TERRI AGNEW: Good morning, good afternoon, and good evening. Welcome to the APRALO APAC Hub webinar, Basic DNS and DNS Ecosystem, on Thursday, the 30th of July, 2015 at 5:00 UTC.

We will not be doing a roll call as it is a webinar.

But if I could please remind everyone on the phone bridge, as well as computers, to mute your speakers and microphone, as well as state your name when speaking for transcription purposes.

Thank you for joining. I'll now turn it over to our moderator, Ariel Liang, At-Large policy analyst.

ARIEL LIANG: Good morning, good afternoon, and good evening everyone. Welcome to our third APRALO APAC Hub capacity building webinar. So just to give you a quick background about this webinar in our series, it has been developed jointly between the APRALO of ICANN At-Large community, and ICANN's APAC hub. And this is part of the implementation of the APRALO APAC hub pilot framework, with a focus on capacity building and [inaudible] building, to enhance our member's understanding of various Internet policy issues.

And for the recordings and transcripts of our past two webinars, you can see on the slide that we have this Wiki work space link, and you can click on that, and it will take you to our previous webinar recordings. And also, today's webinar recording and transcript will be uploaded there as well.

So it may be a good page to bookmark for. And before we start, the [inaudible] this webinar, we have several housekeeping notes. First, this is an interactive webinar, and if you have questions or comments during the webinar, please feel free to put in the Q&A pod, which you can see it's at the bottom part of this AC room, next to the chat.

And once you type in your question, we will take note on that and let the speaker now. And our speaker will answer them at the end of the webinar, and also if due to limitation of time we can't answer all of the questions, we will answer them in writing, and publish the questions and answers on the Wiki page that I just showed you in the previous slide.

So please feel free to put your questions in the pod. And then second, we have several segments of this webinar, and at the end of each segment, we will have one pop quiz question, just to make sure that you're really paying attention during the webinar and also have an opportunity to interact with your fellow audience and the speaker.

So please make sure to put your answer in the pop quiz pod that, at the end of each segment. And the third, at the very end of this webinar, we have a really short survey, it's only four questions, so that staff can gather the input from you, and we will understand how well we organize this webinar and what areas we can improve in the future. So we would really appreciate your feedback at the very end, so please make sure to complete that short survey at the end.

And now, I have the pleasure to introduce you to our speaker today, Steve Sheng. He is the director of RSAC and SSAC advisory development

support. And he leads a team of policy staff and research fellows, supporting SSAC and RSSAC meetings and working groups. As these groups advises the community and Board on matters related to the security and the integrity of the Internet's naming and address allocation systems, and operation, administration, security, and integrity of the Internet root server system.

Steve holds a PhD in engineering and public policy from [inaudible], where he studied computer security. He is also a non-residential fellow at the Stamford Center for Internet and Society. And without further ado, I will let Steve start his presentation and introduce you to the world of domain name systems.

STEVE SHENG: Thank you Ariel for the warm introduction. It's my pleasure to be on today's webinar. Looking through the attendance list, I've met some of you in person. I hope to be able to meet more of you.

In today's seminar, I'm going to cover a few topics. The first one is IP addressing. As ICANN is responsible for the coordination, the assignment, of three sets of identifiers, and one of them is IP address. Then I'm going to provide an overview of DNS, the domain name registration process, and the domain name resolution process.

Finally, I'm going to talk about a bit of DNS security and recent efforts on DNS privacy. So, here are the slides. So first, introduction to here. Introduction to IP address. So before we introduce the IP address, I want to briefly touch on the concept of [packing?] networking, because this is essential in the Internet.

Before, the networking concept was called circuit networking, where two ends have a dedicated circuit connected when they need to communicate. So this is very common for the telephone network. When the Internet was developed, they used a concept called packet network, where the Internet path, it could break down into small packets, we'll call it data grams, and those are sent across the Internet.

The analogy is very similar to today's transportation and service industry, where the goods are put into boxes, you know, packages. The packages tell us who it is from, where the goods are going, and then that good going through a variety of physical delivery mediums, can use them at the land, the sea, and the air, and deliver to its final destination.

Essential to this delivery chain, the key in that box is that package. So the Internet is very similar. This is the hour glass model for the Internet with different layers. And then, in between, the key part of that is the Internet layers, where the Internet, you know, IP layer, right? Where all of these higher layers application transport relies on the [echo] layer, to probably encapsulate the packages, the data grams, being sent to a variety to a physical mediums.

So as with any package you have a label. So what we call here, in the Internet term, it's called a package header. This specifies where the package is from and where the package is going to. Very similar for the IP packet, the IP packet header, so at that label. Here you see you can have the source address, the destination address. You're able to specify what higher level protocol [inaudible].

And that serves as the label to transport data grams from places throughout the Internet. So what is the IP address then? An IP address is a number that identifies [inaudible] on a computer network. It is fixed format, so the IPv4 is 32 bits, so the total number of IPv4 address you can see is two to the 32 power, that's about four billion addresses.

In IPv6, version six, you know, it's 128 bits. It's the same as, the same concept as IPv4, but just a larger pool of numbers. The properties for the IP address, in other words, the used [inaudible] and every entity handling packets must be able to read and understand the address. You come to the address, it's broken down into two parts, a network part and a host part.

So those are all identified in the IP address. And also in a very important property it must be globally unique, so that means the address is ambiguous, and this is why it caused a need for some kind of coordinated assignment from a single pool address. Currently, IANA allocates the blocks of IP addresses to what we call Internet, regional Internet registries.

And these are further divided, further allocated address into ISPs, into local countries. For the Asia Pacific region, the regional Internet registry is the APNIC. So this is [inaudible]… This is a [mark that's here?] that shows about the IPv4, the [recent] status. This is the number of slash eight. Slash eight here is a technical terms used for the [classless?] routing, that means the first eight bit of the address is one, a mask, that identifies the network.

So the slash eight in each region, as we can say [CROSSTALK]…

So that's a quick introduction to IP address. So before we go to the next section, I believe we have a pop quiz question.

TERRI AGNEW: Thank you Steve. We'll now begin our first pop quiz question. IPv6 IP address are blank bits. Two, eight, 32, or 128? Please vote now.

Once again, IPv6 IP address are blank bits. Two, eight, 32, or 128? Please vote now.

And Steve, I went ahead and broadcast the votes if you want to go ahead and share the answer.

STEVE SHENG: Yeah, I think everyone got it correct. It's 128 bits. Maybe that question was too easy. I'll have some harder questions next time.

Okay, next question.

TERRI AGNEW: Which organization is in charge of allocating IP addresses for the Asia Pacific region? ARIN, RIPE, APNIC, LACNIC, or AfriNIC? Please vote now.

One moment please.

Once again, which organization is in charge of allocating IP addresses for the Asia Pacific region? ARIN, RIPE, APNIC, LACNIC, or AfriNIC? Please vote now.

Steve, I have broadcasted the results, if you want to share the answer.

STEVE SHENG: Thank you. The APNIC is the correct answer. If you have an opportunity, I would encourage you to visit the APNIC website, and also attend, you know, [inaudible] in their policy process and also attend one of their meetings, if you can, and that will be the most, the best introduction to the RIRs. Okay.

So now let's move on to the… After talking about IP address, and we briefly talked about domain name registries and registrars. So a domain name is a series of labels separated by the dot. So here we seen [inaudible] of a domain name. This is for a UK [inaudible], Cambridge University. One thing I want to know that, the main thing, the proper name to address a domain name is for it to end with a dot, you don't usually see this when you type an address.

The last dot is usually omitted, but usually there is the last dot there. And the last dot represents the root. Now, here is another view of the domain name tree structure. It's structured as an inverted tree. On the top, it is the DNS root, it's managed by ICANN, we need that what we call top level domains. So these are further divided into different categories, generic top level domains, and country code, specific country code top level domains.

I think as of last week, we had 10,023 top level domains altogether. Around seven or 800 of those are gTLDs, and then the rest are the ccTLDs. For the second level, these are, you know, one layer there are 288 to 300 million names. I wanted to provide these numbers for you to get a sense of the magnitude of the system, the ecosystem. In terms

of the registry and registrar ecosystem, the registrant interact with resellers, registrants, also ccTLD registries.

And then we have 2,000 registries at ICANN. I'm going to go briefly into a bit more detail here. So registrant is individuals or organizations seeking to have presence on the Internet. That means I want to register a domain name, and through the domain name system, to have a type into a host an IP address, where I can have some sort of presence on the Internet.

It is the customer, in the provision chain in the domain name industry. So we can separate an industry into provision versus provocation. Provision is the provision of the name, these are registries, registrars, resellers registrant. The publication, you know, registries and the DNS hosting providers, those are indeed publication aspect of the industry.

And one important thing to note, the registrant is considered the service provider to the Internet users. So when he or she or an organization has established a presence, [inaudible] starting good services publishing. Registrars, many TLDs can be registered through different registrars. One of the first [inaudible] for, since the creation of ICANN, is to introduce competition in this space.

Originally, we only have one registrar, the network solutions, right? Nowadays we have over 1,000 registrars, you know, drastically bring down the fee. You know, before when you registered a domain name, you had to pay $50, now it's much less, it's much lower than that. In the market, they compete against one another.

Some of them, only some domains. Some others, on domains, with other services they provide, for example, DNS hosting, web hosting, you know, bundle names, bundle the services. [Inaudible] interact directly with registrants and are the point of [sale].

The registry, you know, serves the authority of the master database of all domain names registered that, talking about domains, and there has been exactly one per TLD. They offer a shared registration system for the TLD, for interaction with the variety of registrars. And they generate the zone file for the TLD. They also, you know, put it in the generative zone file, and put it in their DNS server.

The Internet [inaudible] is outside the [permission] model here, you know, these are, there are billions of them around the world. I don't need to speak to you, you know, we should be looking to you in that regard. There are interested on goods and services, you know, using that throughout [inaudible].

I want to touch briefly on the concept of reseller. Some registrars use resellers as the actual point of contact with the registrant. So sometimes the registrant, when you are registering a name, you may not be interacting directly with the registrant, but instead it's the reseller. So they are agent of the respective registrant.

The typical reseller is, for example, when you want to create a web presence, you go to a web hosting company. And the web hosting company, and some of them are resellers, so you can get the names there too, instead of going to registers and come back. So at that point, they act as a point, direct point of contact for the registrants.

There is another service called privacy and proxy, and this has recently been in the news a lot. If you have been following the ICANN policy process. This is generally a third party appearing as a registrant in the registration data. It's either offered by the registrar, or contracted independently by the registrar. So some registrar has the privacy and proxy service. There is ongoing policy development process on their potential accreditations.

In the registration data, we also call the WHOIS data, if you register through a privacy and proxy, it will not show your actual information. What it will show is the contact for the privacy and proxy, and they will relay the request to you.

Speaking about the various players, the various components of the industry, I want to briefly talk about the domain name registration process. It's a simply, a fairly simple process. A registrant, talk to a registrant, or in some case talk to a reseller, we used to talk to a registrar, ask for the availability of a certain name, the registrar will [contact] the registry, to see if the name is available, you know, if the name is available, and then the registrar presents the opportunity for the registrant to register.

So when the names are registered, I want to highlight here, the information, the registration data, are going to different places. The are stored in the registrar's database, and also if the registrar is providing a WHOIS service, those going to the WHOIS service database. At the registry level, there is going to the registry database, the DNS, and the WHOIS record database.

So the data is stored in these various databases. Once in the DNS database, usually the TTL for the registry zones are usually 15 minutes, or even less. So that means that when you register names, once you get permission after 50 minutes, you'll actually have resolution to them, you'll actually be able to have that name translating into an address, and then going to a proper web presence.

Now, ICANN's operative role here is to establish registries, it accredits registrars. A very important part of our role is ongoing compliance activities, performance monitoring, and in the case where registry fails, it's for emergency transition. So we're here to establish for the public good, for the public interest, and then to ensure the security and stability of that. That the operation was in [inaudible].

So this is ICANN's operation. Another part of, a big part of ICANN's role is coordinate the policy involvement, you know, associated with these set, with the allocation and assignments of these identifiers. So you go through, the provision you name is the new gTLD, you need to go through a policy development program.

The policy development works with WHOIS, inter-registrar transfer, because that's usually one of the biggest complaints is for transferring names. So those are the policy aspects of ICANN's operations.

So that's a quick introduction to domain names, registries, and registrars. Let's have a quiz.

TERRI AGNEW: Thank you Steve. And this is Terri. While we bring up the quiz, just as a quick reminder, it should be on your screen in a moment. In the top right hand corner. If you could please use that, versus the chat box. And the quiz is open now.

And the question is, which of the following statements is true? Domain name is a fundamental identifiers on the Internet. There are over 1,000 generic top level domains. Internet users need to register domain names, add a registrar or registry. Resellers are accredited by ICANN. Or, none of them.

Once again, the polls are open. Please use the poll on the top right hand corner. And the question is, which of the following statements is true?

Steve, I just broadcasted the results. If you want to go ahead and share the answer.

STEVE SHENG: Yes, thank you. The answer is really none of the above. Let me explain why. The fundamental identifier on the Internet is an IP address. That is the fundamental identifier. There are over 1,000 top level domains, but there are not that many generic top level domains. There are country code top level domains too. The third one, you could argue that is correct, but Internet users need to register domain names at a registry or registrar.

They can register it at a reseller. In many cases, for the generic top level domains, they don't deal directly with the registry. You have to work

through a registrar. And then resellers are not accredited by ICANN. So I would say none of the above here. Okay, with that, let's move on to the next one, the domain name system.

We've talked about the ecosystem and the various players that form the ecosystem. Now the following produced the domain name system. Just quickly, the [inaudible] that we talk about the fundamental identifier on the Internet is an IP address. It hosts connected to the Internet has an unique IP address.

You can have IP version four or IP version six, and its uniqueness is guaranteed through an allocation through a single pool, from IANA to the regional Internet registries, to the local ISPs, however there is a problem here, these numbers are hard to remember, and sometimes it changes.

It often changes. So it will not serve as well as a persistent identifier. So that is where the domain name comes in. It's a [inaudible] mechanism, through translate objects into other objects. I want to make it clear, translate objects into other objects, not simply translate names into IP addresses. Because you can use the domain name system to translate IP addresses back to domain names, as well.

There are other records, you know, mail servers, reversed which I just talked about. It's globally distributed, loosely coherent, scalable, reliable, and a dynamic database. So I [inaudible] this is another view, it's [inaudible], from a technical point of view, it's an inverted tree. You have root at the top, and then these are top levels going down that tree further.

How does the resolution process work? You go through [inaudible] resolution process. When an end user is trying to look for, trying to go to, you know, let's say, www.cnu.edu, type that into the web browser, they have a resolver first trying to look up the address record, what we call the [inaudible] record for IPv4, for [inaudible]… for the IPv6 address.

He's looking at the, followed that to a recursive or caching DNS server, and asking, do you know where, what the IP address for www.cnu.edu. Now if there are, if this has never been queried before, the cache resolver wouldn't know, but it has a way to find out. So you start with the root, he asks for the root server, what is the DNS sever authoritative part, the EDU zone. And then the root provides an answer back.

And then he went to the EDU server, saying what is the IP address, or the CND dot edu zone? The domain name server. So he went, the EDU answer back, and then he was able to make that query directly to the CND EDU dot eu server, and asking what is the IP address for www.cnd.edu.

Now the CND server provided back the answer, and that the IP address is 128.2.42.52. At that time, the browser will make a direct connection to that IP address and this one on port [inaudible], the [inaudible] protocol. So that's how, in a nutshell, the domain name resolution process works.

So as you can see, there are many components of this to make it work. That's what I want to highlight the importance, it's very scalable and distributed database, and yet it's also very coherent.

There are four components of the DNS, a name space, which I mentioned, servers making name space available, so we have, these are the authoritative servers. And resolvers query the server about name space. So these, what we call, usually call, the [inaudible] resolver and the recursive resolver, and finally the DNS protocol.

These two components make up together the global DNS. Now I want to provide some quick numbers here. There are on the [inaudible] 10 to the sixth power of authoritative DNS servers around the world. These are serving the root zone, these are serving the TLD zone, these are serving the second level, so these are the authoritative, they can provide answers, authoritative answers to those queries.

On an average web page look up, we see three or 10 DNS queries. On a heavily traffic website these days, that you usually see more. There is lots of domain names used to put an ad for here, used to put [inaudible] there, different domains. And each of those underneath is a DNS lookup to make it happen.

So there are lots of things that need to happen to [inaudible]. And on the other, there are two queries a day. That's on the other [inaudible], and that's just the queries that we [presently now?] receive. So there are, on that magnitude. I want to convey these numbers to drive the point that the domain name system is fundamental to the operation of the Internet.

Without a domain name system, when you type in something, when you type an address on the webpage, or a website, there is no way that it goes to that, the system knows what to look for. If there is no domain

system [inaudible] function [inaudible], because the mail system would know where to send your mail to, and that's how fundamental the domain name system is.

So, quiz questions.

TERRI AGNEW: Thank you. And just as a friendly reminder, as we bring up the quiz questions, if you could please use the poll in the right hand side pod.

And the question is, which of the following statements is true? The domain names [inaudible] to translate a name to a corresponding IP address. On average, there are on the order of 10 billion DNS queries a day. A root zone is a central database that stores information for the root servers. In the DNS, domains are defined in an inverted tree structure.

Once again, the question is, which of the following statements is true? The poll is open at this time.

And Steve, I did broadcast the results, if you want to share the answer.

STEVE SHENG: Thank you. The correct answer is four. In the DNS domains are defined in the inverted tree structure. Now the others are right in some sense, but they're not quite right. So the domain name system is used to translate an object into another object used to translate naming into IP address, but that's, although it's a most common use, it's not the only use.

There are many uses. For example, as a network operator, what you usually want to know is to, given an IP address, you're given to know, want to know what the domain name is, what domain name is that IP address from, and you know, that and using the domain name system, to be able to find that as well.

No one select two. The root zone [inaudible] database stored, not the information about the root [inaudible]. It's about the top level domains, you know, underneath root, the authoritative, the IP address is for the authoritative top level domains. The name servers for those, so that's what the root zone is for.

The root servers are something called, in a file called root [hint] file, that sometimes the recursive resolvers is flat, because they need to be [inaudible] to be able to find malicious server, root servers to send queries to. But it's definitely not part of the root zone.

Okay I want to move on to DNS security and privacy. This part of the presentation is going to be more technical.

So when we think about the data flow of the DNS, this is a sample data flow. On the permission inside, you have the zone file loading to the master DNS server, that's replicated in secondary servers, what we call slaves. And you can through dynamic update, to update the server, master server. So that's the provision side.

And on the publications side, you have the resolver, you have the cache forwarder, you know the recursive resolver send these queries to masters and slaves. Now there are a couple of [inaudible] associated with these. These are, you know, masters can be, the slaves can

impersonate master. You know, there is cache poisoning by data scooping.

By cache poisoning, what I mean is, sometimes the answers to a DNS query is stored in the cache of the resolver, so that they do not need to re-query. This is used to reduce the load of the DNS servers. But the miscreants, the bad guys, what they do is that they poison the cache with wrong answers. So, think about it. If you can, you know, poison the cache for a resolver, and give them a domain name, then [inaudible] is all of the traffic instead of going to a legitimate website, it's going to be directed to a malicious website.

So that's why cache poising is [inaudible]. The [inaudible]…

In terms of the DNS use something, the transport protocol called the UDP, user data gram protocol. And it turns out it's sometimes easy to make cache poisoning happen. So here, a DNS query, you know, from 1.2.3.4 to 2.4.6.8 with a reference number and the question is, what is the [A] record for ICANN dot org?

When you get that, the answer is 192.0.2.0. And then they verify, the send a… Okay. The reference number is correct. So that's how the check is. However, it's pretty easy to attack that. These are the, you know, possibilities, and when you combine them together, it's easy for an attacker to come back, to provide a first answer.

So whoever sends a first answer back, to manage the correct reference number, that will be stored in the cache, and then it will be further used for resolutions. So how [inaudible] is to do? Before it was, you know, it

was thought to be, oh, you know, it's still very difficult, even though, you know, the possibilities are not many.

But then the Internet researcher was able to make an attack happen through a technique, and it would only cause 1.3 seconds to do that. So this is a wakeup call for the community to adopt the DNS security extensions. The security extensions was developed a long time ago, but it hasn't seen much update until after the [inaudible] attack was announced.

[Would that] system use a public key topography to verify the authenticity of zone data. So what it does is the zone data is digitally signed using the private key for that zone. And then when the DNS server receive the DNS signed zone data, can verify the origin and the integrity of the data, by checking the signatures using the public key.

So this is asymmetric. You sign, you encrypt, using your private key, and then the others can verify using the public key. The private key is private to you, but everyone knows your public key. So they tend to verify that, if it's indeed brand new. So that's just a simple concept. And that's been implemented.

I won't go through here, that's what I just described. Very simple, in here, when an end user [inaudible] we're asking cdu.edu, [inaudible] just get back the IP address. Now what it gets the IP address [inaudible] the signature, by you know, signed by CDU. So that when you verify the signature, using CDU's public key, you know that, ah, this is indeed from CDU.

So this eliminates cache poison, right? Because an attacker wouldn't be able to have, wouldn't be able to sign a message using CDU's private key, and that's the, these are designed in the signature and the keys in the DNS.

I want to highlight, there are three security tenants. The availability, integrity, and confidentiality. The DNSSEC is for the integrity for the message and response, but there is [inaudible] availability, or per confidentiality. And here is the status for the DNSSEC to, the deployment status. It's the… All the new generic top level domains under ICANN's new gTLD program has to use DNSSEC sign their zone.

And then, you know, these are the ccTLDs that have RSSAC enabled, and the various statuses. Now I'll quickly move on to DNS privacy. So this is a recent effort by the IETF. In November 2013, IETF plans to [harden?] the Internet.

[Inaudible] IETF [says] pervasive monitoring is a technical attack that should be mitigated in the design of the IP protocol where possible. So it turns out the actual query reviews quite a lot, it reviews who is requesting, what it's requested, and sometimes there are sensitive information than that.

And then there are two types of, people can listen, there is the eavesdropper on the wire, and there are also the enablers. So that's what the DNS privacy efforts have protected again. The principles that IETF take is first, send as little data as possible, and second, you know, encrypt the data. The approach that is minimizing among the data sent from DNS resolvers. Because right now, when you are making a query

to www.cnd.edu, that query seems like recursive resolver, by the root server, by the EDU server, and by the CND server.

So that, the same information is displayed in all of those places. And there really is no need to be able to show those. For example, when you heard a root for EDU, you need to tell the root I'm looking for CND dot EDU. When you, you know that, kind of the amount of information, that the less you send, the better.

The IETF is currently in the early stages, so there are lots of opportunities. Your working group is called the [B Prime] working group, and also the DNS op, the DNS operations working group in the IETF. So I would encourage you to participate in their mailing list discussions and IETF meeting.

With that, that's the end of my presentation. I'll hand over to… Do we have a question, or do we have time? But I'll give that, leave that to Terri and Ariel. Yeah.

TERRI AGNEW: Hi Steve. We do have one final pop quiz question. We'll go ahead and quickly run through it. Our final question is, DNSSAC is used to solve the following problems, availability of DNS response, the confidentiality of DNS responses, the integrity of DNS responses, or none of the above. Please vote now.

Again the question is, DNSSAC is used to solve the following problems.

STEVE SHENG: Thank you Terri. The correct answer is the integrity of the DNS response. All right, so the DNSSEC itself is not the, solve the confidentiality problems, the communications be confidential. So those are being solved in the DNS privacy efforts that is ongoing. Thank you.

That's all. I want to turn it over to Ariel or Kelvin.

TERRI AGNEW: Thank you Steve. I'll now turn it over to Kelvin. He will moderate the question and answer session. And Kelvin Wong is head of outreach and public responsibility of APPAC. Kelvin?

KELVIN WONG: Thank you Terri. And thank you Steve, so much, for giving such a comprehensive update and an overview of the addressing, and security, and privacy of the DNS. I think we already have some requests for the slides. And just to update everyone, the slides can be found in the Wiki, community Wiki, and I think Terri, maybe you can do us a favor by putting up the Wiki on the chat again.

And so you can scroll down right to the end of the page to find the slides. These are very useful slides. And so that's [inaudible]. We have a question here, from a [inaudible], what is a shared registration service? If you can answer Steve.

STEVE SHENG: The shared registration service is something that an interaction between registries and registrars. So that's be able to, [inaudible] find

out, you know, what names available, and the provisioning of that. When they used something, you know, before, you know, when you have one interested player, that's not a big issue, but when you have, when you create competition with thousands of registries, and thousands of registrars, that interaction becomes very important.

Technically, [inaudible] common set to implement that, right? If the registry has their own system, and talked to each registrar differently, that will create much operational burden on the registrant. Right? And so to elevate that, they developed systems so that registrant and registrar have a common understanding, so that once the system, you know, registrars will be able to talk to different registries through the same protocol, so that they don't have to reinvent for every registry. Thanks.

TERRI AGNEW: Thank you.

KELVIN WONG: Thank you Steve. I think we still have some time, so if there are some, any more questions, please input them into the Q&A pod. Now for the second question, we have a question from Satish Babu, what is the present ICANN policy on privacy proxies?

STEVE SHENG: I think it's ongoing. I think we have a public comment that received a lot of comments, so I think the current is ongoing. I will probably ask if we can share the URLs of those public comments as well as those

reports. And the mailing list discusses with this community, so that you can join the conversation as well. Thanks.

KELVIN WONG: Thank you Steve. I think we actually have time for a question or two. If you have any questions, please feel free to enter them into the Q&A pod, or you can unmute your speaker to ask Steve. Now is your chance.

Okay. Going once, twice, okay. I think we can let Steve off for now. Thank you very much Steve. But before everyone goes… Ali has something. Ali, go ahead please.

ALI ALMESHAL: [Inaudible]… on behalf of the APRALO leadership team, I would like to thank him a lot for a wonderful presentation, which is very much informative, and would like also to thank you [inaudible] and the staff for such preparation and arrangement. And let's not forget all of the ALSs which have joined us.

If you missed anything, or you were not able to join from the beginning, the recording and the presentations all will be at the [inaudible]. Thanks to all of you.

KELVIN WONG: Thank you Ali. I think there has been some audio problem. I think Ali was a bit too soft, but thank you for the comment. And that we will be real happy to do this for everyone, and we will be sharing the slides with everyone. And the recordings, again, will be shared very soon in the

community Wiki. And before we go, I'm also running through everyone, through the survey that we have for you.

So this is a new thing that we are doing. We used to do this afterwards, but right now we hope to incorporate this at the end of the webinar, so because as [inaudible] mentioned, we really want to hear from you how we did, and how else we can do better, and what you like to see in the later editions of this webinar series.

Okay? So if Terri, I can get your help… I'm sorry. Thank you so much. So in your opinion, is the webinar well structured? Please take some time to go through. This will be anonymous. It will not be, of course we won't have your names. And so we're just going to give you another 30 seconds or so.

All right. Maybe we can move on to the next question. Overall, were you satisfied with the webinar? Let me give everyone another 30 seconds or so.

All right. I'll just go to the next question. What topics would you like ICANN to cover for future webinars?

Well, for those who choose others, there is going to be a free text for you in the next question, under general comments for you to fill in, as far as a topic of your choice. So you can click on other two, and then you can input your choice of topics in free text, in the next question.

All right. So are there any comments or feedback next? So please free to input your comments here. Of course, this will be anonymous. Nobody can see your comments or feedback.

And it has been brought to my attention that there is one more question from Peter.

STEVE SHENG: The further clarification I wanted to make is not the TLD itself, registered to registrars, but the names of the TLD, the registrar to the registrars. So thank you for catching that. I will update the slide to make sure that is clarified. Thank you.

KELVIN WONG: Okay. I think it's time to let Steve off, and thank you everyone, including those who [inaudible] here, this is a webinar series in collaboration with APRALO between APRALO and ICANN hub. And again, I would like to thank everybody for attending. And with that, thank you everyone, have a nice day ahead.

[END OF TRANSCRIPTION]