ICANN Board with Technical Experts Group
15 October 2014

Steve Crocker welcomed the nearly sixty participants to the meeting and stressed the importance for ICANN of starting to actively seek high-level technical input into its work, in addition to the input it receives from the Security and Stability Advisory Committee (SSAC), the Root Server System Advisory Committee (RSSAC) and from ICANN's technical staff. Steve then handed the meeting over to David Conrad.

What is the Technical Experts Group (TEG)
DAVID CONRAD: Okay. So to start out, there was a discussion on the mailing list and some people had asked the very good question, you know, exactly what is the technical experts group

The TEG is focused on forward-looking technical and technological issues, particularly as those issues impact the use of the Internet's system of unique identifiers that, in the view of TEG members, ICANN's board and staff should take into consideration when considering ICANN's strategies and operations

Introductions around the table:

>>MARKUS KUMMER: Markus Kummer, incoming ICANN board member.

>>PATRIK FALTSTROM: Patrick Faltstrom, SSAC chair.

>>JIM GALVIN: Jim Galvin, SSAC vice-chair.

>>HOWARD BENN: Howard Benn representing ETSI.

>>JAY DALEY: Jay Daley, dot nz.

>>DANIEL DARDAILLER: Daniel from TEG.

>>WARREN KUMARI: Warren Kumari, one of the IAB TLG folk.

>>WENDY SELTZER: Wendy Seltzer, W3C.

>>ASHWIN RANGAN: Ashwin Rangan, ICANN.

>>STEVE CROCKER: Steve Crocker, ICANN board.

>>DAVID CONRAD: David Conrad, ICANN CTO.

>>PAUL MOCKAPETRIS: Paul Mockapetris.

>>RAM MOHAN: Ram Mohan, SSAC's liaison to the ICANN board.

>>LARS-JOHAN LIMAN: Lars-Johan Liman, co-chair of the Root-Server System Advisory Committee.

>>MARK KOSTERS: Mark Kosters, ARIN, your token regional registry representative.

>>DAVE PISCITELLO: Dave Piscitello. I'm Mark's friend.

>>JONNE SOININEN: Jonne Soininen, the IETF liaison to the ICANN board.

>>SUZANNE WOOLF: Suzanne Woolf, RSSAC liaison to the ICANN board.

>>KIM DAVIES: Kim Davies, ICANN.

>>MARGIE MILAM: Margie Milam, ICANN.

>>PATRICK JONES: Patrick Jones, ICANN.

>>FRANCISCO ARIAS: Francisco Arias, ICANN.

>>DAVID CONRAD: I had sent out a set of topics sort of as a conversation starter, and these are sort of the questions that I had in my mind that I thought would -- might be helpful at some point for the TEG to actually engage at some point. We can engage these questions as they are opened.

1. What are the key areas of technical risk that ICANN faces? [more discussion later]
2. How can ICANN best improve its technical stature?

>> DAN YORK: David, when you say technical stature, what are you looking to improve in your sense? How do you define technical stature, I guess I'd say.

>>DAVID CONRAD: So an understanding that ICANN has, for example, thought leadership is ICANN is recognized as knowledgeable in ICANN's space, which in my view is the Internet system of unique identifiers, and is respected for that knowledge.

>>JAY DALEY: ICANN doesn't have a GitHub page. Let's let ICANN get a GitHub. Let's see everything that ICANN writes and stuff out on GitHub.

>> KIM DAVIES: actually we do, yes. Github.com/icann. I mean, there is not a heck of lot there, but there are about six projects there.

>> JIM GALVIN: The SSAC Fellows program has been working well and you should increase that kind of involvement. You bring in someone who wants to come on for six months or a year or so and provide some specific expertise who has facilitated some work products and could continue to do that.

ICANN has a very good track record in growing various kinds of fellowship types of programs and it occurs to me that you could use that as a path for beginning to understand what your options are and who you might be able to attract and what you could do with them.

But that's at least a partial success right now in what SSAC has experienced. And increasing that, perhaps providing a way to support some of the other groups technically would be useful, too.

>>WARREN KUMARI: ICANN should actually participate more in some of the technical groups like IETF, et cetera, have staff have the ability to come along and participate and speak as individuals, not necessarily with the concern that they're actually representing ICANN.

>>DAN YORK: Dan York, Internet Society.
If I look at the ICANN Web page, I see nothing at all about technology. So that might be one detail, would be to expose something on it about what you do in that space.

>>DANIEL MIGAULT: Daniel Migault. One thing is to take part in other organizations, but the other part is to bring those organizations at the ICANN, for example. There had been a workshop, I think, yesterday on public safety, and that was very nice for people at the ICANN to see what is going on in other organizations, given the fact that people can attend all the different meetings and so on. So...

>>JIM GALVIN: Jim Galvin. I'm thinking about the security team. You know, so being able to say more about what they have and what they're doing on the Web site in particular, making that resource available and much more accessible and known.

>> DAVE PISCITELLO: The ICANN security team pages somehow did not convert well in the makeover from the previous version to the new version. And if you do manage to find any of the new content we used to have, it is in an archive. It actually took me over two weeks to find and curate all the stuff that we lost. It is fortunately not lost; it is just hidden.

I've already put together replacement pages. It will look quite a bit like the SSAC environment when we're done. And we have some other ideas, especially in the area of security awareness where we will be putting up some frequently addressed questions pages. We will be putting up some resources that people will use for various levels of competency or non-technical competency. So there will be a section for just regular Internet users, there will be a section for ICT users, and a section for ICT administrators

>>DAN YORK: Dan York, Internet Society. Improve the visibility of some of the technical work already going on in SSAC, RSSAC, and some of the different monitoring and different I think as you expose that information, that would be useful to improving ICANN's technical stature.

I would also point out with my role with The Internet Society where I'm advocating around DNSSEC and pieces like that, you know, I'm heavily promoting the DNSSEC workshops that happen every ICANN. But if you look for those sites, or promotion of the events, it's not happening from the ICANN side.

This is one of the best pools of DNSSEC people that you will find anywhere around. You know, come to these events because you get people from the IETF space but you also get people from other operators and other people who come here because of this. And so exposing that, giving it more visibility in some way. ICANN already has some good technical stature in there. It is just not being shown to the rest of the world.

>> MARTIN LEVY: I think there is one other vector that you could add to this which may be slightly less work. If you look at all the constituencies and then you talk about the working done inside IETF and other groups or even within The Internet Society and IANA and the like, you could, in fact, generate a mapping in some way of protocol specs, of technical work done, and which constituency has an involvement in that.

And if that mapping was built in some -- I want to say in some tool manner but in some way that we could then get constituency members involved in either operational or standards that really affect them, you can think of WHOIS and all the work being gone on which has touched many groups, of course, but there are other areas as well. And I just think that that mapping would help drive, who has to be aware of what as opposed to doing specific work and exposing specific work inside ICANN.

>>WARREN KUMARI: ICANN is actually doing a fair bit of technical stuff. Just when we think of ICANN, that's not what first comes to mind. I mean, there is the training that John Crain's group was doing with ccTLDs, or helping support that; abuse coordination; a bunch of monitoring, the root key rollover stuff, which I believe you helped organize discussions.

But the messaging isn't really there. When people think of ICANN, they see the big front page; and they don't think the technical stuff.

>>FILIZ YILMAZ: Okay. Filiz Yilmaz, ASO AC/Akamai Technologies. I actually want to make a very practical suggestion based on what I'm already hearing here. There used to be tech tracks somehow, tech days, during the ICANN meetings. I think labeling it correctly and maybe creating a program committee among the SSAC, RSSAC, Address Supporting Organization chairs, and making sure that there is going to be some kind of program, this can be easily led.

I think we should create one track for those technical-minded people to come and sit in a room in a continuous way and they will be seeing actual hot topics presented by the SO or ACs or even by the general public. If there happens to be a coordination for a program committee, I think there can be submissions towards that track easily. Thanks.

>> SIMON MACCALLA: Simon Maccalla, Nominet. Does ICANN want to be known for great DNS engineering? Does it want to be known as a great knowledge base? Does it want to known as great research or great innovators? Because actually all of those disciplines require different sets of skills and quite often different people. And so I appreciate that doesn't help in answering that specific question that way, but I wonder whether focusing on those different groups might be helpful.

>>PATRIK FALTSTROM: I think I'm happy to hear what you're saying, Filiz.
CcNSO have had their tech day for quite some time, and the reason why I want to talk about this is because I'm not ccNSO, to explain how good I see ccNSO has managed and is managing to try and turn the ccNSO tech day into Tech Day or Tech Days.

And I'm now participating in the program committee from SSAC to broaden the scope. And we also had OARC working together with that as well.

So I think we see an embryo of what you want, but we can do so much better. And just the fact you are asking for this at least gives me more energy on working on this.

>>JAY DALEY: It's clear that we can improve technical participation in ICANN if we can ensure that technical meetings are contiguous over the early part of the week so that people can justify the cost of coming. And that's something that a number of us have been working on for some time.

So on the tech day, we have just about managed to jettison it from the ccNSO to make it a top-level ICANN thing so that it will then become Tech Day in that type of way.

And one of the things that we're still hoping to do is to get the program schedule to be tagged so that you just have a nice big colorful tag that says technical against the session or policy or legal or three tags against one. It really doesn't matter. So that at a glance, those of us who obviously cannot stand certain other kinds of tags can find the ones that we would like to go to and we can -- we'll all immediately be able to see how contiguous or not those things are.

So that's part of it, is trying to build that stream so more people attend.

>>PATRIK FALTSTROM: In the meantime, yes, we call it "Tech Day" but I think in reality it was Saturday closed, OARC, Sunday open, Monday open, Wednesday open. So it is just kind of this naming thing as well. Just because we failed with communication, because we name it "tech day" in singular also make people think it is only one day. But some people, technical people, are pretty busy this week.

Patrik Faltstrom presentation

This was my immediate reaction when I got the mail from David with these questions So it was some kind of sparking the discussion. Of course, including discussion between me and David. And then after having that discussion, then we started the discussion whether we thought we actually would agree at the end if we continued the discussion. So anyways, here are the slides.

For the first thing regarding what are the *technical risks of ICANN*, the biggest problem I see is actually marrying issues, that people are mixing so many things up.

So to be able to sort out what are the actual sort of risks for ICANN, I think, is important to try to when looking at the various things to divide them in different categories. So here's an example of categories.

- ICANN itself,
- the internal tools,
- communication, in and out,
- root key management, and
- all the various systems that ICANN itself hosts.

And note here that I'm mentioning these things, doesn't imply that I think that what ICANN is doing is bad. It is just that when people are complaining and other kind of things, we need to sort of untangle the various. So this is one area where we need to make sure that ICANN continue to be stable and sound, should be -- it could be, for example, quite interesting for people to also understand what people -- what ICANN has done as examples so other enterprises can copy what has been done.

The next thing has to do with *IANA stewardship*.

We have written two reports from SSAC, SAC67 and SAC68, that explain what the IANA function is from various perspectives. And in SAC68 that is looking at the actual contract between NTIA and ICANN, we come to the conclusion that the only place where NTIA do have active involvement is in the authorization -- in the chain of authorization for root zone changes.

Of course it's adult supervision. It's like you have the room with teenagers, the adult is in the room, and just by having the adult there, the teenagers will not start to sort of do bad things, but if we talk about real actual involvement, it's very, very limited.

So I see a risk that people are sort of overexaggerating what NTIA actually is doing, and because of that, it might be the case that people are requesting many, many more changes than what is actually needed.

Regarding DNS and DNSSEC -- I divide the DNS -- first of all, the DNS issues in three or four different ones.

- The clearly DNS issues,
- DNSSEC issues
- DANE issues
- General acceptance issues for domain names
- Root key rollover.

I personally am very worried about what's happening on the security side. We saw the SSLv3 thing coming here, and -- but on the other hand, as you know that have been following SSAC and work that I've been doing personally during the years, I don't really like the -- how much we are relying on CAs and XY9 certificates and that straight hierarchy. I think DANE, and because of that, DNSSEC, but for good DNSSEC, we need good validation and lots of other kind of things but that's the ultimate goal, and for me that's the driving force to go down that path.

And then the other thing, the elephant in the room, of course, that everyone is talking about has to do with -- with *routing and the issues we see with route announcements*. And we have the IAB statement since a couple of years back that talks about RPKI, how important it is. The question there is, are things happening, are things not happening, and what is, if any, ICANN's role.

>>IZUMI OKUTANI: Izumi Okutani from JPNIC. Thank you, Patrik, for categorizing. This is very helpful. And I have a question about any other possible thing to add on this. I'm just wondering, there's a lot of discussions about the WHOIS review, and I understand there's another consideration at the IETF, the very technical level, but I don't know if it's appropriate to consider what's being discussed in WHOIS in the ICANN context and on this platform and something to be, you know -- look more from the technical perspective how this would be affected. I'm interested to hear others' opinions about this.

>>DAVID CONRAD: My personal view is that given that the TEG is focused on forward-looking things and the evolution of WHOIS is definitely -- it's both past, present, and future looking -- that it is some -- a topic that is appropriate for this group.

>>WILFRIED WOEBER: Wilfried Woeber, Vienna University, and wearing a hat of National Research and Education Network for a couple of minutes.

I'd really like to suggest that maybe even the SSAC has a closer look at RPKI.

We were running lab tests for that new technology for the most recent three or four months in our little shop. In the little shop, the -- sort of the focus is little. We're not a big T1 provider. We're just a network out in the streets.

And what we found is that, first of all, the availability and the quality of implementation on the various boxes is pretty limited at the moment, so this is something which is, well, giving me grief because there is a lot of people who know how to deal with accidents on the routing plane these days and there is not too many people being trained and having the same level of experience with properly managing RPKI, or managing the RPKI'd subset of the network connected to the non-RPKI'd part of the network.

And the last thing that I wanted to bring to the table here is that I am pretty worried that the current implementation allowing any announcements to carry just one digital signature is actually introducing a new single point of failure, and this is, in my -- sort of in my books, this is something which should not happen.

If we want to deploy that in production environment, we should try to make sure that we do not introduce new single points of failure, just in the interest of getting a hold on some accidents that we knew how to handle.

Sorry for taking too much time.

>>BILL SMITH: Bill Smith. I'm here representing myself today. I wanted to follow up on Patrik's point regarding the -- the NTIA contract and its scope. While its scope might be seen as relatively broad, as SSAC pointed out it's a very narrow and limited contract. I'll also add that it's no-fee. And if a business person is looking at this, they're going to look at something and say, "Well, no money is changing hands. How much time do I want to spend figuring out the replacement for it?"

>>FRANCISCO ARIAS: Francisco Arias, ICANN staff.
On the topic of WHOIS, I just wanted to point out that tomorrow at 10:30, there is a session on starting a discussion on deploying RDAP, and this is closing the loop on what SSAC started three years ago with SAC51, in which SSAC requested ICANN to work on replacing the WHOIS protocol.

>>WARREN KUMARI: So Warren Kumari. So going back to the RPKI topic, I was part of the original RPKI design group and active in the CIDR working group.

If you're interested in that topic, there is an IETF meeting in Hawaii in a couple of weeks and the CIDR email list is very active.

I think the main discussion people have been having about stuff revolving around RPKI and ICANN is mainly the single trust anchor for RIRs, and I think we have some RIR folk in the room who might have some strong views on that.

>>BILL SMITH: Bill Smith. I'm here representing myself today. I wanted to follow up on Patrik's point regarding the -- the NTIA contract and its scope. While its scope might be seen as relatively broad, as SSAC pointed out it's a very narrow and limited contract. I'll also add that it's no-fee. And if a business person is looking at this, they're going to look at something and say, "Well, no money is changing hands. How much time do I want to spend figuring out the replacement for it?"

So I'm a little concerned, of all the activity I've seen over the last year or so dating back to NTIA's announcement, about how are we ever going to, you know, replace the role that the U.S. Government and NTIA specifically has played.

I think there's an awful lot of emphasis on this, and it's -- there's actually not much there. This may not be the right forum to raise the issue, but I am concerned about it, that we will end up with, you know, something that will be very expensive to operate and very difficult to navigate. I see it as a big risk.

>>PATRIK FALTSTROM: Yeah. I just wanted to say, as the name SSAC was mentioned together with RPKI, I can just say that, yes, RPKI is one of the topics that we are discussing, and we are trying to keep track of what's happening in the community for the reasons that other people mentioned in the room, but it's not one of the work items that we have picked up yet.

>>DAN YORK: Well, I see Mark reaching for his mic and I would just, I guess, say from my perspective it seems that most of the RPKI work right now on the operational side is being driven out of the RIR community, and so I think really in my -- in my view, it seems like it's something that ICANN should really, you know, look at how they can support that effort that's happening through there in some ways, but it seems like it's an RIR-led effort at this point in time.

>>MARK KOSTERS: Yeah. Thanks. So the regional registries have been working on this particular endeavor for a number of years now and there's been a fairly low adoption rates. It varies on the region.

The most successful region is -- essentially is RIPE's region, and Kaveh, you're more than welcome to say something about that if you wish. But from the regional registries' perspective, we're looking at this and trying to work all the kinks out, and all the kinks are not out on RPKI yet, in terms of the operational sort of footprint, how this thing should work, and there's going to be quite a bit of tuning going on as we -- as we learn more.

As far as ICANN's role in this is, at some point we're going to want to do some interrupt testing with ICANN on dealing with the GTA, the global test anchor. That has not happened yet and it's not on the schedule.

>>DAVID CONRAD: To reiterate that point, I believe a couple months ago, the chair of the NRO sent a letter to ICANN indicating that they had suspended any development on the global trust anchor.

ICANN was and is in a position to work on that when the RIRs are willing to move forward.

So now getting more into the DNS-related questions,

What technical innovations in the DNS should ICANN encourage and how?

I believe Patrik has indicated DANE is pretty high up there on the list. Are there any other technical innovations that ICANN should focus on?

>>DAN YORK: You had a question earlier about DNSSEC and the validation signing pieces. So this is really a combined answer of the -- of the -- a couple of those.

You asked about whether ICANN should encourage validation or signing, and I want to answer that as a path to getting to the first one.

Which is to say, one of the topics we've talked about at DNSSEC workshops and the pieces that are here is that if we look at the two pieces of signing versus validation, you know, we're getting pretty good in some of the signing areas. We're -- but validation is certainly a critical need. But what's interesting is we're seeing a lot of good growth in that. Geoff Huston was mentioning at our talk today that his stats show we're now at about 13% of all DNS queries that are being validated. And the -- Kaveh from RIPE was

showing on the ATLAS measurements it's around 26, 28% of the items that are out there. We're seeing some good growth in that. There's a lot more to be done to encourage that, but I guess the question that I would put out there for discussion at some point is, is that an area that ICANN can really exert any influence.

A lot of the space where validation is occurring is in the network operator space and a lot of the -- the enterprise networks and the places that are out there, and so I wonder if that's not perhaps something that really more of the network operator groups and the piece -- the places out there, you know, can play a role in encouraging the validation side.

But where I would love to see, personally, ICANN focusing is taking some of the friction out of the signing process and helping with the better automation of the spaces that are in there.

And I'll give you two examples.

One is right now there remains challenges with people -- you know, if the average person who comes to a session here wants to go back and sign their domain, there remains challenges getting registrars, in particular, to accept DNSSEC-related records. DS records. You know, now -- in many cases.

Some -- now, the 2013 RAA is supposed to require that, but there are registrars, including one at which I have domains, that even after they've signed the 2013 RAA, they still don't accept DS records. And I could get into the reasons why, they tell me, but there's some work that ICANN could do to help do that.

The other piece is that we have this issue with when you do a key roll, how can the parent zone and the registrar be updated. Warren's giving me a frowny face like he wants to talk about this, but there are some new ways to make this work that ICANN could really help grease the process there and make that signing and automation side a whole lot more easy for some of this to work, and I think this is an area that ICANN can directly have an impact in because of the connections out there to the registrars and registries.

Channeling Mr. Faltstrom, two seats to my right, I would also say there's a great amount of issues within the connections from a registrar to multiple registries in terms of uploading records to the registries. So there's a whole lot of automation that needs to happen on that side, on the signing side, that ICANN is uniquely positioned to go and push at this and really make some of this happen.

So I had one wish coming out of the DNSSEC workshops that I wish ICANN could do, it would be help to make the auto- -- help automate that process of signing inside the back end of all this.

>>DAVID CONRAD: Okay. Let me -- I had thought that part of the RAA 2013 was a requirement to actually support that sort of stuff, and if someone -- if a registrar has signed onto the RAA -- 2013 RAA, then -- and they didn't do that, then they were actually technically in breach.

Is that right or --

>>FRANCISCO ARIAS: Yeah. Francisco Arias from staff here. I would say if that's happening, my compliance colleagues would like to know about that.

>>DAVID CONRAD: And in fact, there's a form, a Web form, that has one of the check boxes "Doesn't do the right thing for DNSSEC." Paraphrasing a bit.

>>DAN YORK: Yes. And I -- we have been promoting that and talking to it, but it still is a friction you'll see out there. So I think perhaps publicizing that if people aren't supporting that, they ought to, this is where they would go, et cetera, would be good.

>>WARREN KUMARI: So Warren Kumari. I'm generally disagreeable and so I'll disagree with Dan.

On the DNSSEC side, I think ICANN has already done a whole bunch to try and push the signing side. You know, it's in the RAA. There's been a lot of outreach, et cetera. Yes, a lot of lookups are now being validated. Unfortunately, that's because a lot of them are going through a number of large providers. There are a lot of much smaller providers who are not doing DNSSEC validation yet.

I'm not entirely sure what ICANN can do, other than just publicizing the issue, outreach, et cetera, but sort of pushing the validation side I think is useful.

>>WARREN KUMARI: Something that ICANN might want to be watching is also some of the potential new work on *confidentiality in the DNS*.

The IETF believes that pervasive monitoring is an attack on the network and so we're going to be doing work -- the working group should actually be formed before Hawaii, which is in two or three weeks -- to encrypt the DNS or at least provide some sort of confidentiality between the stub and the recursive resolver, so that people won't be able to see what users are actually doing. Or at least passive -- passive monitors on the network won't be able to see what users are looking up.

>>DAVE PISCITELLO: I'm sorry. So things like passive DNS replication are going to be, you know, taken away from, you know, a criminal investigator's toolkit?

>>WARREN KUMARI: So the current thought -- and this is a -- please, we would like ICANN and technical people, technical staff within ICANN, to be involved in this discussion.

The current thought is there -- between the stub and the recursive, there will be some form of encryption.

The recursive will still need to be able to see the actual query. The recursive will be trusted.

This means that you'll be trusting your recursive resolver, you can choose which one you'd like to use. This means that passive DNS stuff, which watches from the recursive to the authoritive, that will continue to work. And recursive resolvers that would like to provide input to that will be free to be able to do so. But just as it is currently, there's no correlation between what the recursive is doing and the actual client who made the lookup.

And I suspect that this is getting too technical for this audience, but I think that what -- that will take away information -- and actually the working group will be called "Deprive." It will deprive attackers on the wire from what's going on, but not -- not hide information from law enforcement, et cetera.

>> KAVEH RANJBAR: Kaveh Ranjbar, RIPE NCC. So on the first question on DNS, what technical innovations should ICANN encourage, I think the two words "technical innovation," I have a little bit of an issue with that. If it is technical innovations, I would say none. There are other mechanisms for that. And innovation is also a little bit -- it is not clear enough.

I think we have a very good example, which I think we can follow also in the DNS arena. For SSAC came up with challenges with WHOIS. So they came up with few problems. They sent that to ICANN. ICANN actually with Francisco and his team, they followed up with a few people who already had some implementations, some ideas, including us, ARIN, some other registrars. And they brought that to IETF, so they actually planted a seed. They really made that group. We had a BOF at IETF and a working group shaped.

And then they followed up until to now we are very close to having the final RFCs and all this stuff. Then from the ICANN side, again, now we have this as a requirement for new registrars. So I think this is a very good example. So it shouldn't be about innovations. I think it should more about finding challenges from channels, RSSAC, SSAC, and other ACs, and ICANN following them up through the right channels. And what we shouldn't -- because there is a big risk of going in parallel. Like when you say "technical

innovation," I expect, for example, that in IETF or sometimes W3C. I don't want to see ICANN getting into that line of business.

>>JIM GALVIN: Thank you. Since Francisco either announced or threatened the compliance police, I wanted to point out there is a subtlety here in the support that's required for DNSSEC that is very much subject to interpretation, okay, and one has to be careful about this. Registries are required to sign the TLD zone. But they're not required to offer signed delegations.

And registrars in the 2013 agreement are required to offer DNSSEC services for registries that require it. Okay. If you look at the words, if you look at the words, this is really the way it is down there. So, you know, there is a gap there.

I have been calling this the policy gap. I call it a policy gap. People disagree with me on whether there is a gap there or not.

>>STEVE CROCKER: Irrespective of what to call it, are there registries that are taking those words and interpreting them the way you're suggesting?

>>RAM MOHAN: Sorry. This is Ram. As far as I know, almost every registry is taking advantage of that interpretation of the words.

>>STEVE CROCKER: Oops.

>>FRANCISCO ARIAS: So this is the first time I hear something like that. The registry agreement is very clear. It says the registry operator shall accept, fully implement (indiscernible) domain names (indiscernible) best practices. I'm not sure the results of the part about signing the zone. So what is there missing? I'm lost here.

>>JIM GALVIN: Certainly -- it says they have to have the feature, and the PDT will test that and see that it is there. But they don't have to allow registrars to do it. I mean, anyway -- it is open to interpretation is the point. There's a bit there.

>>DAN YORK: Real quick, Dave. One other aspect that ICANN is positioned to do is helping with metrics. One of the challenges we've had around getting good deployment metrics of DNSSEC is to understand what's happening at the second level. We know how many TLDs are signed. But once we start getting down below that, we can't really know.

Now with the gTLDs we have the CCDS so we can gather stats out of that. But for the existing TLDs, one thing that ICANN could do would be to help facilitate those registries providing some kind of information around the number of signed domains in a common format or manner or something that could be exposed we know with some nice charts, et cetera, that we could be able to look at. That's another place that ICANN could really play a role in helping us get DNSSEC out there.

>>PAUL MOCKAPETRIS: Yeah. I was going to suggest that one of the things that doesn't seem to go out to the general public is evidence that users are protected by the existing deployments of DNSSEC. I mean, it all seems like you guys are running around in white lab coats and deploying all this stuff.

But there's no particular evidence that User A didn't fall in the well because DNSSEC was there. And I think that being able to tell that story is going to get people interested in letting it pass through the end systems and so forth. And I think that getting it out to the end systems and proving that that actually helps the users is a place with great leverage.

>>DAN YORK: We just had a discussion at the DNSSEC workshop about email and some of the efforts that are happening with SMTP and the protection of MX records through DNS and DNSSEC. And there's actually some very interesting work coming out of CERT/CC recently in September where they were

identifying some actual redirection of email that's happening out on the Internet because of poisoned man-in-the-middle attacks against MX records.

You are absolutely right. These kind of stories need to be given a higher visibility.

>>DAVID CONRAD: Okay. Next topic was related to financial viability of DNS software vendors. And this will be introduced by Steve, and there will be a presentation, one slide, from Jeff Osborne.

Financial Viability of DNS Software Vendors

>>STEVE CROCKER: Those slides or for him? Okay. So I have been drawn into discussions about funding for Open Source software for DNS in a couple of fronts. And it's led me to not only think about the specific cases but the broader issue of whether all this is viable. The Internet generates and runs on a huge amount of money. A lot of people are making money on it, big businesses.

DNS is a critical part of the infrastructure, but somehow this isn't all connected. Why is it, to borrow a phrase, that we have to hold a bake sale for DNS?.

One approach is, well, let's go around, pass the hat, and get some more money for the free Open Source software. It's one thing when the network was young and a lot of research money was going into it and it generated free software that came out of that. We are much closer to being in essentially a steady state or certainly long past the beginning. So I wanted to stir that pot and see what people have to say.

>>LARS-JOHAN LIMAN: Lars-Johan Liman. Yes, that thought occurred to me, too. I've come to realize as I watch my growing children, you pinpointed it well. The DNS part is part of the infrastructure. Now, how exciting is the Internet infrastructure to my 14-year-old daughter?

>>STEVE CROCKER: Take it away and see how exciting it is.

>>LARS-JOHAN LIMAN: Exactly, just as exciting as the power grid.

So just what you said, the research money is now going elsewhere. And what we have is the existing system that doesn't develop as quickly anymore and, therefore, is not a blooming target where -- it is not a blooming ad where people can see indirect money.

But you are also right. There is an awful lot of money in the operating infrastructure. So there is a disconnect.

>> JEFF OSBORNE: The slide says: What's the financial viability of the DNS vendors? When the question is actually: What's the financial viability of the Open Source non-profit DNS vendors? And the difference is important because the for-profit DNS vendors are doing fine because fully 100% of their users pay for the product. Whereas, of the estimated 270,000 users of BIND on the latest date we have, about 110 of them pay us. So compare and contrast, 100% pay the commercial vendors and 0.048% roughly pay us. So there is a challenge there, and there is a gap.

I've been involved with the Open Source community for long time. I've been president of ISC for a year. Before that, I have been involved in the commercial Internet for a long time but also in Open Source and other areas like the 3D printing world, in both hardware and software.

And it's led me to really ask the question: What the hell are we thinking? Because if you describe the Open Source world out there and sort of -- let's get geeky for a minute here. On the X axis you have the amount of money that they have and to the right descending order, let's sort all of the people there. Up against -- there is a they asymptotic curve with a long skinny, skinny tail. So up against the axis with a lot of money, there is the Linux Foundation, Mozilla, there are some other people you know of, and then there is an unbelievably long underfunded group of companies.

Earlier in the year when the Open SSL vulnerability showed up, Heartbleed as on the shirt, brought to you by Indifference, it was amazing to see how little those guys were making. It was six people in a rough confederation working together, deployed, you know, in literally hundreds thousands of places around the world. And their total donations in 2013 were 2,000 U.S. $2,000 U.S.

So somewhere this model has broken. When you ask people in the Internet industry, we tend to reflexively say: Open Source is important. And then when you ask for checks, you tend to get people who cough and claim that the dog is eating their hat and all kinds of other things.

So last week at NANOG, I was offered the chance to stand up for ten minutes and talk. I got in front of the 600 people and said: It's broken and the fixes are not obvious. So let's at least have a discussion before we close up our tents and go away.

The obvious steps would be -- Red Hat is the first successful version of this I knew of where they sold some subscriptions. And that's kind of an easy process. We are selling subscriptions. It's challenging. But after doing some adjustments to staff earlier this year and focusing on only a few things we're good at, ISC is actually a well-funded startup. We are on the left end of that asymtotic curve.

We have got a few million bucks in the bank. We're breakeven. Terrific, that's nice.

But there is a lot of Open Source out there. There are a lot of other vendors just in the DNS space. And what we do with them is a really good question.

So if the subscription model doesn't work for everybody, the feemium model is often -- and I would argue if you give free software to everyone and the good stuff to the people who pay you, you have committed the software equivalent of a sin. It is morally reprehensible in my opinion to give crap to the general public and the good stuff only to people who can afford it. That's just a moral decision, and we are not going there.

Bake sales, gun running, extortion, we haven't tried these yet. The bake sale is coming along well. The gun running and extortion is tied up in legal. I should hear from them later. So maybe we will have that in time for IETF.

So, again, this is really just a request for comment and for people to think. I'm jeff@isc.org.

The issue of how to fund Open Source is not a resolved one, and it is one that I think is important because if we end up with only for-profit commercial entities involved with implementing the standards, the RFCs, and everything else the Internet runs on, it's going to be a very different Internet than the one that got us where we are now that I'd argue has really been a net good for the world.

>>WARREN KUMARI: I believe a number of registries and registrars as recursive resolvers are the ones who are actually contributing to the big vendor because without the DNS they would have no reason to exist. It sort of seems to me that without the DNS and without I.P. addresses and stuff, ICANN wouldn't have a reason to exist either. I don't know if ICANN is contributing to the big Open Source nameserver vendors, but perhaps they should.

>> JAY DALEY: Open Source has not been broken in any way, shape, or form. Open Source to me is getting stronger than ever, okay?.

Now, Jeff and I have discussed this. I have given some very clear views over email about how to fix this, okay? In this specific case, I will share some of it. A subscription model means that I as a small ccTLD, for example, pay 10,000 U.S. dollars to get basically security released information three days or five days after it originally, you know, comes out, okay?

>>WENDY SELTZER: Wendy Seltzer. And I suppose I'm thinking more about the services than about the software when I think of some of this sort of public goods problems to which one answer that we might not like very much is the sort of surveillance-driven advertising model. And so if we can find other options for funding from the sources of revenue of those public goods are a valuable alternative.

>>DAVID CONRAD: I see a couple of additional comments,

>>EVAN HUNT: Evan Hunt, ISC. I wanted to address the comment made by the gentleman over there. I'm sorry, I don't know your name.

I have -- ISC employs me. I have a sentimental attachment to them. I get a paycheck from them. It's a very nice little company and I would like it to survive, but I don't think that's the problem that Jeff was addressing here and it's not the problem that I think is important to solve.

When we say that funding of open source is important and broken, we're talking about things like Heartbleed and Shellshock. If ISC goes under, okay, that's too bad, but somebody needs to be looking for these problems and addressing them, and if we're not paying the people that need to do that enough money, then that's a systematic problem.

>>WARREN KUMARI: So yeah. I agree with you fully, Evan.

I think that the whole open source view where anybody can download it and use it is great, but I think there should also be an expectation that if you're a large organization and you're downloading it and relying on it for your services, you're expected to contribute some money back to the project or to the open source world at large.

I think that currently, some people do that, some don't, but it's not really expected. And possibly putting stuff in license agreements saying, you know, "This is open source, go off, derive stuff from it, et cetera, but if you make large chunks of money from it, please give us some too."

>>JAY DALEY: Great. So I may be alone in this, but I see an observed trend in the way that things are happening and the expectations that people have of ICANN.

And this is about the dependencies in the way that we operate and ICANN, or centralized infrastructure, being part of that dependency. So I see three things happening.

- That we are moving from asynchronous dependency to synchronous dependencies.
- The other one is in decentralized to centralized dependencies which I'll talk about.
- And from end source to mixed source dependencies, so that we're no longer dealing specifically with one organization, we're dealing with contracts that may have been issued.

For example, there are certain things that -- protocol parameters lists and things that we can just download from IANA anytime we'd like. That's what I mean by asynchronous.

Moving to something where we actually have synchronous, we have to do a lookup to go and get that data there and then.

The centralized zone data service to my mind does two things. One is centralized authorization and the other is centralized data access.

I understand the first. I don't understand the second.

The next thing is expert working group on WHOIS, which is also about centralized authorization and centralized data access.

I don't understand the second, and I only partially understand the first.

And the third one is bootstrapping in WEIRDS, which is real-time use of a centralized infrastructure -- okay? -- in order to do that.

So I have three questions:

- Do we know this is happening?
- Do we want it to happen?
- And what are the guiding principles?

>>DAVID CONRAD: Questions? Comments? Thoughts?

Yes, Steve.

>>STEVE CROCKER: In some number of seconds, I'm going to bolt out of this room to go to another meeting which is precisely to the joint board/GNSO working group on how to identify the questions that need to be dealt with to take care of the expert working group report and figure out things.

These are exactly the kinds of questions, and a few more, that I expect we will raise to the surface, because I think that however -- I mean, the expert working group did excellent and great work but I think that these questions actually do need very, very strong attention and some examination.

>>BILL SMITH: Bill Smith. Thanks for raising the issue on centralized authorization, authentication, et cetera, for WHOIS. I'll just leave it as it's a pretty poor idea.

>>JIM GALVIN: Okay. So I want to respond a little bit, I think, on that particular point.

I mean, I think we need to separate that into -- into two parts, okay?

Because as a party that would have to -- a lot of these things are interrelated, is kind of the problem, so I mean, I like your questions, Jay. I should first say I think they're great questions. They're just absolutely outstanding observations and they deserve a lot of attention.

But on this thing about centralized authorization being a bad idea, as one who would be a party, if you will -- to the notion of a centralized database which -- to provide differentiated access, so looking at the WHOIS stuff in particular, the problem is how am I supposed to authenticate all the people that would come there, you know.

We need to separate the problem of identifying who -- where the credentials come from and who creates them versus who uses them.

And that was a question that was never separated in that whole discussion, as far as I can tell, and so we move towards a centralized model and, you know, we all have our issues with a centralized model, but, you know, it's a deeper question.

>>DAVID CONRAD: So I am afraid we have run out of time and I have been informed that this room is actually being used at 4:30 for the next group.

So I thank everyone and I apologize deeply to Howard for being unable to get to his presentation. I will send it out to the list and I hope people will be able to continue the discussion on the list. Thank you very much.