get the v6 address, and you know, we get people sending messages to ICANN, saying hey, this is address, just like private addresses, a lot of addresses to IANA, if they're a protocol addressed space. So, we get a lot of questions about how this works.

So, one of the interesting things is we deploy these new protocols, or the industry deploys them, and it does cause some interesting times as we deal with lack of understanding. And I don't think it's ICANN's job necessarily to teach anybody how to do v6. I think we should be aware that as these come up, they're going to cause interesting conversations, and you'd be amaze what people think ICANN should be doing.

DENISE MICHEL: Okay. We have Cathy, Kerry-Ann in the queue. Anyone else?

CATHY HANDLEY: This has been an interesting conversations. And anyone that was standing outside the door would probably didn't know what we were talking about, would be terrified to use the internet.

But we can't tell them that. But my question that it goes to, part of what Matogoro said, I think Kaveh touched on it, this is all really neat stuff to hear about, but out of all of these discussions, we have a pretty narrow scope when it comes to most all of this. And I guess my question to staff or anybody else that cares to answer is, what out of this discussion, do you think is actually in our scope? Because having been around these folks for a lot of years, they tried really hard to fix a lot of stuff, but not even close. It's just more stuff, so what do you think, or is anybody on the team, out of all of this, what is within our scope that we need to get on to deal with? Thanks.

UNKNOWN SPEAKER: So, personal opinion here. I [inaudible] to look to the things where the policy realm can actually have an effect. A lot of the operational stuff we do is whack a mole. You know, we'll never be able to train everybody. We'll never be able to educate everybody, and that's just part of life. But there are… One of the questions that I always have, when we deal with these issues, is there a policy inflection here where we the ICANN community can actually make a difference?

Sometimes there is, sometimes there aren't. I don't believe I know the answers here. That's one of the pivots I try to use to make myself not go insane. I think some of these things are actual solutions in the policy realm. I don't know if that helps a little bit. I mean, I can't point out specific ones. I could, I guess, but like having a process to not hinder registries when they're trying to do public [inaudible], things like that. So, that's a policy or a process implementation that we were able to do to actually at least not be part of the problem.

DENISE MICHEL: Go ahead, Cathy.

CATHY HANDLEY: That's, you know, it's nice to sit here and say, I do policy. I've done policy for more years than I care to count. And so, this is policy directly related here. And like what you're saying what you did with the registry, you know, maybe to steal this from something another person in this room said, at one time, is given there is not a lot of interaction, given v6 with the RIRs, maybe a recommendation is, right now it's done back and forth when you request the [inaudible], you request it via email.

And everybody knows each other because they've all worked together for 100 years. But going forward, maybe a suggestion is something like, do that over PGP. It's those kinds of policies that I'm looking for a response out of anyone, that can recommend doing, you know, those kinds of things. So, thank you.

DENISE MICHEL: Thank you, Cathy. I think we have others in the queue on this topic, and I'd also like to note that I see a whole range of items, numerous ones, that I feel are within scope for a whole variety of reasons, and I think it will be really useful to talk more about this in specificity as we get into that part of the agenda. David?

DAVID CONRAD: Yeah, just, one of the reasons I sort of started this by reminding people what ICANN's mission statement actually says is to, provide the context under which some of the discussions that we're having could be cast, and map them back into things that ICANN actually does have control over, ICANN either the community or the organization.

You know, ultimately, the review team will come up, yeah, well, it doesn't have to, but it presumably will come out with a set of recommendations. I don't think anything needs to be fixed, and don't recommend things, but presumably you will come out with a set of recommendations, and those recommendations should be actionable and allow us to improve the SSR of ICANN.

So, ultimately, it will need to map back into the mission statement and into the things that we're actually responsible for. And that is, you know, somewhat broad, in the sense that the mission statement also includes the grandfathered strategic plan. So, pretty much anything can be counted as in scope. But, you know, hopefully it will be limited to things that are directly relevant to sort of the day to day operation of ICANN.

DENISE MICHEL: Thank you, David. Anything else on this particular question? Cathy?

[SPEAKER OFF MICROPHONE]

Sure.

DAVID CONRAD: I may be stepping into the catastrophically frank realm here. So, this is John Crain speaking.

JOHN CRAIN: Thank you, Mr. Conrad.

DAVID CONRAD: Some of the things that are uncertain whether they fall into the SSR remit, I take a very broad view of domain abuse and feel that is squarely in our remit, and there are people in the community who disagree, but part of the bigger picture of understanding how ICANN organization and community can manage many of these threats is to understand whether compliance has the right enforcement tools.

Compliance is criticized, yeah, you know, often for, especially by law enforcement on one side, for not acting in what seems to be patently obvious situations. They're criticized on the stakeholder side for trying to enforce things that actually, [inaudible] to, you know, business and the like. That tells me that there is a [inaudible] match on both sides.

And so, possibly looking at something like the RAA and saying, these are the things that seem to be aligned correctly with moving forward on security threat litigation, and these are the things that are not. As an example, people in law enforcement will say that the RAA is open loop. You can have 800,000 inaccurate WHOIS records, if you correct them, there is nothing beyond correcting them that compliance will do.

And so, an operator who has, perhaps persistently, a poor record in managing, managing is his obligation for WHOIS, you know, whatever that obligation may be contractually, you know, essentially operates unregulated, and unregulated I use very carefully because we have a self-regulated industry, and that's all well and good, except there are no controls for when people don't self-regulate.

And so, this is part of, I think, the process that a lot of the GAC and a lot of the law enforcement and the public safety working group look at ICANN to try to solve. And one of the specific ways that many people have mentioned, that would help, is to seek some way to at least narrow the gap between an acceptable use violation, or terms of service violation, and the month long process that's involved in mutual legal assistance to get action on domains through the legal system.

Certainly, the legal system needs to accelerate, we all know that. But surely, there is something that we can do that is between the four hour objective, or even less objective, of taking down a domain that's hosting malware, and nine months to get a court order. So, even if you started with a conversation that talked about the major security threats that the GAC has identified, and say, "Is there a way for the entire community to agree that these are a baseline for an acceptable use policy?" And say, "This is the recommended acceptable use policy." What effect would that have?

I'm not saying do it, I'm saying think about what effect that would have, and have a serious conversation about trying to close that window. Thank you.

DENISE MICHEL: Thank you, David. I think this follow-up on that topic specifically from Zarko and James. Anyone else? And Steve.

[SPEAKER OFF MICROPHONE]

Thank you. No. No coffee. Let's close out this topic in the queue. We have a few people, Zarko and then James.

ZARKO KECIC: I just want to tell you a story, because James told you one, and I want to contribute. Why ICANN policies are very important, they are not influencing ccTLDs, but we are using, that we recently changed our software, and it enables us to impose additional checks on registrants, and our registrars, and we got a lot of complaints from them. What you are doing, you're typing stuff, and things like that.

And my answer was, those are mostly new ICANN policies which are imposed to gTLDs, and most of them, we accepted was new policy for gTLDs. But I like for some of them, because it ensures that people are not going to read ICANN policies at all. But, it is important to have new policies especially on abuse issues. We cannot fight all of them, either ICANN or ccTLDs, but we can try to do the match.

DENISE MICHELE: Thank you, Zarko. We have James and Steve on this particular topic, and then we'll go back to our queue.

JAMES GANNON: Two things. So, I'm trying to think how to phrase this. Yes, there is a role for us to look at certain aspects of security coordination and making sure there is an effective internal process at ICANN for helping law enforcement do their job. Both having spent two years of my life on privacy proxy PDPs, and the wonderful world of, how far does that facilitation go with ICANN?

It's incredibly important for me to put out there that ICANN is there to follow-up the laws. If law enforcement come to ICANN without a warrant, then it is not ICANN's role to provide a process to get access to data that they still don't have a warrant for. So, I get scared when I hear things about [inaudible], because they're there as legal treaties between countries for a reason, and I hope that we won't, when looking at these topics, get to a point where we consider what maybe happens in other discussions at ICANN of circumventing those national processes and those legal frameworks that exist for a reason.

I just want to put it out there having been through those conversations before. I hope we don't get to that point in this group.

DENISE MICHEL: Thank you, James. And I would just like to insert a note, that we're not simply talking about law enforcement requests. In a nutshell, this is a global platform like Facebook that serve billions of users, are reliant on the ICANN community and ICANN organization in particular, to implement the fundamental requirements and the registry and registrar contracts, which is very important to mitigate a whole range of abuse.

And there is substantial evidence, and has been for several years, that we are, as a community and staff, not where we need to be, and enforcing what we already have, let alone examining the RAA as to whether we need more tools. Steve, you're in the queue.

STEVE CONTE: So, this goes back to Cathy's question of scoping of everything that we've talked about, and what part of it is within ICANN. And as I was, I had my card up, and as I was listening to David, I was agreeing. So, I lowered my card, but the risk of this being my last day at ICANN, I want to counter some of what David asked and approach, bring it to the review team.

One of the things that was brought up was to make… And I fully support this in regard ICANN as the organization, when a recommendation is made, please make it very clear, very actionable. But I struggle with this, and I've been thinking about this for a number of weeks now, is you know, and I ask the review team, are you looking at ICANN as the organization or ICANN as the community?

And does it impact the level of questioning and recommendation? So, if something is important that's affecting ICANN as the community, affecting SSR or a country affecting the SSR, ICANN as a community, I ask that, first of all, acknowledge the difficulty of making a recommendation around that because it's not directly actionable and implementable, or could not be necessarily.

And if there is something that is community wide, or [inaudible], I think there are probably some items that you guys will talk about, that's worth discussion that might not be directly implementable by ICANN as an organization. And when discussing that, and if you recommendation around that, please make sure that it's written as such that you understand that it might not be implementable, but be as a best common practice, or some kind of form of that.

So, we know that you know, two years from now when we go back to the SSR 3, and we're trying to show you implementation that we, or whatever review team at that point, that you know, it might be directly actionable from ICANN as an organization's perspective.

DENISE MICHEL: Thank you. That's a really useful reminder, and I would note that previous review teams on a range of topics, have issued recommendations and specified whether that recommendation is for staff, or for the ICANN Board, or for some element of the ICANN community, to implement, and I think that's a really useful reminder. Thank you.

We're going to go back to the queue now. I have Kerry-Ann, Dave Piscitello, and I have Karen in the queue to address, I think, additional comments and questions in Adobe Connect, and then we still have Rom's question on IPv6 to address.

KERRY-ANN BARRETT: I think the… There are a couple of things going through my mind. It goes back to Kaveh, it goes back to what Kaveh said earlier. I'm going… Now, you didn't think I was disagreeing with you entirely. Because there is context to what Kaveh says, based on the dialogue we just had, and to tap onto it, James said something earlier that we're not talking about cybersecurity. I think it's very important for us to, as a team, to appreciate that.

The reason I keep going back to the clause, is because it says, to ensure the stable and secure operations of the internet's unique identifier system. In 2015, you guys had done, ICANN has done a presentation on what is the unique identifier system, and it went through what the community is responsible for, what the operators are responsible for, and I think when we get to the subcommittee [inaudible]…

The subcommittees that James suggested, where we get to that discussion, I think there is a need to add an additional one and probably remove the first one. And I'll probably say why. We will be talking about SSR 1 recommendations here. But in terms of actually talking about what is direct and indirect, and then keep going to that, because that is the discussions have been, what has been our remit and what is outside of our remit.

And I think if we start to contextualize ourselves to think what are our direct recommendations? What will break the internet if we do not recommend these things? And what will be nice to have to ensure the improved resilience of the internet?

Because I think we have to talk about the security [inaudible], stability is one thing, we [inaudible] is one thing. I think each subcommittee has to think about it in that context. And my comment is a more general one, that as we approach, as Jim said, the actual work, we should just starting thinking about what can we [inaudible] through policy, technical, community versus operators directly.

How do we…? I think our recommendations has to be holistic, and each time we give a recommendation, think about, as you said, who? If it's at the operational level, if it's at the community level. Will this directly break the internet? Or is it that it will improve the resilience of the internet? And I think that's where the technical discussion comes up, because the technical…

We will not be able to give technical recommendations, but we can say to the technical person, I think you guys should look at this in a little bit more detail. I think you guys should work together. As Cathy said, I think there is a lot of cross-pollination that's not happening, that I think as the internet…

As David rightfully said, it's going to get crazy. I told James [inaudible] anticipation, optimistic view. In two years, it's going to be absolutely ridiculous. ICANN, as you said, cannot fix it, but we do have a lot of influence and are responsible for a stable and secure operation. That's something that is where our view is.

So, in terms of talking about limited scope, there is a lot of discussion that is happening in the chatter about limited scope. And I think when Karen explains [inaudible] concerns, I think at the end of the day, for me personally, as a [inaudible] is making sure that we give direct, indirect.

And I think once we approach it that way to [inaudible] concrete recommendations we give at the end. Thanks.

DENISE MICHEL: Thank you, Kerry-Ann. Dave Piscitello, did you still have, I had you in the queue. Did you still have comments?

[SPEAKER OFF MICROPHONE]

No. Yes.

Of course, everyone feel free to leave when you need to. We're just about to, I think, wrap-up the queue. We've got Karen to run thorough things that are in the Adobe Connect chat. And then we have David Conrad to respond to Ram's IPv6 question. Go ahead, Karen.

KAREN MULBERRY: Yes, thank you very much. Karen Mulberry. I was a reading comment from Matogoro in the chat. He's come up with, policy consideration might be within our scope, but also we might have recommendations that deem important, the community outreach will also give us more input on this matter. ICANN limited mission should not be an obstacle of making internet a safer platform for everyone, in the coming generation.

DENISE MICHEL: Thank you, Karen. And thank you, Matogoro, for your contribution. David.

DAVID CONRAD: Yeah. In regards to IPv6 related threats that we've seen. I think what we are tending to see is that people are deploying IPv6, but not applying the same control policies and other controls, that they have applied to v4. I was just speaking with one of the speakers yesterday, [inaudible], who is looking at information that's going to corp dot com, and when right now, corp dot com is only being served on v4, when he turned on v6, the amount of traffic spiked up significantly and seen all sorts of new things, that weren't seen on v4 because the v4 control policies had blocked those sorts of activities.

So, the threats that we're seeing are sort of like history repeating itself. Hopefully more quickly, so we can get parity with the sort of security with v4 more quickly. But we aren't seeing a whole lot of like spam, as yet, on v6. It's starting, but it's just, you know, sort of the beginning bits, at least as far as [inaudible] or John might have different perspectives on that.

Other than that, you know, v6 is sort of just likely for just v4 with more bits.

DENISE MICHEL: Kaveh, do you have a follow-up to that?

KAVEH RANJBAR: Just as a follow-up to Matogoro, just for the record. I actually want to say that I completely disagree with the assessment. So, I think ICANN the scope of the review should be completed within the remit of ICANN. Within the ICANN, meaning what ICANN has to do. Within the mission of ICANN.

DENISE MICHEL: Thank you. I'm not sure whether it's the desire for coffee, or that we've actually run out of things to discuss on this. I spoke to soon. Kerry-Ann.

KERRY-ANN BARRETT: [Inaudible] is asking for a coffee break.

DENISE MICHEL: Matogoro needs it. We'll take a break for 10 minutes, and then we'll come back. We will tackle the SSI one implementation upon our return. We have additional questions relating to the DNS Symposium topics yesterday. Please put them in the chat room or send an email to the list. We'll make sure that we get answers in writing. Thanks.

Could I ask staff for help in corralling [inaudible], let people know that we're going to start again? Thanks.

Okay. This is Denise, and we're going to get started again. Next on our agenda, we have the implementation of the first security review team recommendations. Not all of the recommendations, but a majority of them we'll receive a briefing on this morning. We'll be following up with additional staff, to round out the recommendations we aren't able to address today.

We've got a little less than two hours before lunch at 12:30 ish, so we'll get started. I'll turn this over to staff.

STEVE CONTE: Just wanted to, [inaudible] before get started on this, I just want to jump in and say, the dialogue we had this morning, very fruitful, and in the background we're like, well, this is on slide X, and slide one and stuff. As we go through the recommendation implementation, please keep that in mind, that the dialogue that we had was very healthy and relevant to the implementation of SSR one, with the caveat that much of what you'll be seeing in the implementation is also historical that the SSR one was 2012, and the implementation that have taken place any time between 2012 and present day.

So, you might see some variance in the answer because that was the answer back then, and yet, some of the items still might be relevant, most of the items are still relevant, and the answers might have changed due to the evolutionary, you know, evolution of ICANN, of the internet, and just you know, time moving forward. So, just please keep that in mind.

DENISE MICHEL: Thank you, Steve. Yeah. That's important, and I would invite staff to also help remind us of the context of the first security review back in

2012. The new gTLD program had not launched yet, so there was very much a different landscape in many ways that they were addressing, and a different ICANN organization that they were addressing in their recommendations.

Go ahead. I'm not sure which staff person is going first.

NEGAR FARZINNIA: Good morning everybody. Negar Farzinnia, ICANN staff. MSSI. I'm going to be going through the implementation briefing with the team today. And hopefully that will help provide some insight into the work ICANN has done to implement the 28 recommendations from the first SSR review.

Just a quick highlight of what we did for the implementation. So, ICANN organization has enlisted a significant amount of time to implement the 28 recommendations. The implementation time spent as Steve point out across, any time the recommendations were first approved by the Board in October of 2012, and we closed the most recent ones in April of 2017.

Majority of the recommendations was on within the first two and a half years of implementation timeframe. And some of the highlights include, the office of the CTO that was announced in June 2014, with a mission that is directly aligned with this period of the SSR recommendations. David Conrad, as you know, took the office in August of 2014, and has since built a team of 14 professionals who work to understand and ensure the security, stability, and resiliency of the unique identifier system.

The creation also helped align the mission of the office of the CTO security, stability, and resiliency team, led by John Crain, with the [inaudible] technical advancements of the internet. We have since created SSR framework. That was a result of defining ICANN's SSR rule and technical mission, and this work is not published annually.

And one of the things that ICANN organization is striving towards, is increasing and improving this outreach and engagement efforts with the SOs and ACs to promote SSR related best practices. And with this brief highlight…

DENISE MICHEL: Can I interject with a question? When was the [octo?] chain created? And there are 14 members of the [inaudible] team, I assume that means everyone under, in the [inaudible] team answer the question of how many staff are on specifically on the SSR part of the [inaudible] team.

UNKNOWN SPEAKER: Sure. So, we joined ICANN in, when was that? September of 2014. And initially the office of the CTO, my job had no staff, and I was reporting to Akrim [inaudible] the president of GDD. And if I recall correctly, I guess May of 2015, it was a restructure of what were then called the global leaders, the executive team, they reported directly to Fadi. And the, my role was moved to report directly to Fadi, and I was allocated…

The CEO at the time. And I was allocated resources to bring on staff. And that has since grown. I believe FY 18 slots for personal is at 18, but I don't have that money for 18. So, end up being 16 total. In terms of the SSR related staff, right now we have three dedicated SSR individuals. Four. You're right, four. Sorry, four. And I'm in the process of doing a minoring restructuring that will probably increase that to 4.25.

DENISE MICHEL: John.

JOHN CRAIN: To give some context here. We started the SSR function a couple of years before that, and we had some areas where we were working in, and we'll get to that. One of the areas was research, and frankly, we weren't doing much. So, we're the guys with the SSR title, that all of the research that was in our original remit is, [inaudible] worry about. So, it's actually not getting done, they just don't have the SSR title on them. So, there is a lot of SSR work being done, but it's not, they're not direct SSR staff.

DENISE MICHEL: That's useful. Thank you.

NEGAR FARZINNIA: No problem at all. Okay. So, ICANN organization has taken a thematic look at the 28th recommendation as a result of the SSR 1 review. And the reason we did that is because we follow up on interconnection between recommendations, and we essentially identified a list of core recommendations, which are highlighted in dark blue on the slide that you're seeing, and those are the ones we're going to go through into this presentation.

These core recommendations are essentially the basis for the rest of the recommendations, and everything else is derivative of these 10 recommendations in one form or another. So, we're hoping that going over this 10 will provide a really good basic understanding of what we've done to accomplish the implementation of the recommendations and help with any questions that you may have.

Just to highlight the recommendations, these are the 10 we're going to cover, and I will go through them one by one, so no need to identify, this is just to provide an overview for everybody. And with that, we'll start talking about SSR framework, and to help set up the basic pillar of SSR one implementation, and we'll start with the first recommendation, which is asking ICANN to publish a single, clear, consistent, statement of a SSR agreement and limited technical mission, through gaining public feedback and reaching a consensus based statement.

I'll turn it over to David. We've talked about this already. We have discussed ICANN's mission and core value as part of earlier conversations today, but I wanted David to provide a brief overview of ICANN's mission as stated in the bylaws today.

DAVID CONRAD: All right. So, when we did this, when the SSR one review, we're actually under a different mission statement, so some of this might, there might be a little mismatch between the previous mission statement and the current mission statement, that structurally, they're about the same thing. As I mentioned earlier in the previous session, the mission of ICANN is to ensure the secure and stable operation of the unique, the internet's unique identifier system, as described in the following section, and I guess, that's what it, yeah. Hold on, go back. I thought there was more there.

So, with regards to the section 1.1, that leaves out the, what the ICANN coordinates, facilitates, and collaborates each of those, again, dealing with the different functions that ICANN performs from dealing with the IANA function, which consist of dealing with the root zone, providing top level blocks to the RIRs, and managing the internet protocol registries. As well as doing things like coordinating the development and liquidation of policies, concerning the second level registration of domain names in gTLDs.

And facilitating the coordination of the root name server system. So, all of that is incorporated into the mission. As I mentioned, the mission has changed over time, so the current mission for purposes of SSR two is obviously what you'll need to be working with. So.

DENISE MICHEL: Kerry-Ann?

KERRY-ANN BARRETT: David, you gave a very good list just now. And that was based on the old mission?

DAVID CONRAD: No, that’s the current mission.

KERRY-ANN BARRETT: The list you [CROSSTALK]…

DAVID CONRAD: Sure. It was actually just cribbed from the bylaws…

KERRY-ANN BARRETT: …summarized…

DAVID CONRAD: Okay, yeah, I’ll be happy to. Sure, yeah.

NEGAR FARZINNIA: Kerry-Ann, we actually we slide later on the day [CROSSTALK]… that has those details broken down.

KERRY-ANN BARRETT: [Inaudible] really good, boom, boom, boom. [CROSSTALK]

NEGAR FARZINNIA: The boom-boom is already there. It’s all there.

All right. Moving on to the next slide, I believe last time we met in Copenhagen, there was a question that came up about definitions for the review, and we have three basic terminologies, clearly pertaining to

SSR. I wanted to ask Patrick to help us talk about where these definitions came from to begin with, and how they were [inaudible] the community.

What you see here are the definitions in their current form today. They have evolved over time. The definitions were part of the SSR framework, back in FY 12, repeated in FY 14 framework, FY 15, 16, and this is the most current version of the definitions we have, but with that Patrick, please lead us to the discussions.

PATRICK JONES: Thank you very much. Patrick Jones. So, I'm going to talk about this from my perspective of when I was part of the security team, back from 2009 to 2013, but I've been around ICANN environment for a very long time. So, much of this has a historical perspective it will bring. The SSR framework, as a term, was hard coded in the original affirmation of commitments.

It's no longer in the new current bylaws, the current bylaws only state that the review team should access the extent that ICANN has successfully implemented in its security efforts, whatever that means. So before, under the previous bylaws, we had an annual obligation to produce a framework. And we had produced that framework going back to 2009.

So, even before SSR one, we are producing this document. Now that document really grew out of early discussions within ICANN of security and stability, and resiliency was added later as a term, as John can also talk about. That term was added around 2008. I wrote up a document that we published in 2013, that looked at the historical use of these terms, security, stability, resiliency, even going as far back as the earliest appearance of these terms in RFCs.

So, security has been around as a concept long pre-dating ICANN, goes back into the 60s with the original ARPANET. Stability and even coordination, appear as a concept in the white paper, which for spelling out for this. For those who may not be familiar, it's the 1998 US Department Commerce statement of policy on the management of internet names and addresses.

So, the terms that we've been working under, stability, security, and resiliency, first grew out of an ICANN meeting that happened in 2001, that was focused purely on DNS security and stability issues. Then there were, as mentioned earlier, the four original DNS Symposiums that were held, so this goes back to, I want to say, 2009 and then the Tokyo meeting, the meeting in Italy, and out of that, a lot of, you know, discussion with DNS community, security experts, start to coalesce around these terms.

We, as in ICANN security, published these terms in the SSR framework, and the FY 12 version, but it's essentially commonly understood terms that we have been working under. Those went out for community consultation and revision, and then we've been working under these terms all the way through the current version of the framework that was published.

Hopefully, that helps set the stage. And if John and Dave want to add any other historical perspective, that's where the terms have come from.

UNKNOWN SPEAKER: This is a [inaudible] comment actually. There is an intermixing of security, stability, and resiliency definition, because if the system is secure, it can [inaudible] malicious attacks and [inaudible]. So, there is… Once we call it a system is attacked or not, so if it is attacked, it can be considered as an unsecure system. Or that it can [inaudible] malicious attacks.

With the security and the resiliency, there is a confusion.

UNKNOWN SPEAKER: So, I don't want to get into a discussion about what is and what's not the right definition, because we spent months having those arguments, and this is what we came out with and what we're using because we had to take something. And I will just say there is no such thing as a secure system. So, no matter secure it is, when it breaks, hope it's resilient back. So, but yeah, we had many, many discussions about the terminology, so here, we're just trying to lay you out what we're using.

And actually, from each of those four, and I always forget Puerto Rico. There were actually reports. Those weren't ICANN driven meetings. When I set up those symposiums, as an idea in the late 2000s, the idea was to get the community together and help us develop what we thought all of this stuff were.

So, there is actually reports out of each one of those, and you can find them on our website, and I think they're included in the documents that you have, if not, we'll make sure they are. So, they make really good reading, because it sort of gives you some context about how the community was thinking about some of these problems back then.

UNKNOWN SPEAKER: Thank you. Did you have more? Okay. Dave.

DAVID PISCITELLO: Dave Piscitello. The distinction between resiliency and security is really system versus distributed system. So, if you have some telco background or networking background, I mean, I had wanted to use the terms redundancy and diversity, because that's really what the resiliency aspect of this represents. And so, you know, I think the security, as you say, is a system is able to withstand, yeah, [inaudible] attack.

Resiliency is, if you attack a system, there are other systems that can take over for the loss of that one system.

DENISE MICHEL: Thank you, Dave. Okay.

NEGAR FARZINNIA: If there are no other questions, we can move on to the next slide, talking about the challenge that the unique identifier system faces. And John, tag, you're it.

JOHN CRAIN: Well, luckily, we've had this discussion. Right? So, this is what are some of the challenges we're looking at? What is the threat landscape? And I think we've talked to these and many more. So, I don't know if you want me to spend a lot of time, the DDOS attacks, the botnets that were out there, etc.

And some of the trends that we've observed over the times. You know, we're operating in a changing environment, and we have to recognize the risk and the opportunities there. So, I mean, if there are specific questions about them, I'm happy to go into them, but you know, we've had a long discussion this morning.

DENISE MICHEL: Emily and then David.

EMILY TAYLOR: Yes, I don't want to repeat the discussions this morning, which I thought were really, really good. It's just quite, sort of flip it on its head. We've got ourselves into sort of like, it's so terrible out there, but I think it is also worthwhile for us to think about achievements, and things that have improved.

Can you just give a very brief outline of what you feel has actually got better?

JOHN CRAIN: So, as I say, risks and opportunities, I always try to say one without the other, because you know, they go hand in hand. The couple that we've listed here is actually, we haven't nationalized domain names. We take it for granted, don't. Right? There were times that that was probably not going to happen, and we have that. That's good. Yes, we don't write the numbers, but we do actually have DNSSEC, and we are actually going to roll the key, and David's going to go to jail for breaking the internet.

You know, there are other things. Collaboration across the industry, around SSR issues, is much better now than it was 10 years ago, 15… Remember, [inaudible] from the DNS cert discussion. I think if we had that discussion today, it would be completely different, because you know, now the, for example, the ccTLDs have a mailing list of all of their security experts, not only invited the list, I'm on the management group for that list, and they've added other stuff.

So, the relationships and the trust is much better now. So, things are getting definitely better. V6es are actually getting deployed, so we don't have… We still have issues around v4 marketplaces and things like that, but it's not, oh my God, will this work? So, there is a lot of progress. Nobody even talks about autonomous system numbers running out anymore, right?

That just happened. Right? So, there is a lot of good going on, and I think a lot of the things that help me sleep at night, are the fact that I know that a lot of this collaboration and the cross community working together is much better than it was even, I would say, five years ago, and I think it's continually increasing. Always needs improvement, but things are, there is a lot of positive out there.

EMILY TAYLOR: Thanks a lot for that, John, and I think that this is a really important aspect for us to bear in mind as we work, you know, as our work progresses, is to think about what has been working, and things that have changed in the landscape for the better. And techniques that you have used that have worked in some context.

I notice that the DNS cert issue, which Noorul first raised, seems to be bubbling beneath the surface and could well be an aspect for us to examine more closely. Thank you.

JOHN CRAIN: To me, that's a terminology. So, it's really about collaboration.

UNKNOWN SPEAKER: Just touching on some of the trends that are on the slide that we probably didn't get into too much detail in a previous discussion, we're now, I believe, upwards of 90% of TLDs in the root zone have been signed. Obviously, all of the new gTLDs are signed, and the majority of the ccs are signed these days.

We are beginning to see increased deployment of DNSSEC validation being turned on in resolvers, but that's an area of improvement that's needed across the internet infrastructure. We're at 600 plus root instances across the planet totally. ICANN, I think, is 155.

The ccTLDs, as John mentioned, IDNs have been deployed. What else is interesting there? Oh actually, that last bullet. This is an area, a sort of strong pressure on my team, and ICANN the organization, in general, and that is the area of capacity building. We get a lot of requests for capacity building, a lot of training. People want to understand the DNS, understand ICANN, understand help to identify and mitigate DNS abuse, way beyond our capacity to actually be able to fulfill.

So, that's an initiative that we're trying to figure out how to address internally within the octo group.

DENISE MICHEL: In case not everyone is aware, could you explain what you mean by capacity building?

UNKNOWN SPEAKER: Yes. Primarily training, either hands on labs that we have been doing in the past with, for example, deploying DNSSEC, although given the depth of deployment and the entities to which ICANN is directly responsible, we're probably going to sort of redirect focus on that, but also training for law enforcement, government officials on what the DNS is, how it works, how it's being abused, how to mitigate those abuses. Dave, if you want to touch on that a little more, one of the primary drivers for that in the context of…

DAVID PISCITELLO: Yeah. So, we have a program that we deliver in conjunction with Europol and Interpol, and we also go to national law enforcement agencies that [inaudible], for example, the Austrian cyber competency or some agency like the national crime agency, various DOJ branches. And we do four to eight hours of training where we explain the identifier system, the DNS ecosystem.

We show investigative techniques that we've all practiced in our extended day jobs. We build a lot of relationships with, you know, with law enforcement through this, as long as the training. It facilitates some of the global activities that we have to get involved in as ICANN and the stakeholders, for example, the Avalanche take down or the [inaudible] takedown and the like.

So, it's a very popular course. I was the only one teaching it three years ago, and now we have someone who teaches it in Asia Pacific, someone who focuses on South America. I cover US and North America, and we're bringing in some trainer to cover Africa and Middle East. So, it's a lot of work, and it's very, very rewarding because we, we're helping in a sort of public interest perspective.

And I think that's extremely important for ICANN's optic, and also for combating all the use that we've been contending with.

DENISE MICHEL: Thank you, David. Noorul, then John and Patrick.

Kerry-Ann, did you have a follow-up question on this? Okay. Thank you. Sorry…

NOORUL AMEEN: Thank you. I think we are facing some issues for IDN look ups, generally if you [inaudible] for a domain or IP, generally [inaudible] databases. I don't know whether [inaudible], we didn't find a [inaudible] database of IDNs WHOIS. So, can anybody guide us how to get an exact information of exact WHOIS information for this IDN domains?

Because once you [inaudible] these things for a line which would be changed, then it's getting difficult to resolve a particular contact. Actually, we worked with the law enforcement agencies, the [inaudible] and all the other things. [Inaudible] for us to trace these kind of issues.

UNKNOWN SPEAKER: So, ICANN does have a WHOIS server, WHOIS dot ICANN dot org, that can be used, I believe, to look up the IDNs, they're basically all of the top level domains.

NOORUL AMEEN: [Inaudible], do you suggest like maximize database ICANN [inaudible]…

DAVID PISCITELLO: So, there is an effort to deploy a new system. That is R-DAP. That, at some point in the future, should provide that mechanism. Right now, the way the system works is each registry runs its own WHOIS server, and you just need to [inaudible] already knows where the WHOIS database is actually located.

So, there is a convention where we do, what is it? WHOIS dot nic dot top level domain. And that applies for all of the new gTLDs, and I believe all of the fast track IDN, but I'm not positive on that. Actually, Margie might… The requirements for the WHOIS on the ccs, fast track IDNs, was there a requirement? I don't remember.

EMILY TAYLOR: Dave, I might be able to help with this. So, my understanding is that in the moment, in the ICANN environment, WHOIS data is still has to be in the [inaudible] character set, so there isn't support for UTF-8 characters in the WHOIS. And that is work going on within working groups and translation and transliteration, and replacement of the WHOIS.

It's definitely an aspect that needs to be, you know, tidied up, if you like, in relation to IDNs, but they are also, I just wanted to make a kind of [inaudible] slightly higher level point is, I think that there is a piece for us around IDNs and universal acceptance, through the lens of the stability and resiliency and security of the system. Not just viewing IDNs, all for nothing, English is a first language view, [inaudible] attacks, or IDNs in the context of security threat, but I think there may also be just sort, I don't know whether this is the right time to mention it, but as it comes up in the conversation, it might be a piece for us to look at around what happens if universal acceptance doesn't advance sufficiently, a sufficient rate to include the next billions who are yet to come online.

Will they find alternatives and what will that do to the unique identifier system? I know that's a very big piece, and others in the room will no doubt be worried us kind of rambling off in different directions. But I just wanted to place a marker. I think there is something for us to do around universal acceptance.

DAVID PISCITELLO: One thing I did want to clarify, the conventions that are requirements contractual obligations obviously only apply to the contracted parties. So, the ccs, country code TLDs, have no requirement to even run a WHOIS server. I mean, the concept of requirement doesn't apply to them. There is no mechanism by which a requirement, ICANN community organization could impose on the ccs to do that sort of stuff.

NOORUL AMEEN: I mean, I'm sorry. Actually mention [inaudible] and service distractions. Actually I observed the first [inaudible] BGP prefix hijacking in 2012, [inaudible], maybe before that, it may be there, but I don't know. So, the internet traffic diverted through some countries. [Inaudible] and [inaudible] published some [inaudible].

So, my question is, did you address those specific issues in your review process, so you can come up with some solutions like BGP SEC as an implementation solution, and one more question. I see [inaudible]

2012. Did you think that in 2017, DNS will get abused for [inaudible] and implication in this manner that were clear [inaudible] of traffic?

DAVID PISCITELLO: So, with regards to the BGP SEC, I'm actually part of the initial implementation team, Patrick might know more about any thoughts that were discussed during the SSR one related to securing the routing system, but it's generally seen as outside of ICANN's scope.

What are role is in the context of addressing is to facilitate the development of the global policies, that may, stressing may, change with the deployment of PRKI, if that ever takes off, and there is a single trust anchor as the IAB has suggested as the appropriate way to deploy, but it is, to my understanding, it is not how RPK is currently being deployed.

But again, the implementation of BGP Sec is something that will be done by internet service providers, not is something that we would have very limited control over. The best we could do is help facilitate through these [inaudible] the RPK infrastructure.

[SPEAKER OFF MICROPHONE]

DENISE MICHEL: So, we haven't gotten to the slide on recommendations. [CROSSTALK] The questions are very fruitful, as is the discussion, I just want to remind people that we have a number of recommendations to get through in the next hour and 15 minutes, about.

DAVID PISCITELLO: With regards whether we foresaw the reflection attacks, and that sort of thing, I think anyone who has dealt with the DNS is aware of the Achille's heel of the EDP based protocols. The proliferation of open resolvers, I think, might have taken some by surprise. Just the myriad of open resolvers out there. But you know, even [inaudible] specifying DNSSEC, there were concerns raised that the increased packet size would allow for amplification attacks.

And that was back in the late '90s. And so, that is something that we knew would probably be haunting us in the future.

PATRICK JONES: I'll sort of add to what David had said, but also answer your question. While SSR one was meeting in 2012 as they were working to finish their recommendations, ICANN staff was in the process of rolling out the single, the new structure for running L root in the cloud system, and so we were already ramping up before the review team had finished its recommendations.

So, even at that time, we were taking steps to make sure that we had more capacity.

DENISE MICHEL: Karen, could you quickly bring us up to speed on the Adobe chat? And then I would like to ask people to keep their comments and questions as short and direct as possible. I have Kerry-Ann, then John, Patrick, Dave, Emily, and… Go ahead, Karen.

KAREN MULBERRY: Thank you very much. Some of the questions were posted in the chat early on in the conversation. So, it might have bypassed what they were trying to address. Anyway, Matogoro had a question on, do you have any KPI that one may assess on the implementation status of recommendation one from SSR one?

There is a comment from Ram on DNS and DNSSEC capacity building program in the APAC region is excellent. And then Ram also posted another question for discussion. What is the current status regarding deployment of RPKI? And that is all that they have posted in the chat in terms of the questions and comments and discussions.

UNKNOWN SPEAKER: So, with regards to the KPI [inaudible] implementation status of recommendation one on SSR. Each of the implementations of the recommendations were tracked during the implementation phase, which began back in 2012. I think [inaudible] may actually have information related to that, that we'll get to a bit later.

With regards to the question of the current status regarding the deployment of RPKI, actually, Alain may have more information, but my understanding right now is that there are a few operational pilots that have been deployed. LACNIC, I believe, actually set up a RPKI for their resources.

I don't know their status of ARIN. Cathy might be able to comment.

[SPEAKER OFF MICROPHONE]

CATHY HANDLEY: It's moving along. I can see what I can find out. I will find out, but I don't think it's totally…

UNKNOWN SPEAKER: In general, there is a… An IAB statement back, I don't remember exactly, quite a while ago, had suggested that the RPK higher hierarchy should follow the address allocation hierarchy, and there should be a single trust anchor housed at the, with the IANA to create a single rooted tree, similar in concept, at least, to the way DNSSEC has been deployed.

Single root trust anchor, and then the chain of the delegations of addressed base down to the [inaudible] nodes, through the RIR system. My understanding, and I'll admit not having followed this particularly closely recently, is that the current model of deployment is a multi-rooted tree forest of trust anchors, one each associated with the RIRs potentially with one at IANA, but it hasn't been established that…

And this… It would mean that the [inaudible] party would actually want to make use of the RPI, would have to deploy multiple, would have to configure multiple trust anchors, so five or six depending trust anchors in the software that would be doing the validations of this stuff.

There has been some pushback on the idea of deploying RPK, particularly in the RIPE region. Some concerns about the implications about deploying the RPK in sort of the power that it would give to the regional internet registries, or potentially IANA on a single rooted tree model. And some ISPs don't feel that that's appropriate. But as I said, there are pilots that are being deployed in various places that seem to work when they actually are used.

DENISE MICHEL: Thank you. Eric has a comment on this particular topic. John are you on another topic or this one?

[SPEAKER OFF MICROPHONE]

Okay. Eric?

ERIC OSTERWEIL: Yeah. Eric Osterweil. So, I've been sort of measuring my words on our PTI, I have spent quite a bit of time in that space. [Inaudible]. So, I just want to point out a couple of observations about it, and let people [inaudible]. So we talked about the web PTI, some of the disaster that that's wrought upon us because there are multiple roots, and our PTI is the exact same thing.

Without a global trust anchor, the RIRs are basically, I think a couple actually have put zero slash zero in the RPTI, which basically means they're all claiming to be authoritative for everything by default, which means that they can give conflicting answers, potentially.

And without a global root, it's not really clear who owns what address space. So, there is the exact same avenue for ambiguity, especially when we start doing [inaudible] and stuff, and blocks of IP addresses start changing regions. It isn't really clear where an address block should be attested to. And in addition to that, it doesn't actually address a lot of the fundamental concerns with things like route links, where somewhere can stick themselves in the man in the middle for BGP.

It doesn't address that at all. So, I mean, architecturally. So there is some concerns with that. Like I said, I've been trying to keep my mouth shut. It's now failing. But nevertheless, it certainly is good to see progress being made towards recertification in general, it's something that is desperately needed, but we probably want to be circumspect about considering RPK and [inaudible] to [inaudible].

UNKNOWN SPEAKER: And I'll also point out that in addition to Eric, another expert on RPK is a member of the review team that Jeff Houston, I guess, is at [inaudible] today.

DENISE MICHEL: Thank you. John and then Alain, quickly, and then we're going to move back to Negar so she can run through the slides.

JOHN CRAIN: I just wanted just a little bit of context on the capability building. So, this, the original capability building from ICANN goes back to conversations with myself and a gentlemen called [inaudible] had in early 2000s at some point, about the capabilities of operators of TLDs. There were very divergent from extremely well resourced type efficient operators, to those that have no resources and [inaudible] to get training.

So, the training is not just about abuse. It actually stems from a series that we call the registry operations courses, together with, in partnership with an organization called the network startup resource center, I believe, [inaudible]. And these were demand driven training. Mainly ccTLD operators were coming to us and saying help.

And we've… But those courses have ranged from the very basic of how do I configure a name server, I'm talking more than a decade ago now. And went through how do we monitor networks? To how do we disaster preparedness? So, not really a technical thing, but an actual… So, these are all things that we thought had a direct effect on the security, stability, and resiliency of the ecosystem, because these are operators in that.

So, I don't want people to get the idea that we're just doing like abuse things, there is also a lot of operational training. And we do a lot of these, either at the request of, or in cooperation with other organizations. For example, the TLD operators have regional organizations such as LACTLD, and those are the kind of organizations we try to partner with. And the best case scenario is that we've actually trained them to do the training because we're resource limited.

And we actually have a list of the kind of training so we can share with you if we've not already.

DENISE MICHEL: Thank you, John. A quick comment from David, and then Alain, and then we're going back to Negar.

DAVID CONRAD: Yeah, and just to add a little bit. A year and a half ago, we initiated, within ICANN meetings, a sort of capacity building thing called how it works. And with the exception of the policy forum, we have basically four sessions, two times during the ICANN meetings, and they talk anything from how the DNS works to how the root server system works, to how basic internet technology works.

And they're pretty popular.

DENISE MICHEL: Thank you. We're going to go back to the slides on the recommendations. [CROSSTALK]

KERRY-ANN BARRETT: I don't think you're seeing this side of the table. So, I want to highlight that sometimes it goes up, but I don't know what it is in terms of the [inaudible]. Suggest we can [inaudible] on this side as well, because my comment went up even before Alain did. So, I just wanted to see what the view that you have.

DENISE MICHEL: My apologies. Is there anyone else on comments that we…?

KERRY-ANN BARRETT: I did just have one thing to add. [Inaudible] I think it was relevant. Eric's explanation, I think, was pretty good comment. And I wanted to probably ask you directly, in terms of the… The statements you made in terms of… Because there are so many things going on, and who is actually going to be responsible for some of the… Where should we direct that concern to it's not within our remit, can we flag it as something for someone else's remit? On who do you think that would be…?

ERIC OSTERWEIL: Yes, so this is Eric again. So, I think you actually talked on it. You've made a formal recommendation that you're going to do recertification, and if you're going to do RPKI, it is… You have to have a global root. You simply have to. And I can't remember exactly what the language in the publication of the RFC was, but it was something like you basically…

Well, since you're going to be using this to unambiguously determine who is the rightful resource holder for something, it can't be ambiguous when you get, when you ask a system, and the only way to dis-ambiguate it is to have a root. That's authoritative for something at the top, and no one else can [inaudible].

And so, what you have now is you have five roots, and they always [inaudible] now starting to attest to being responsible for zero slash zero, which is the root of the address space. So, if you were to sort of say there needs to be a policy implication, you'd have to [inaudible]… I mean, the global root has been tried, and the RIRs didn't like it. They basically said, you can't make us do it.

But that would be what would have to happen. And so now Cathy is going to get up and kill me. But that… Okay. Bodily harm might come my way at some point, but yeah, so that's, I don't know if that clears up…

DENISE MICHEL: I think it raises more questions than it clears up. But definitely a very useful topic area to pick up after we run through these recommendations. Go ahead, James.

JAMES GANNON: James. Just really wanted to… The potential future role of the IANA, so functions operator would be that ecosystem is something that's within our remit as a future challenge and consideration.

DENISE MICHEL: Thank you, James. Cathy, did you have a comment?

CATHY HANDLEY: I'm not sure why, now I have my RIR hat on. Why this group…? Having been aware of the, what I would call perhaps, much less than positive discussions that went on over the topic, that Eric said, why do you want to bring that up to this team? Because I don't think this team has got the wherewithal to tell the RIRs what to do.

DENISE MICHEL: David, would you like to respond to that?

DAVID CONRAD: Sure. So, obviously, ICANN has a SSR 2 review, SSR one review, any of the reviews have no mechanism by which to instruct, or make recommendations to, the RIR system. However, in the context of RPKI, based on the IAB statement, there is a single root that is associated with the allocation hierarchy, which is rooted in the IANA, therefore the RPI would be in the IANA, so the one could conceivably see a mechanism by which a recommendation could be associated with that particular aspect, whether or not the RIRs listen, is…

CATHY HANDLEY: I would go on record immediately as recusing myself from that entire conversation.

DAVID CONRAD: And actually, what I would recommend just as a topic of interest, is there are two people, on the review team, who know this stuff better then pretty much anyone else on the planet. And it would actually be sort of entertaining to put them on opposite sides of the table, because Jeff has certain opinions, and I believe Eric might…

DENISE MICHEL: Go ahead, Eric.

ERIC OSTERWEIL: I guess, if you think that's worth doing, we can do that. I just wanted to point out that this is a really, this topic is a really slippery slope, because among the many criticisms that I've been a party to that I think is valid, one of them is that our PTI is fully deployed because essentially it could be a mechanism to control what's routed on the internet, period.

In other words, an entity could [inaudible] a routing blackout through policy at that point. And without a global route, that entity could be a different region in the world from where that resource is allocated and running, because there is no global route, so I could have a RIR take a, be forced to take an action that would effect a resource in another part of the world, by merit of fact that no one could prove where it was actually allocated.

But even if it was allocated in the right place, the system is designed to say, someone has made a policy statement that that block should be routed, and that is gone. So, we may want to consider this third rail as something we don't want to touch, or not.

DENISE MICHEL: All right. All right, so we have one last comment from Zarko, and then…

ZARKO KECIC: Just a short comment. Because there are two parallel things going on, RPKI and BGP SEC. So, which one will prevail? I think BGP SEC is more constructive. But I really don't know…

[SPEAKER OFF MICROPHONE]

ERIC OSTERWIL: They actually work together, so RPKI is about the resource certification and BGP SEC is about trying to [inaudible] control paths, and implement, use RPKI and then do a little bit more with it. So actually, they go hand in hand with each other. You could do RPKI without BGP SEC, and that's what the pilots are doing now.

Mostly is they're putting up route filters and stuff like that.

ZARKO KECIC: Yeah, but personally, I didn't study that, because I'm not doing routing as much. But my understanding is, there are some issues with RPKI, with BGP… [Inaudible]

But implementing BGP SEC will solve most of the problems with routing.

[CROSSTALK]

DENISE MICHEL: Yes, we've identified another issue for debate and exploration. So, with that, we're going to turn it back over to Negar for the slides.

NEGAR FARZINIA: Okay. So, back to SSR one implementation. Kerry-Ann, [inaudible] is the boom-boom list, that's for you. And I think because we've talked about it multiple times, if there are any questions or objections, we can move along to the following slide.

All right. John, would you mind giving us a very brief overview of some of the SSR related activities?

JOHN CRAIN: Okay. So, just to be clear, these are not all within my group, right? So we have a lot of SSR related activities across ICANN. We have an operation excellence program, one is for IANA and the other is for PTI are obviously, we want that to have operational excellence if we want it to be secure, stable, etc.

We have a HTI, there was a whole session on that here. And apparently you have one tomorrow. At some point, you will be ready to go through that again. We have actually quite a few measurement programs going on, to understand what's happening in the identifier system, not just [inaudible] but some of the [inaudible] that our research guys are doing. A lot of engagement, we talked about that.

That's not just training, that's also, or capability building, that's also providing subject matter expertise, my group and other groups throughout the organization, especially the technical folks work with our engagement folks, to provide subject matter expertise on related topics.

One of the things we've been trying to do is build what we call force multipliers, or by doing things like train the training programs. We worked with a, I guess it's an organization in Egypt called the DNS operation excellence center, to train people there so that we don't have to go through the expense and resources of sending our staff constantly.

That's having mixed success. One of the advantages that ICANN staff have here is that we're actually paid to do this. Often when you get volunteers from other parts of the industry, they may not have the resources from their bosses.

So, it's actually, it's a really good theoretical idea to do the training of actually implementing the use of those resources, turns out to be harder than we expected. And encouraging best practices and protocol deployment such as DNSSEC. We have a whole program around that. We've worked with many TLD operators, and ISPs, etc. to help understand how to do this.

And we have a link here of the point zero, the framework, which has a lot of this information in there. So, I would recommend that you all read the framework. I don't know if there are questions about specific things, got the idea that we're running out of time here.

DENISE MICHEL: Go ahead, David.

DAVID CONRAD: Just I wanted to highlight. John indicated the SSR activities are not entirely within the SSR group. One of the things just to keep in the back of your mind that there is this unfortunate name collision that's occurred between SSR as something that ICANN does, and the SSR group, the SSR stuff that occurs within ICANN has actually, sort of marbled throughout the entire organization stuff that some of that, a good portion of that, is done by the SSR group, but it's not exclusive to that group.

DENISE MICHEL: Thank you. Negar?

NEGAR FARZINNIA: Yes. And I would like to point out that throughout this presentation, we have, in short, to make that distinction by referring to ICANN, or after SSR. To identify what faults within John's team, versus what falls with the entire ICANN organization in terms of responsibility and remit. Okay. We've talked a lot about what ICANN needs to do in terms of SSR. Let's talk about what falls outside of our responsibilities, because I think this is a critical point. John, go ahead please.

JOHN CRAIN: Okay, so, I'm hoping everybody in this room knows that, not the police of the internet. All right? That is not our job. We do not generally take an operational role in combat, we may provide [inaudible] for example, to public safety officers, but we're not public safety officers. We're not kicking down doors, arresting people, things like that.

DENISE MICHEL: Hey John? Could you, as you run through this, clarify when you're talking about [octo] SSR? ICANN staff, ICANN organization.

JOHN CRAIN: Yeah. I think this is across all of those, although you might argue, when you talk about the community, there are, of course, elements in the community that do some of these things. If we talk about combating criminal behavior, obviously, we have public safety working group, which has law enforcement members. So, but certainly, for staff and the organization, we don't have that role.

DENISE MICHEL: So, this particular slide relates to the ICANN staff, specifically not the community groups, okay.

JOHN CRAIN: At least not individuals within the roles. For example, as some of these, I don't think ICANN as a community has a role either, probably. People may disagree with me. We're talking about cyber warfare and espionage, but I would argue there isn't a working group inside of ICANN that's working on that, that I know of. Then again, maybe we wouldn't know if…

DENISE MICHEL: It would be useful to be more specific on this slide, that we're going to use as sort of a background resource.

JOHN CRAIN: Yeah, okay.

Let me finish, and then… So, ICANN does not have a role in determining what constitutes illicit conduct. Obviously, there are laws and things around that, [inaudible] agencies, that's now what ICANN does. And we have to remind people, because people sometimes forget this, we don't operate all of the infrastructure.

There are a lot of people out there that think that ICANN run the internet, or ICANN run the DNS, and we don't. You know, we happen to run a root server, and we run the infrastructure that enables our operational functions, but we don't run the core infrastructure. I think these are mainly things that speak for themselves, but we like to [inaudible] in case people are mistaken.

DENISE MICHEL: Thank you. Kerry-Ann.

KERRY-ANN BARRETT: [Inaudible] you put it, so… I just wanted to put [inaudible] just to see for all of our common understanding. ICANN is an entity. So for only the purposes of every time we have to say ICANN community versus ICANN, I don't know if it's necessary to be honest, because ICANN is a registered entity, and we speak of ICANN's role for the purposes of SSR team, it has to be ICANN the entity, because the community focus is huge.

So, I just want to say for ICANN is registered, [inaudible] everywhere. ICANN not the community, ICANN not the community, we're actually challenging our work going forward, so if we want to see if we, if it's necessary, or what [inaudible] when you said it.

DENISE MICHEL: I think specifically when we're talking about, we're talking about our job, to assess the effectiveness of the implementation of the SSR one recommendations, and their impact. It's important, I think, for the team to understand the role that the staff played in this. The role that the specific groups in the ICANN community played in this. And whether or not it's within the, elements are within the remit of ICANN. In other words, if you were assessing the effectiveness or the impact, and particularly for those who haven't been involved for ICANN for very long, I think it's important to understand staff has a specific role and ability to impact a certain set of activities, different elements in the community like the RIRs, RSSAC, SSAC, have a defined role and an ability to impact.

And when we're addressing effectiveness and impact, I think it's just a background. It's important for the team to understand those distinctions. Does that answer your question?

UNKNOWN SPEAKER: As somebody who has been at ICANN staff since sometime in the 1800s, it feels like, these distinctions can be important. And when you're talking to people like [inaudible], we forget to mention them because they're sort of in the back of our heads, so sometimes calling out the distinctions can be very important.

You don't have to do it all of the time, I agree, but you should always be able to ask about that distinction, because it is important.

KERRY-ANN BARRETT: [Inaudible] I keep thinking about subcommittee level, when we actually begin to write, if these distinctions are important, meaning at the subcommittee level when we start to write, it will [inaudible] because when we put the report back together, we're talking about different things, it will impact the target of the recommendation.

So, that's the only reason why I asked for the distinction because it came up, and I was just wondering how important it was. So, just for the record.

DENISE MICHEL: That was a useful classification, thank you. And John, I mean, excuse me, James and then John. You're done? James.

JAMES GANNON: Yes, just for context of the team, and even staff… I believe now the convention is the three different units within ICANN. There is the ICANN Board, the ICANN organization, and the ICANN community. So, when we're building our report, that's the terminology that I hope we'll be aiming at.

DENISE MICHEL: Thank you, that's useful.

Sorry, was there another question? And I apologize if I missed someone's hand. Please don't hesitate to correct me. Matogoro has a, go ahead Karen.

KAREN MULBERRY: Yes. Karen Mulberry for the chat and Adobe connect room. Matogoro has a comment. I'm also confused on ICANN as an organization, ICANN community, ICANN SSR.

DENISE MICHEL: I'll give it a shot. [CROSSTALK]

Thank you. Negar.

NEGAR FARZINNIA: Okay. So, [inaudible] addressed how security, stability, and resiliency fits into ICANN's functional areas, the comments for the team. Any questions on this slide? Or would you like us to cover this again?

DENISE MICHEL: I think we're good, go ahead.

NEGAR FARZINNIA: Okay. And with that, we finished with one recommendation, recommendation number 18. SSR framework was a big one. So, recommendation 18 is asking ICANN to conduct an annual operational review of its progress in implementing a SSR framework, and include this assessment as a component of the following year's SSR framework. As we have noted before, SSR framework has not been published annually, and every new framework that is published tracks progress of the commitments made in the previous framework in the new version of the document that's been published, which allows for tracking of the commitments made.

And the components are also included in our strategic plan, which rolls into our next slide. The five major items in the strategic plan have been noted here, for reference, and to break that balance a little further for the team, we have identified SSR related KPI's in the strategic plan, all of the updates related to these items are on ICANN org's web page. And we're happy to answer any questions when you look through them, if there is any. Okay?

With that said, we're moving on to slide number 19, or recommendation number 19, and this is just asking ICANN that allows the community to track the implementation of SSR framework, for it to be provided with enough clarity that the community can track the execution of the SSR responsibilities, and as is stated in the previous recommendation, every new annual SSR framework that is published, is tracking the commitments made in the previous SSR framework.

And that's available publicly for everyone to look at. The link you see on this slide points to the [inaudible]… All right. We can move on to the next topic, which is ICANN's SSR role and remit within its limited mission. And that brings up to recommendation number 24, which is asking for ICANN to clearly define the charter roles and responsibilities of the chief security officer's team.

And with that, John, I turn it over to you.

JOHN CRAIN: So, interestingly, we don't actually have a security officers team, or we didn't at this point. It's not the terminology we used, right? So, we actually have, I'd say there is really two areas, functional areas inside the organization that deal with most of the, at least the technical SSR areas, and that's [octo]. We're going to do SSR separately, because it was at this point, when this was written, but now, of course [inaudible] SSR [inaudible] and there is our CIO office, our Chief Information Officer, Ashwin.

And we work together very closely. So, there are various processes inside. For example, if we have a SSR issue, we actually have an internal start, and we have members of both teams in it, etc. So, our collaboration is, I would say, on a daily basis, we offer expertise. We offer operational capabilities in the case of crisis, etc.

So, you know, I don't know if I would be able to point to a clearly defined document that documents all of this. I don't know if you're aware of one, David, but it's all there. We have internal documents, how the cert works, etc. I believe there is actually [inaudible]. Unfortunately, Patrick had to leave. Patrick would probably know when it was written, in fact, he may have even written it.

But yeah, we'll have to get back to him on that.

DENISE MICHEL: The document on what?

JOHN CRAIN: On whether there is actual framework on how that direction works.

NEGAR FARZINNIA: Moving on to the next slide, it is to discuss the vision and mission of ICANN SSRT as defined today, not at the time the last [inaudible] was written. John, go ahead please.

JOHN CRAIN: So, really, okay. I don't have my glasses on. That's a slightly difference… Okay, you have [inaudible]… I have an extra slide in my slide deck here. So, the basic concept that we work on is that we work in partnership with the community. You know, our vision is really to be a trusted partner, to work with people in the industry, and by doing that, to enhance or ensure the SSR of the system.

We have a mission statement that we use. There is actually [inaudible] we're about to preserve. We use different words again. The security, stability, and resiliency internet system of unique identifiers that ICANN helps coordinate to promote user confidence interest in these systems, and to strengthen these systems for capability building and the communities ICANN serves.

I hope that talks for itself. So, you know, some of the things we're doing here is, we talked about the SMEs, we talked about research, we talked about just basically trying to improve the knowledge, and improve the understanding, because we believe this should then filter into the policy processes.

I'm a strong believer you make better policy if you are better informed, and part of that is data. We've been doing a lot of these trainings that we talked about, a lot of this already. We also write a lot of documents. We publish a lot of blogs. We're in the process of writing a series of white papers, so disseminating information to the community and to the policy makers, and diverse as a trusted partner.

And all of this, hopefully, makes the system work better. I mean, that in the end, is the end goal to have a system that is secure, stable, and resilient. I mean, that's what it says in the bylaws, and that's what we aim for. And we do this in collaboration, not just with the research guides from also, but all of the various staff and community groups that we work with.

We're very much about collaboration, because we're a small group, and as we said before, ICANN doesn't actually operate most of this stuff. So, collaboration is our key.

DENISE MICHEL: I think we have a question. Kerry-Ann.

KERRY-ANN BARRETT: Just a quick one. I had taken note when we distinguished that [octo] is not responsible for doing what ICANN is [inaudible] which is the SSR. When I have gone [inaudible] with the research, and I looked at the mission, and the mission says exactly that. So, I'm just wondering , if it's the mission says that, but yet, we're seeing that the distinction that you do not do that, and that's where it says that, then how will the community [inaudible]… distinction, because the mission to me is to be a trusted partner and collaborate efforts to ensure…

So, the language is strong in the mission to ensure, is the exact language.

JOHN CRAIN: So, I think what we talked about as a group, yes, that is ICANN's mission, so it's also our mission, but it's just not our mission. Not everything is done to improve that [inaudible], but it is…

KERRY-ANN BARRETT: But just a suggestion, in terms of when you do have your strategic review committee, weekend, [inaudible] probably just put something before ensure, like to contribute to the ensuring off to, but it puts a word, I think you can probably should just put a little word before the ensure, because it goes straight into to ensure, and that will put an extra burden on your office.

JOHN CRAIN: Okay, noted.

NEGAR FARZINNIA: I think this actually rolls into the next slide, which you already spoke to. And Karen, go ahead.

KAREN MULBERRY: Yes, there was a comment in the chat by Matogoro. Actually, it's a question. To what extent does [octo] SSR mission envision is realized in Africa?

JOHN CRAIN: So, we work with a lot of organizations, like we collaborate, that's what we do a lot. So, we don't have a dedicated staff person for that reason at the moment, so it tends to be shared amongst us. We do work with AFTLD, we have connections with AfriNIC. We've worked with law enforcement in the region. I mean, we work globally, so it's not that we distinguish one area against the other.

So, we are active in Africa. I think we may be more active in some other regions. One of the reasons for that is we've done a lot of trainer to trainer work in Africa, especially for AFTLD and [inaudible], so in many ways, there is more local resources there. So, we all support those resources, but a lot of the training, I think, that the knowledge is actually being given by local people such as Alain here, who has worked for NSRC and we've worked with other the years.

So, we are active in Africa. It's just a slightly different mechanism because we, in some ways we're further along there on the trainer to trainer programs.

UNKNOWN SPEAKER: I'll just add, in the context of Africa, we have been involved… There was a workshop a couple of months ago, between the, for the GAC public safety working group and the lesser developed countries working group, and they held a workshop in Nairobi, a three day workshop that [octo] SSR presented at similarly just currently in the planning stages, but just prior to the ICANN meeting in Johannesburg that will be, there is plan, works underway, a plan for another sort of similar workshop for the Southern Africa.

NEGAR FARZINNIA: Okay. So, moving on to recommendation number four, ICANN should document and clearly define the nature of the SSR relationships it has within the ICANN community, in order to provide a single, focal point for understanding the interdependencies between organizations. So, this has been done via multiple channels. We have MOUs in place that have been incorporated as part of the agreements.

We have several links in place for ICANN security resource locator development, and a document that we just recently published in January of 2017, that identifies, in detail, all the relationships. And the next slide actually provides the link to all of this information can be found.

These documents will be updated, especially the ICANN SSR relationship. That document will be updated annually, and is available for everyone's reference. If you have any follow-up questions later on, what's going through them, please feel free to let us know.

And with that, we'll move on to recommendation five. Asking ICANN to use the definition of SSR relationships to maintain effective working relationships to demonstrate how these relationships are utilized with each SSR goal. And again, we are doing this in two ways. We have our key relationships the result of the recommendation prior to this recommendation number four, and the document that has been published and to be updated and maintained annually.

And we're also tracking all of the work in the KPIs that we have in our strategic plan. And for reference, I've included the table of the KPIs you've identified that are SSR related for future reference. The next segment we're going to go into, is SSR community outreach and information sharing, as well as security threats and mitigation.

And we have talked about this question also in that, so hopefully we have covered most of it. Recommendation number 14, asking ICANN to ensure its SSR related outreach activities, continuously evolve to remain relevant, timely and appropriate. And the feedback from community should provide a mechanism to review and increase this relevance. The next couple of slides are information that we have included in the SSR framework, the last time it was published.

So, some of these events and outreach activities are out of date, however, John and David covered these engagement sessions for the current time in the previous discussions. So, I believe we can move forward. Again, [inaudible] we've discussed this. This is a framework for reference, if further information is needed.

And the list of events and activities supported by [octo] SSR, this has also been discussed before. If there are no questions, we can move on. And with that, we'll go into recommendation 15. I do want to point out, this is one recommendation that is a great example of a measurable, achievable, and implementable recommendation from staff's perspective. So, something to keep in mind.

EMILY TAYLOR: Sorry, I am aware of time and that you've got a lot to get through, but just a question on the outreach and training programming, which really, I can tell by the way you describe it, and having the plans that you circulated, the feedback that you get from people who received it is incredibly positive. To what extent are you able to be proactive and, you know, rather than reactive to, you know, requests for training?

In other words, my sense, I don't know if this is correct, there is obviously a resource constraint, and I think it brings in Matogoro's question as well. You know, with a plan, and a strategy, that could then be fully funded, you could go well, we're going to be doing this in Africa, this in this region, this targeting this stakeholder group where we see a particular need.

To what extent are you able to do that level of planning and proactive engagement? I suppose it's a [inaudible] question too.

STEVE CONTE: This is Steve Conte. If I may take that. I think you can ask any number of [octo] generally, but specifically that they all, everyone gets, you know, it's very heartfelt to think about getting up in front of people and do training, and share that knowledge. I think you nailed it in some respects, that we are very resource driven, and have sounded very…

It's difficult to put the successive training into a KPI into a pretty graph, especially when you're looking at a long-term investment, where you're trying to share knowledge with an individual who might not necessarily express that knowledge until a later date. So, trying to get adequate resources to be proactive is very difficult. And then a couple of other factors around that too is that as a team, and a department were question, because of limited resources, we have to be, we have to act on the request and an aspect of that.

Those requests come from the reasonable strategies of a global stakeholder group. So, various vice-presidents of global stakeholder groups. So, collaborate with the region, work out what the regional strategies are, and based on that, tend to, will come to [octo] SSR to make the requests to do different strategies.

So, although John might have his own idea of what a perfect world looks like, and his strategy with SSR because we are a partner, department with our primary internal stakeholder being the GSE department, the Global Stakeholder Engagement department, we limit and try to align our activities with their mission. And James, your card is up, so if you want to add to that?

JAMES GANNON: I think that's pretty good. What we do, there are some things that we have in place. So, for example, we try and plan around a six month process, minimum of three months before we'll go in and engage, so that we can actually plan and control our resources. We try and conjoin efforts so that we're out doing training, we're also doing outreach. We also work with our government engagement folks, and areas of the organization.

So, we're very much a resource for the organization and the community. Unfortunately, a lot of the planning is around what we can't do. Right? That's just the reality…

DENISE MICHEL: In terms of resource availability?

JAMES GANNON: Resource availability [CROSSTALK]. Yeah, I mean, occasionally, we'll get things outside the mission, but it's very rare. It's really nearly always resource issues, and frankly, I want my staff to have a life outside of ICANN. And most of them don't like to say no, they love doing this, so they're all running at full speed. So, a lot of the issue is trying to figure out how much we can do, and then one of the priorities. We don't get to set all of the priorities, because they do come from GSE and other areas in the organization and the community.

DENISE MICHEL: We've got Dave, and then David, and then Emily.

DAVID CONRAD: Yeah, just to point out that, actually [inaudible] with a lot of these discussions internally within the organization. Government engagement, global stakeholder engagement, [inaudible] and policy are all working on coming up with a better strategy by which we can manage the requests that we get for capacity building and other related training.

And that's an ongoing internal effort of just trying to figure out a better way of utilizing resources more effectively.

DENISE MICHEL: Thank you, David.

DAVID PISCITELLO: Dave Piscitello. There are a couple of other ways we need to look at training. [Inaudible] generally does not have travel budget. You know, and so we have to go to them. In some cases, there are well funded enough where they can provide an interpreter, and in some cases they cannot. And so language is absolutely a constraint. Yeah. Not that I expect ICANN to be able to provide a translator every time we go to a country, but I think there are countries where that might be valuable.

We do work with the major pol agencies, Interpol and Europol, and [inaudible] pol actually contacted us. And we do work closely with GSEs, so that what we can do is try to hit as many places regionally as possible. So, for example, I'm going to [inaudible] and Warsaw and Vienna in eight days.

That's better, but budget wise and travel wise for us. So, we try to economize to the extent possible. But being proactive, one of the best ways for us to be proactive is to go, be invited to a law enforcement conference, where we talked about what we do and we see we have the expertise, and then they come up to us. So, we actually end up being like a military recruiting opportunity in front of a gymnasium, right?

If we had more money, and we had more people, we could easily do double what we do. In fact, we've been, since I started this, we've been increasing about 50 to 60% each year over four years. So, the consumption rate exceeds our ability to deliver.

EMILY TAYLOR: Thank you very much. I've got some more thoughts around that, but we have a section after lunch, so I won't hold up the presentation.

DENISE MICHEL: Okay, thank you. And can I get a… We have Kerry-Ann in the queue as well as myself. Can we get [inaudible] from staff, whether we have the ability to take some of our time right after lunch to finish the presentation on some of these recommendations? What's staff availability for the next two hours on this? Yeah?

UNKNOWN SPEAKER: I'll make myself available.

DENISE MICHEL: Okay, great. So, if we need to extend our time with you on this, we can. Thank you.

NEGAR FARZINNIA: And just one quick highlight. We have very few slides left. We are nearing the end of the presentation we've prepared.

DENISE MICHEL: Great. Question. So, I mean, it strikes me that many of the entities that maybe in most need of the training and expertise that can be provided by ICANN staff, are the same entities that can't afford to send people to a number of ICANN events, or take time to participate in the global strategy framework development process that identifies the needs in the region, that then influences how SSR staff spends its resources on training? I'd appreciate some additional insight into that. How do you get around that?

UNKNOWN SPEAKER: And so, part of, in the context of GSE, the regional vice-presidents who are responsible for representing their regions. They are the ones that actually do the outreach to various groups, various entities within the regions and [inaudible] requests back up into GSE global, which then contacts us, which… So, that's the theoretical change. Pragmatically speaking, the context of like capacity building law enforcement.

The law enforcement guys talk to each other, and then, yeah, they do references, end up calling Dave, probably at his home when he's sleeping and we, yeah, something like that. It's more informal, you know, and that's one of the things why, one of the reasons why GSE [inaudible] policy and [octo] to come up with a better process by which to basically in take requests that are generated by the regional vice-presidents and the groups that they represent and bring them back up.

And John might have additional comments there.

DENISE MICHEL: That's quite a concerning bureaucratic oriented process. I would like more information about that. What you described is a need quite outside the very small limited community of who attends ICANN meetings, who knows the global stakeholder contact in each region. But I'll save this discussion for another time. Go ahead.

UNKNOWN SPEAKER: It actually works well in some regions, and doesn't work quite so well in others. It has to do with the nature of the relationships of the countries and the region. And whether they compete or cooperate in some cases, has to do with the energy of all of the people involved. But one of the problems I didn't mention before that is really one of the biggest challenges in trying to do something as comprehensive as cyber investigations is, training the trainers is not enough.

You have to have the people who have the practical operational security experience, who do this, you know, 20 hours a day in some cases. And there aren't a lot of people who have that. And so, we can go into a country, but if… And if anything happens with people we train, if we're not doing it every day, you know, in two weeks they're going to lose 80% of what we've trained.

And so, we always see some people rise and become stars. And that's because they're constantly working with law enforcement. But you know, probably as often as you see anyone else training and becoming impassioned by it. But it takes multiple months and successes training just to train inside our organization, and even then, we need to understand how to allocate time for people to do what John and I do.

You know, which is work with people all day long, on weekends, wherever it is that they have the need. So, it's a very, very hard group to populate and to sustain.

JOHN CRAIN: And if I can bring this back to the division of being an interested partner. These trainings are not just about passing out the information, they're also about relationship building. So, you know, that's why they are so important. This is where, one of the places where we build trust. And the fact that we can even do these, is actually, in some ways, a self-fulfilling, I hate the word KPI, but a self-fulfilling indicator that [inaudible] building, something that we've been in for way over a decade.

And you are correct about the issue of attendance because of the same funding issues that does not allow them to get this training, that does not allow them to participate. But having said that, and being an old geezer who has been in this for a while, we actually have a public safety working group now.

We actually have people coming and participating. We didn't have that 10 years ago. And that was something that we worked on, that was to bring these people into the community. And it takes time, and it takes resources. You know, there is never enough no matter what job you do.

So, I'm not complaining about the resources, because nobody has enough. That's just life.

But it is long-term. It's not we go in, we give a week training, and everything is done. This is about relationship building and it's very long-term. And once again, it builds back into the policy process by bringing them into the fold.

DENISE MICHEL: Thank you, John. Karen has something from Adobe. Emily, did that…?

[SPEAKER OFF MICROPHONE]

I'm happy to accommodate either direction. And Dave Piscitello, do you still have yours up on purpose? Okay. Karen.

KAREN MULBERRY: Thank you very much. Matogoro had a comment in the chatroom. And [inaudible] but I think it's more of a question for you. Do you have engagement with academic community? Which sometimes has an unlimited budget.

DAVID CONRAD: Unlimited, but I think, not… The answer is yes. We do work with academia. We go to university. I'm actually planning something in a couple of weeks [inaudible] going to come to with Oxford at Cambridge. Every time we go on one of these trips, we just do the one training. We say, who can we reach out to? And that would include academia.

So, yes, absolutely, there are one of our strong partners. This is where GSC actually does help us quite a bit. So, when we visit for training, we often get an opportunity to do a seminar at a local university. And they're generally exceptionally well-attended.

DENISE MICHEL: Thank you. Kerry-Ann?

KERRY-ANN BARRETT: [Inaudible] but I wanted it to be like a specific item on the AOB later. Is there any way in terms of [inaudible]… is TFC as in terms of how we actually establish a more permanent solution to this training and outreach capacity building?

Because it's something that I think is second to last point, it's very critical. So, I pigeonhole as a specific topic on the AOB.

DENISE MICHEL: Thank you. Were there any follow-up comments from staff on that? Are we really ready to move?

UNKNOWN SPEAKER: You should probably add them to the list of people you wanted to talk to if they're not on it.

DENISE MICHEL: Thank you.

NEGAR FARZINNIA: Okay. So, recommendation 15, asking ICANN to act as facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques. We've addressed it in two ways. By working in a coordinated vulnerability disclosure document, and by collaborating [inaudible] and trust security community entities on DNS security threats and mitigation techniques.

And on that first item, I will turn it over to John. Could you forward the slide please? The remote is not working. The next slide is, no, the one before this.

So, John if you could talk to the coordinated vulnerability disclosure reporting at ICANN, please.

JOHN GANNON: [Inaudible] I'm getting old by the way. I turned 50 some years ago. So, we actually have a process for this. It has been used a few times. We've actually talked about this earlier. The one that's probably got the most visibility that we had this, was something called [inaudible], which was around the name collisions. And I think it was one of the, we've also had a couple of DNS resolver bugs that we passed forward.

And what this does is it allows people to come to us with problems when they don't have the capability of getting to the platform provider or the software provider themselves. It works. You know, [inaudible] was a case of that. Vulnerability disclosure is a very interesting area, because there is a lot of…

It's not always done correctly. Especially researchers sometimes like to go and publish things. So, if we take [inaudible] as an example, there was a lot of pressure for us to release data that would have given visibility into that bug. We actually managed to sit on that for over a year, and I think the Microsoft guys were rather shocked, because the process worked. We can actually sit on a vulnerability and disclose it in a coordinated fashion in a responsible manner.

That's all I can really say about that. I mean, it actually works. It's not our key roll, but if something comes up to us, we have the mechanisms in place, and we've practiced them and they worked, which I thought was kind of awesome because a lot of times they don't.

DENISE MICHEL: Can I ask a quick question? So, in considering our ability, I guess, collective ability to proactively prepare for a draft vulnerabilities or attacks, is there some…? Does ICANN troll the dark web for things like the attack that is sweeping the world right now and was solved by the registration of a single domain name?

UNKNOWN SPEAKER: [Inaudible] that's interesting. Anyway, we are… So, the dark web is one thing, and it's one of those, it's actually ones that people like to talk about. But the way the operational security community works is through trust relationships, and trust platforms, and ICANN staff specifically, in the [octo] group, not just SSR but also in the research group, are members of most of those platforms.

I believe Facebook may have a platform, and we may be on that too. But I wouldn't be able to speak to that. So yes, we are involved, we're constantly trying to be aware of things. If people have things that they want to us help disclose, we can do that. More often, they may be coming to us for expertise, or data points.

We have the ability to do that insecure manners. Why disclosure? A lot of the times, they're not all vulnerabilities. So, it's not our job to do the disclosure, the public disclosure. We normally sit in there as… Either the effective party will report it to the person owning the code, if it's a code issue, so there will be a report, but we won't necessarily disclose it to the public. Or at least not without coordination.

If you look at [inaudible], we did make some statements, but it was in very close coordination with the OS operator. So, we are heavily involved in those platforms.

EMILY TAYLOR: Could I just do a quick housekeeping thing to remind people to announce their name? Because I think the people following remotely and doing the transcript are tearing their hair out.

DENISE MICHEL: Thank you, Emily. This is Denise. Alain.

Sorry. I like this side so much better. I'm sorry.

I apologize. So, first James an then Alain. James.

JAMES GANNON: Thank you. James Gannon. So, looking a bit forward, have you guys thought about doing [inaudible] 29 47, and for context for other [inaudible] members, the world of coordinated vulnerability disclosure has changed a lot over the last few years. There has been a huge amount of work that's been involved in, and you know, it really has evolved from the point that this recommendation was put in, and my personal opinion, to where ICANN stands at the moment within the role of [inaudible].

So, have you looked at that? Is that something that has been on your radar? Is that something that we should be, you know, fleshing out as well but as part of our work?

UNKNOWN SPEAKER: So, I regularly look at the idea of certification like [inaudible] etc. I think the decision of whether or not to do that, that they would talk to more about that probably [inaudible] which is a lot of expense involved in these kinds of things. We follow of the norms, but that's different from certification.

DAVID PISCITELLO: So, we actually do have a relationship with… I'm sorry. Dave Piscitello. We have a relationship with [inaudible] and so, if you attend, if you're a law enforcement person and you have a CSSID, you get continuing education units. So.

UNKNOWN SPEAKER: So, yes, we know the norms. We try and follow best practices. There is always a question of which one, but the question I think was also doing certification, which is a whole different question. Yeah. That's an interesting thing, maybe, you think about whether we should whether or not…

DENISE MICHEL: David Conrad, do you have anything before we move to the next? Okay. We have Alain, and then Karen for the Adobe Chat comments. Alain?

ALAIN PATRICK AINA: This is Alain Aina. I think one of the goals of this session is to understand the implementation of this recommendation. Okay, at the end of the day, we can discuss and say what we think about this [inaudible], but we want to agree, use accommodation has been implemented, and how we [inaudible].

Some of the recommendations are very [inaudible], so make it different to implement [inaudible]. But I'm expecting that staff should tell us, before they implement, what was the staff understanding? What were the limits? To allow us to [inaudible] the implementation. For this recommendation, I can see is completed. How are we going to measure these things? It's complicated.

The recommendation is about ICANN [inaudible] responsible disclosure and dissemination of DNS? How are you going to measure these things to say that 15 has been implemented and we're good?

DENISE MICHEL: Thank you, Alain. We have David and John, I think, for answers, and then we have James, Karen and then James.

DAVID CONRAD: Just directly. I think at the very first meeting in Copenhagen, one of the things that I did, I don't want to say [inaudible], asked strenuously, is that when you develop recommendations, that the clear and actionable… And my experience with SSR one, a lot of the recommendations were unfortunately vague and ambiguous. They didn't, they weren't sort of actionable in sort of the smart sense, right?

So, in, you know, we're happy to provide what we recall, because remember, that this is five years back, what the status quo was to sort of explain to you sort of how things work to how they are now. And this actually, I believe, addresses Mr. Matogoro's question.

The… What has changed after the implementation recommendation 15, before recommendation 15 we did have a, I guess, an uncoordinated, undocumented mechanism by which people could, they call up John or call up Dave and say, here is an issue. And then things would happen the right way.

With the documentation of that process, that actually made it easier for folks to take advantage of it. We could point them to it, they could, the rules were much clearer, so it actually facilitated greater communication and more ease of implementation of that. But it didn't actually change the number of vulnerabilities or anything like that, obviously.

So, I hope that answers the question. With regard to the other ones, there are specific interests that the review teams on sort of how things were before the implementation of the recommendations, just let us know and we can try to figure it out, to track down people who have since retired.

DENISE MICHEL: Karen, do we have Adobe Connect contributions?

KAREN MULBERRY: Yes. It was actually from Matogoro. David read what he had in the chatroom.

DENISE MICHEL: All right, James.

JAMES GANNON: James Gannon. There [inaudible] to make now with regards to reviewing SSR one and it's something that's very [inaudible] through the review team. Security moves very quickly, and the review team was five years ago. There is an additional element I think we need to add to smart when we're writing our recommendations, which is [inaudible]. We need to fix them in the plan that we're making them, because for example, let's take this one that we have in front of us.

Doing coordinated vulnerability disclosure and building a policy around that five years ago is extremely different to what it is right now. So, when we're assessing these recommendations, we need to take them into context of when they were made. So, I would say that this was implemented well, as of when it was implemented. Not necessarily as we would if we were assessing it as a recommendation that was being made today.

That's just something to keep in the back of your mind when we're reviewing, and also when we're building our recommendations going forward.

DENISE MICHEL: Yes, excellent point. Other comments before we turn it back to Negar? Did I miss anyone on this side? All right. Back to my favorite side.

NEGAR FARZINNIA: All right. So, I'm so glad I'm on your favorite side. [Inaudible] recommendations.

Well, this just means I can get through the slides and finish the implementation. So, the next topic that addresses recommendation 15 is referring to identifier system, attack, mitigation methodology, and Mr. Dave Piscitello, please tell us a little bit about this.

DAVID PISCITELLO: I'm sorry. This is Dave. I spoke about this earlier. Do we need any more detail?

UNKNOWN SPEAKER: Actually, Dave, you said you would be talking about it later.

DAVID PISCITELLO: This is practicing social engineering, and you're all so smart but you didn't fall for it. So, part of the response to the recommendation. We sat down and we decided that any type that ICANN staff would have in trying to not only identify but take the lead in identifying remedies for a number of globally perceived threats against identifier systems, would not fare any better than the DNS cert.

So, we took a different tact. What we proposed is that the community work towards coming up with some recommended practices and some assessments of the threat landscape. And in this mitigation framework, we identified 10 of the threats that seem to be the most visible. And so, the idea is to have the community work in conjunction with staff, if that's their chance, in developing what we've loosely called tech notes.

And the tech notes would cover, in fact, the threats that I mentioned earlier, DNSSEC exploitation, or DNS server exploitation, DNS DDOS, route insertion, attacks against web services, registration service attacks. Attacks against DNS zone files, or authoritative servers, power roots, DNS surveillance and covert channels.

So, you know, the implementation of this is going to require some community participation, and community selection of which of these they have as a priority, it would be very difficult to do all 10 of these in one year. So, I expect that there will be a multi-year activity that has to be brought to the attention of the community that has probably not read the attack mitigation framework.

So, I think that pretty much summarizes what the purpose of the framework is, and I think it would be worthwhile for the review team to figure out how we actually kickstart this.

DENISE MICHEL: Could you…? This is Denise. Could you speak a little bit more about how the identifier system attack mitigation methodology report and the tech notes, have been socialized throughout the community and discussed, and what impacts they've had to date?

DAVID PISCITELLO: So, honestly, I can't, because once I finished writing it, which was almost nine months before it was published, I was moving on to my day job.

DENISE MICHEL: Who can speak to that?

DAVID PISCITELLO: It would be the NSSI team, I think.

NEGAR FARZINNIA: This is Negar. The actual report identifier system attack mitigation [inaudible] from the date on the document was just published February of this year. It has been posted publicly. It has not been posted for public comment or anything like that as, that was not a requirement that was identified at the time. This is a living document, and it is meant to be kept updated over time, as requirements, of course, for mitigation, attack mitigation changes over time.

DENISE MICHEL: This is Denise again. So, what I'm trying to understand is, why did it take five years to write this report? And how has it actually impacted the relevant activities of ICANN organization and ICANN community groups?

DAVID PISCITELLO: So, the question regarding the timing, not entirely sure. I know ICANN outsourced, Dave worked with someone else, his name, I'm forgetting, but to develop the document. Then it got a significant delay going through the approval chain, mostly because it was my fault, in my inbox and just sat there for quite a long time, because I had too many other things.

And then, I guess, it was published, the intent of the document wasn't, it wasn't seen as a policy statement in any form, it was intended primarily just to be a, just an informational document that didn't go through any formal review or anything like that by the community. I don't know if that answers your question.

DENISE MICHEL: Thank you. And I should have clarified. The nature of my question was to identify, was to ask if there was any substantive, you know, issues in development, or evolution of this report, or if there was anything else we should be aware of that contributed to when and how the report was developed, and I wasn't seeking, you know, public comment or review, but rather I wanted to understand how the substance of the report and the tech notes, which seemed really very valuable actually to both ICANN the organization and the community broadly, how that is being integrated into the work.

I think that was the nature of my question.

DAVID PISCITELLO: So, I guess, internally that document is used in the context of IT, and within sort of the operational side of the organization as just as reference material. There is nothing formal, no formal application of it. It wasn't really intended to be something that people would abide by more, just, you know, here are some ideas, here some approaches, here are ways of doing things.

Beyond that, I mean, I think the document, I think as Negar mentioned, is intended to be frequently revised and updated, just based on the new threats that come in, the new mitigations of those threats. So, it's part of the sort of the yearly review that we do SSA with the framework.

And other SSR related activities, that require a periodic refresh.

DENISE MICHEL: Thank you. James. Anyone else?

JAMES GANNON: James Gannon. So, [inaudible] getting a little bit confused between ownership. So, it's a SSR document, obviously. How come it has been published by MSSI? Is it purely because it's an outcome of the SSR one review?

NEGAR FARZINNIA: So, SSI team is responsible to coordinate the implementation of the recommendation, but it doesn't mean that we do the work. The technical work is done by the subject matter experts as needed. But the coordination of getting the document published on their relevant webpages and such, falls in my remit.

JAMES GANNON: James again. So, if I can give some feedback on the implementation of this task. This is a good document. So, there should be an action, in my mind, from a SSI to say back to the SSR team, you know you need to socialize this, because it's the SSR team that would know who it needs to go to, and who this needs to drive through in the community and everything else.

Having a document up on an URL on the ICANN website, is as about as useless of writing it and putting it over there. You know, this is good work. So, a follow up action I would really like to see is [inaudible] to the community and to the, yes, ease it in the text side. This is good to give to policy people, for example.

You know, if you're a law enforcement guy talk to your Department of Justice guy, this is the thing that you need to be giving them, saying here is the stuff we're working on. You know, this is a good document. It's not just have it go up and forget about.

DENISE MICHEL: Kerry-Ann.

KERRY-ANN BARRETT: That's a part of my AOB is [inaudible], because a lot of the things that are coming up… I was shocked yesterday, when we go to the DNS discussion, [inaudible] that this team does, it's ridiculous. And where it has been benefitted, it has really been security side of community that needs to hear all of this. So [inaudible] pigeon hole for AOB, in terms of how we break down the subcommittees to actually look into this a little bit more.

JAMES GANNON: James again. Just a very quick follow-up. Maybe one of the things that we need to say is that maybe the SSR group needs to be empowered to check their form a little bit louder. You know, because I think even for those that are relatively involved in security around ICANN, we're still discovering things that are being done by your teams, but we don't hear about them.

So, maybe there is a bit more of a, you know, you're doing good work, let's tell people what the good work is.

EMILY TAYLOR: I'll just say, we've got more or less an hour, or an hour and a bit, after lunch to sort of, to process our reflections on this piece. So, maybe we could just… Is that the end of the slides, Negar?

NEGAR FARZINNIA: So, we only have two more recommendations to go through, however, we've covered the content for all of them, because they pertain to training sessions and the outreach and engagement activities. So, we have talked about that.

DENISE MICHEL: May I propose, we're into the… I assume lunch is ready. Yeah? Why not let David address that last comment, and then let's pick up after lunch to continue the presentation and discussion on the rest of the recommendations, and additional issues that I think have arisen during the course of this presentation. David?

DAVID CONRAD: So, on the specific point of sort of being more visible, in the ICANN context of the work that we do and how we present it, earlier this year, right, late last year, sorry, [inaudible]…

I'm still tired. [CROSSTALK] [Inaudible] was transferred, and he is vice-president for technical engagement within the organization. He was transferred from GLT over to my group, and is now reporting directly to me, and one of the things that we're undertaking is to develop a… First of all, we have developed a technical portal on the ICANN website.

And I'll just defer comments about ICANN's website. But we're also developing a communications plan that is aimed at both facilitating inward information into our group for us to do research on, as well as and more importantly, propagating the we do outwards. One of the… We're looking at various mechanisms by which we can publish our information, or establish a relationship with the internet protocol journal, and we'll be using that.

Increasing the amount of logging and social media stuff that we do. So, we understand that's a known, not a problem, a known issue that we've had, because to be honest, I have a group of highly technical and very dedicated, but not necessarily the most social individuals on the planet. And we're…

DENISE MICHEL: We'll have time after lunch for a reply to that.

DAVID CONRAD: But yes, we are, we acknowledge that is something that needs work, and we're actually actively engaged in that.

DENISE MICHEL: Are there any further comments that need to be made before we break for lunch? Anything on the chatroom?

[SPEAKER OFF MICROPHONE]

Where is the agenda?

Pardon?

[SPEAKER OFF MICROPHONE]

I'm aware of the time. I was just looking for the timing on… Okay. So, we have a lunch break until 1:15. Do you feel like you need a bit more time or can you make that work?

EMILY TAYLOR: I'd suggest maybe we have three-quarter hour and then we just try to catch up, because I think people, there has been a huge amount for us to assimilate, and I think a proper break would really help with concentration levels after lunch.

DENISE MICHEL: I'm sorry, Emily, you're suggesting [CROSSTALK]…

EMILY TAYLOR: I say, let's take a three-quarter hour lunch, our schedule, just a bit later, and we will make up the time, we've done a lot of reflecting, okay? Already, as we've been hearing about the SSR one, and I would suggest that we do finish that to do the full hour for Dave's presentation on the health indicators. That would be my suggestion.

DENISE MICHEL: This is Denise. Thank you. So, we will reconvene at 1:30, sharp, and lunch is through those doors? Great. Thank you so much, everyone, for a really productive and informative morning session.

EMILY TAYLOR: So, we're just coming back from lunch now. I'm just waiting for the other co-chairs.

So, for those of us in the room, and online, just another reminder from the transcript people to remember to say your name. This is Emily.

So, thank you very much. We will get started now. This is Emily. What we're going to do, just run through, very briefly, the final two recommendations from the first security review, and then we will just spend until half past two, here in Madrid, which is another, until the end of the hour, just reflecting on that piece of work, you know, the implementation of security, the first security review and recommendations.

And just continuing our discussions. We will then go on to Dave Piscitello for a presentation of the domain abuse tool. Okay, so with that, Negar, can I ask you to continue please.

NEGAR FARZINNIA: Thank you, Emily. So, the recommendation we were going to start with, after lunch, recommendation 28, asking ICANN to continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information. We address this, we are afterwards, our activities reporting, as we have discussed in the earlier slides, as well as the coordinated vulnerabilities disclosure reporting, which we also addressed in the earlier slides, and this is just repeat information from earlier decks talking about activities that SSR reports on.

Unless there are questions, we can move past this. All right. Recommendation 16, which is the last item we will cover today, is discussing, or asking ICANN to continue outreach efforts, to expand community participation, and input into the SSR framework development process. ICANN should also establish a process for [inaudible] systematic input from other ecosystem participants.

And this has been addressed through outreach activities that you're going to outline in the follow-up slides, as well as the SSR best practices that, with the support of the GSC, and other ICANN organization teams, we are engaging regional areas, to promote best practices.

Also by providing a capacity building workshops that we had discussed earlier. So, moving into details, we've got, and this is just a tiny subset of what SSR does in terms of training, but this is covering the high level items. We've got a list of DNS training sessions, or subjects that also SSR holds throughout the year, for various topics.

Would you like to go through them line by line? Are there any questions? Or, are you okay with the content? We have discussed this in the earlier discussions.

EMILY TAYLOR: Maybe we can just pause for a second, read the slide, and if there are any comments or questions. Kerry-Ann.

KERRY-ANN BARRETT: Kerry-Ann speaking. Just to follow-up on the discussion that Matogoro had raised in terms of like outreach to Africa [inaudible] as well. Given… Is it that [inaudible] are based on a schedule, recognizing that there is a need for all regions to actually have this information? So you have like, knowing the research that you have, is there any schedule that has evolved?

Or is it strictly, strictly on…? Or, as well, just a follow-up, if [inaudible] also if some certain threat analysis that you have done, and you say that there is a certain region that's probably having more of an issue with DNS or DNSSEC, then the need will then shift to that region, because you see that there is a need. I was just wondering if there was any other logic that could be built in?

EMILY TAYLOR: Thank you. Bernie, did you want to…?

BERNARD TURCOTTE: So, the mechanism we use for designing a lot of this is the regional engagement strategies, the regional strategies that GSC work with other people on the ground. So, that's kind of the formal mechanism we use for this. Going to Africa or… I mean, obviously, we will see more requests coming from an area.

I don't think we've had a case where we've said, well, this is a specific issue and a specific place. I can't think of one where we've had that. But we will see, on occasions, more requests coming from one area, and that will then [inaudible] stakeholder engagements. If you read the various strategies, some have more focus on SSR training than others, because you know, the locals are the ones who know what kind of help they need, they're the ones that tell us. Does that kind of answer the question?

EMILY TAYLOR: Thank you. Denise?

DENISE MICHEL: Thank you. Could you send us the link to the technical, I think that was mentioned, and also, to what extent do you have online versions of the training modules? And to what extent do you also have remote sort of participation and training as well?

EMILY TAYLOR: Steve, do you want to take that?

STEVE CONTE: [Inaudible] so I can actually try and take that one too, and see if you want to add to it. The first part of your question, Denise, can you repeat that?

[CROSSTALK]

…technology part, I just put that into the Adobe Chat. Okay. So, as far as face to face versus remote, is that what you were asking?

DENISE MICHEL: I mean, have you, like, videotaped some of these training sessions? Are they available online as an online training module? And do you have remote training as well? I know recourse constraints have been mentioned several times, I just want to understand.

STEVE CONTE: So, we have not recently taped any trainings we have been in. Lots of discussions as the team that handles the Learn dot ICANN portion, the online learning portion, on how we can… You know, this is one of the first multiplier opportunities that we're looking at, how we can reach more people with less travel, which hopefully, reflects less budget involved in getting people on the ground there.

As an interim step, we have done various webinars, specifically that I'm aware in Latin American region, there might be some other ones too, that I think most of our efforts for webinars in Latin America. And we're trying to figure out how we better maximize our available human resources to reach as many people as possible and still have an effective and impactful operation on that.

DENISE MICHEL: This is Denise again. That's why I was wondering, I mean, is it feasible to use online training, or is so individualized and hands on that it's so much more impactful to have everyone in the same room and an ICANN staff person there, walking people thorough it?

STEVE CONTE: The answer is yes. It's feasible, but when you get to the hands on portion, it begins to be much more difficult to do that online. John and I have been speaking over a period of time on how to look at a virtual lab, or a virtual environment, when we can get more hands on individuals, not just to sit through a webinar, or watch a video of us talking, but you know, so that we could have a moderated learning session along with a remote lab, or a virtual lab, that they can go and actually touch and go through an exercise.

That presents its own set of challenges that we're exploring as well. Something, just to add on to John and hopefully to address Kerry-Ann's question, and I wish Mr. Matogoro's, I wish he was still on too. He reflected that more work needed to be done in some of the outreach, especially in the African region, and I think if you ask anybody in any region that would probably say that they need more training.

I don't think it's unique to any specific region. And you know, if we look at training as a shared and collaborative effort done by I-STAR organizations, you know, Alain in his multiple hats in the African region, [inaudible] and ISOC, Simon [inaudible] got [inaudible]. They've done an extraordinary amount of training effort in the African region, and it hasn't been specifically ICANN, and I think that as we look at this, there should be [inaudible] nor should it be specifically ICANN either.

There should be a collaboration model because there are pieces of the internet ecosystem that do cross between I-STAR organizations and having that collaborative model, and how we can best work together. Also, is a good share of resources as well. So, as John mentioned, the trainer to trainer, we're looking on how we can collaborate with the other I-Star organizations to make the biggest impact with our collective limited resources on how to be most effective on the ground.

EMILY TAYLOR: Thanks very much, Steve. On the list I've got… James, did you want…? You put up and down. What I would like to do, just try to… I've got James, Dave, John, no? Okay. Thank you for your cooperation. Let's go James, and then Dave, and Negar.

JAMES GANNON: Thanks. James Gannon. Take [inaudible] Steve was saying exactly what I was going to say. This type of training is, well should be somewhat tailored. So, it doesn't naturally lend itself to an ICANN Learn style platform, you know, of recorded training session and then just let people watch it. [Inaudible] the follow-up from Steve, which was why I took my hand down, was that a moderated online delivery, you know, Steve said [inaudible] and do this, you know, there is a meeting technical team in ICANN that has a lot of capabilities there.

You know, that type of thing, with a moderated online both remote, that could work very well. You know, that definitely should be looked into. But I think with an ICANN Learn type of thing, I don't think will work with this type of training. So, for other things, but not with this.

EMILY TAYLOR: Thank you. Dave and then Kerry, sorry, then I'll have [inaudible], and then Kerry.

DAVID PISCITELLO: Dave Piscitello. The law enforcement training is not online and probably never will be. It is material that we show in confidence, because if we put it on a public site, then attackers will know what we're training law enforcement to do. The remote delivery is very challenging, because often, law enforcement are comfortable talking about an ongoing investigation when you are in front of them, and you have no idea who is actually participating remotely.

So, there are a number of accommodations that we make, remote delivery really sort of out of scope. And the other thing that is very hard is that sometimes I will show up, and I have eight hour of slides, and they say, well, we really don't want to talk about these three hours of slide, we want to spend the afternoon looking at, having you help us with some specific kind of investigation that they are taking.

And sometimes I have to end up opening up an entirely different set of tools, and you know, it's really, how can we help you do what you do your job? And what can we do to impart knowledge so that you can…? So, they're very, very flexible and pliable.

EMILY TAYLOR: Thank you for that. Very important points being raised there. Kerry?

KERRY-ANN BARRETT: This flows into what I wanted to ask. Steve, touched on… Is it that we could then explore different types of training different types of [inaudible], because some of the more general information stuff like what… [Inaudible]. James. [CROSSTALK]

We were speaking earlier about the report, the identifiers report, on identifier methodology. Information like that, I think, can be on an online platform that's constantly available. Law enforcement, agreed. It would have to be maybe in person. So, I think if we look at the different types of information we need, haven't identified, what are the challenges we found [inaudible] that needs this capacity building.

Then you look at the different models, and then you look at where it's possible.

EMILY TAYLOR: Very quick follow-up.

JAMES GANNON: There is [inaudible] called traffic light protocol to differentiate levels of information, could [inaudible] this is what we have as traffic light white, and can be just put up online. Green for something that's a little bit more, let's have people sign up to look at it. And then, yeah. There are things that we could do there to facilitate that.

EMILY TAYLOR: What I'm going to do now, unless there is anything urgent, is to ask Negar whether we're done with the slides now, or just to finish that off.

NEGAR FARZINNIA: Actually, I reached over to the second to the last slide, as we were talking about additional trainings, and also the last thing out there is international development, which has included some examples of engagements that we've had internationally during [inaudible] 16. And that's the last of the slides.

EMILY TAYLOR: Thank you very much. And thank you to all of the ICANN team for guiding us through these implementation points. So the remainder, so the next three-quarters of an hour, what I would like to do is to have the team, and I would like to hear as many voices as possible, including if Matogoro is back online, or Ram Krishna, to get…

[END OF TRANSCRIPTION]