ICANN76 | CF – ICANN Fellowship Program: Intro to ICANN OCTO and KINDNS
Sunday, March 12, 2023 – 10:30 to 12:00 CUN

SIRANUSH VARDANYAN: Hello, everyone, and welcome to the second day of ICANN76. I hope you all enjoyed yesterday. My name is Siranush Vardanyan, and I welcome all of you to the session with our tech team and IANA team. And they will tell more about all these abbreviations.

But before that, just a short announcement. I will be your remote participation manager for this session, and this session will be recorded and governed by the ICANN expected standards of behavior.

During this session, questions and comments submitted in chat will be read aloud if put in the proper form, as noted in the chat. If you would like to speak during this session, please raise your hand and, when called upon, virtual participants will unmute their microphones in Zoom. On-site participants will use a physical microphones. We have two roaming microphones over here. For the benefit of other participants, please state your name for the record and speak at a reasonable pace.

We do have interpretation in six U.N. languages, and I encourage everyone, before sitting, to take the headsets other and use the interpretation. We have a great interpretation team with us.

So, with that, I would like to introduce our presenters today and would like to start with Chief Technology Officer, John Crain, who is here with

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.

his team, David and Kim Davies, who will introduce and talk about IANA. But we will start with John. John, the floor is yours.

JOHN CRAIN: Thank you very much. Glad to see you all here. As Siranush know, Fellows and NextGen are my favorite groups at ICANN because you're all fresh faces with fresh ideas, etc. So it's always good to be here. I'm John Crain. I'm the Senior Vice-President and Chief Technology Officer at ICANN. I've been at ICANN for a couple of decades or more now. It's been a little while. I'm part of the furniture, so to speak.

I run a group which is called IROS. You don't hear about this very much outside. It's very much an internal distinction we have. We are the group of acronyms. We love acronyms. So IROS is Identifier (so this about domain names, IP addresses, all the [over]identifiers) Research, Operations, and Security. The "I" at the front is the important one. We're all about identifiers and what's going on with them.

And you can sort of split that into three kinds of distinct modularities. We have a group called the IANA (Internet Assigned Numbers Authority), which is managed by this gentleman to my left, Kim Davies. And then we have a group that is very much focused on engagement around technical issues, managed by a gentleman, a friend of mine, called Adiel, but we have David to my right here. And then a lot of research. And there are two of my managers that work on that. I see one of them being very shy and hiding amongst the community. Say hi, Samaneh. Why don't you … You could even come join us if you want. And I don't see Matt, but I know—there's Matt. Matt could come and join us, too, if we wants, or he can just by shy and stay there. It's up to you.

Now those are things that we do. We do research around all things affecting identifiers. The IANA chain manages a lot of those identifiers from an operational perspective. And then we go out and talk about those things.

So I don't want to spend our time preaching to you, so I'm going to give some of these folks a little bit of time to talk about the things they're working on. And I'm going to start on what is arguably the most important thing that ICANN does because you're here at a policy meeting, but policies are only important if you can actually put them into place and actually manages those identifiers. So I'll hand it over to Kim, if you want. Why don't you tell us a little bit about the role of IANA?

KIM DAVIES: So I'll be brief because I actually have a presentation but I'll give it momentarily. IANA's role is essentially to be a central clearinghouse, repository of record, for all the identifiers we use on the Internet. I think most here know about domain names. They're usually the most commonly thought of when we talk about Internet identifiers, but by no means are the only ones. IP addresses are probably also familiar to you, but there are literally thousands of identifiers used to enable day-to-day Internet communications that you're probably not aware of. And for the Internet to work, there needs to be some centralized place where how those identifiers are assigned is centralized so it's done consistently around the world. And that's really at the heart of what the IANA function are about. So we'll get into that in a moment, but that in a nutshell is what we do.

JOHN CRAIN: Okay. And the "R" is for research. So, Samaneh or Matt, why don't you talk a little bit about the basics of what your groups do.

SAMANEH TAJALI: I'm Samaneh Tajalizadehkhoob, and I lead the research group on Security, Stability, and Resiliency (SSR) within the Office of the CTO. The topics that we are mostly related indirectly or directly to the security of DNS. It could be some of the topics that you hear a lot in the ICANN meetings, which is DNS abuse but also security configurations of DNS, all the indirect things that affect names that are also affecting abuse—things like phishing, malware, command-and-control, web security, protocol security, etc.

Now I'll pass it to Matt.

MATT LARSON: I'm Matt Larson. I also run a research team. Sometimes we do security, but not as always focused on security, as Samaneh's team does. We work a lot. We have some big data sets that we work with. We're very fortunate to have access to the traffic to the ICANN-managed root server. So we do research based on that. We also do research based on just the contents of the DNS. We have access to all the gTLD zone files and some ccTLD zone files. So those are very rich data sets as well that work on. We're also active in the standards area, particularly the IETF. So we'll so protocol clarifications and enhancements and operational-related documents as well.

JOHN CRAIN: And David, why don't you talk a little bit about the engagement work?

DAVID HUBERMAN: Sure Hi. Good morning, everybody. I'm David Huberman, and I work in this department we call Technical Engagement. And we are a staff of essentially engineers from around the world who work with both technical and non-technical communities to build good capacity and build skills around DNSSEC, around secure routing, and the RPKI angle with the RIRs. We work on engagement, especially with non-technical communities, on topics related to ICANN to ensure that everyone has a good, strong understanding of the engineering that underpins the Internet infrastructure and how the Internet is built. And we partner a lot with many of friends and colleague here in ICANN in efforts within governments and non-technical communities to ensure that everyone is talking the same language about how the Internet works.

JOHN CRAIN: That was a great overview.

I'm going to ask us to go over the questions in a minute because you've heard enough about us, but before I do, can the IROS staff in the room please stand up so folks know who to go and pick on?

Okay. So there's a bunch more of us here at the ICANN meeting. Now, the staff is much larger than this, but we bring a small contingent to the ICANN meeting so we can interact with the community and do work here. So it's important that I hear from you.

So I'm going to pass it back to my colleague here, and we'll see if there's any questions.

SIRANUSH VARDANYAN: Thank you, John. This session is especially planned for Fellows and NextGeners, so I encourage all of you to be active in asking questions because this is a unique opportunity for all of you. Many of you are note technical people, but it's very important to understand how, from a technical point of view, ICANN works. So, please, please, please don't be shy. As I told you during the first session, there are no stupid questions ever. So please ask questions, and we can start from now even. Whatever is interesting for you. We have microphones. If I can request two microphones to be over here. We do have [them], I guess. So, anyone, raise your hand. Yeah, the mics are coming. Just give us two seconds.

Yes, please. Over here. Can you take the mic? And then it will start over here.

Nicolas, we'll come back to you, yeah. Thank you.

HARISH CHOWDHARY: Hello, everyone. I am Harish Chowdary, ICANN Fellow. So I'm a research scholar in the National Forensic Science University in India, and my research is around DNS security. So my question is, to the research team, how can I contribute? Because I'm specifically working on dot-in ccTLD security and related measurements. So how can I contribute to the work? How can I learn the new technology from the team so that it will help both of these? Thank you.

JOHN CRAIN: Samaneh, do you want to take this one?

SAMANEH TAJALI: Yes. Thank you, John. Thank you for the question. Happy to have you here in the room. Actually, I know for a fact … I don't know if you guys know about the DAAR project at ICANN which has been around for four years now. It's called Domain Abuse Activity Reporting tool. And dot-in is a part of that project. So we are in kind of a collaboration already with dot-in. I would like to hear from you what kind of security topics you work on if you can facilitate, if we can work together, if you can provide data that is useful or talk about it. Point to the right directions if you need. But we do a lot of work around TLD security, so there should be areas that we can either direct your or be of use of some sort.

JOHN CRAIN: Yeah. And if I may, we also publish a lot of documents in something we call the OCTO Series. If you see one of those and it's interesting and you think it's good or you think it's horrendous—hopefully never that—write to us. Comment. Please take time to go and talk to Samaneh or any of the members of the team here. We're always looking for people to collaborate with and figure out if we're doing the right research or if there are ways we can improve our research.

SIRANUSH VARDANYAN: Thank you. Nicholas, please? You are the next.

NICOLAS FIUMARELLI: Hello, OCTO team at ICANN. I have here the routing security is not part of ICANN's mission or objectives, but you recently mentioned about RPKI and its importance on routing security. So how you can clarify how routing security fits with ICANN's work, if at all?

Additionally, if routing security is indeed part of ICANN's research, I'm curious about the resilience of the infrastructure of big companies and popular apps. For example, a few years ago, there was an incident involving Meta (formerly Facebook) that involved DNS and BCP failures. Can you find any insights into how companies like Meta handle routing security and what steps they take to ensure the infrastructure is resilient? Thank you for your time and insights.

JOHN CRAIN: Well, that was a lot of questions. I'll try and break some, and I'll start with the first simple one, and that is, is routing within ICANN's remit? So ICANN is not about DNS. ICANN is about identifiers. If you consider routing to be to IP addresses what resolution is to DNS, then obviously we have an interest in that.

Now, when we're dealing with things around the DNS, our partners—because ICANN is part of a community—tend to be registries, registrars, and resolution providers. And in the IP addressing world, our partners in those discussions and research tend to be the RIRs (Regional Internet Registries) and sometimes ISPs, etc.

So it's a different area to the DNS, but we don't do just DNS.

Let me pass it over to David to talk a little bit about some of this stuff.

DAVID HUBERMAN: Hi. It's a great question, and it's a question we sometimes talk about inside as well because we never want to overstep our remit. But the truth is that the RPKI and this greater idea of routing security, where, as Internet service providers and all participants in Internet routing pass traffic and pass announcements about who they are—"Hey, this is my network; these are the services I have.; if you want to get there, come to me through these routing announcements"—for 30 or 40 years have been very insecure.

Well, now we're securing them. We're securing them behind an infrastructure that can hopefully prevent a lot of the accidents and a lot of the abuse that you sometimes read about. And as an industry, of course, we don't want you to read about that because we don't want it to happen because we want the underlying infrastructure to just work so that, when you pick up your advice, you can go to any sites you want, and it just works, and you don't have to think about it. So we have this layer of security that we're building on top of it, and we need to make sure it's done well and it's done right.

At the same time, we also have to be cognizant of the fact the entire names and numbers infrastructure, which we are very much of course within our remit on, is behind this security infrastructure, is behind this layer of security. And if it's not done well and we can't access nameservers and resolvers, if we can't access the various components that we look at, that's a problem, right? So we pay a lot of attention to it.

Now, you asked specifically about Meta. You asked about how, back in October 2021, Facebook was completely unavailable for almost an entire day. And the reason was because of the DNS. It's a meme in the Internet world that, if something breaks, it is the fault of the DNS because, remarkably, it is very often the fault of the DNS.

Here, Meta had a very interesting configuration where their physical access to buildings, like getting into a data center, getting into a Facebook office … They used badges, like any other corporation, right? But the whole system was tied to a system of DNS. And in order to authenticate who you were, it used the DNS to find the repositories where that information was, right? But there was a breakdown inside. There was a failure inside that cascaded and made the DNS unavailable to not only the world but to all of the systems inside of Meta. So that meant, when you badged into a door, in order to authenticate it, it needed the DNS to find you. But it didn't have access to the DNS. Okay, that's a wonderfully creative way to break things.

And what I think it taught not only Meta but taught everybody is to really think about, when you're building infrastructure, whether it's corporate IT, whether it's this gigantic WAN that lots and lots of people rely on for access or for content, you really want to think about the interplay between routing, authorization, authentication, and the DNS. And don't accidentally create failures that can cascade and make you an island that no one can get off of.

So it was very interesting incident, and I think everybody learned a lot from it.

JOHN CRAIN: And if you look around the meeting space, you may find people from Meta here. It was their network and their issue, so maybe go get their take on it.

SIRANUSH VARDANYAN: Thank you. For the interpretation purposes, please speak at a reasonable pace.

We have a remote question from Shannelle McPherson, ICANN76 NextGenner. So had to drop for the last minute, but her question is from John Crain's team. "How is DNSSEC deployment, and how can a country ISP get involved with implementing this?"

JOHN CRAIN: Okay, well, firstly, Shannelle, I was sorry to hear you couldn't make it. And hopefully we will meet in the future somewhere. Hopefully, you'll keep applying to come to ICANN meeting, and we'll see you next time.

I'm going to pass first off to Kim to talk about how this put into the roots, and then I'm going to ask David to talk a little bit about the work we do around engagement around DNSSEC. So Kim, why don't you talk a little bit about the root?

KIM DAVIES: Thanks, John. So one of the IANA functions that we haven't discussed yet is managing the DNS root zone. The DNS root zone is arguably the most critical piece of the DNS. It's the first place that computers that are accessing the DNS go to to find an address that they're looking for. It contains the authoritative record of what top-level domains exist and

where the servers that are responsible for those top-level domains are on the Internet.

Part of our responsibility in managing the DNS root zone includes managing the cryptographic keys that secure the root zone for DNSSEC. It's a particularly involved part of our operations. In fact, we have a lot of resources dedicated just to that one function within IANA. And the reason for this is simple. DNSSEC works by essentially having one central key that everyone relies upon to kickstart that DNS lookup process. And it's very critical that key be kept in a very secure manner and in a trustworthy that the community recognizes is being done in a way that doesn't introduce any risk of unauthorized access to that key.

So the way we do this is that we keep that key secure. It's part of our responsibilities. We keep it in a couple of very highly secured facilities. And every three months, we go and access that key to make use of it through very public events we call key ceremonies. We bring the community along. We livestream it. It's a very public event. But we do it in such a way that security experts in particular can monitor and watch what we're doing and can come out of it saying, "Yes, ICANN followed a good procedure there, did it in such a way that there's no risk that that key is being used in an unauthorized fashion." And everyone walks away satisfied.

And so, like I said, that's a key part of our operational processes. I can give an hour-long description of how they work. It's quite an interesting subject. But that's really one of the most fundamental responsibilities that IANA and, in turn, ICANN has for DNSSEC security.

But I note that the question was about what an ISP in the context of the DNSSEC. So I'm going to pass the mic over to talk a little bit about that.

DAVID HUBERMAN: Sure. After Kim's team has done a great job ensuring DNSSEC is up and running in the root zone, then we have to use it. Well, how do we use it? Well, we go to the next level down, which is the top-level domain: dot-com, dot-org, dot-museum. Or, here, I'd like to focus in on country codes. We're in Mexico: dot-mx. So if we want to set up DNSSEC in Mexico for any domain that is under the dot-mx TLD, we go to the registry—the registry operator for dot-mx. And that registry operator signs their own zone and offers DNSSEC signing and validation to every domain underneath it.

So I'm looking out at the audience, and I see my colleague, Nicholas Antoniella. Nicolas, who's in Uruguay in South America … And what Nicolas does is he'll go around to different ISPs and different country-code top-level domain registry operators, and he'll work with them to set up DNSSEC signing, to teach them everything they need to know about how it works and, importantly, the tooling you need in order to maintain this. And he can work with ISPs to make sure that they're validating on their resolvers, that, when domains are DNSSEC-signed, they can validate their signatures and pass them on.

So ICANN works at the root level to ensure that everything is signed and to make sure that everything can validate with keys. And then ICANN also works with the ISPs and with the registry operators to ensure that they have all the knowledge and all the tools and all the support they need to offer DNSSEC at the next levels.

SIRANUSH VARDANYAN: Thank you.

Setondji, I think you have your hand raised.

Thank you, Betty, for helping me.

And then, Oliver, we'll come to you and Firuz.

SETONDJI HOUNZANDJI: I would like to speak in French, please. Thank you. My name is Setondji. I'm a system administrator, and I'm managing the Linux server. And I am from Benin, but I live in France.

My question contains to ccTLDs. I am very interested in everything that pertains to DNS, and I work on how to secure DNS servers. So my question pertains to ccTLDS because, as you know, in many countries, ccTLDs and registries are chosen by a governmental decision. And we noticed that, very often, ccTLDs are poorly configured, poorly managed, poorly administered. My problem is to find out whether it is possible to have ICANN audit all ccTLDs to issue rules on what needs to be done. You know that, today, a lot of ccTLDs did not implement DNSSEC. So what ICANN do?

I would like for ICANN to force people. So, for example, you could launch an audit on some ccTLDs, and you tell them, "You are not up to date, and we cannot continue to do business with you. And we will send an auditor. We will impose certain things so that you can be updated," because, if European and American ccTLDs are secured but not

Africans', that a problem. We said that ICNN is one world, one Internet, so we shouldn't have one world and many Internets.

That was my question. Thank you.

JOHN CRAIN: Okay, I broke that down into two parts. One was some statements about the status of the ccTLD environment and the technical status of them. And you made some interesting comments there, but I'd love to have a sidebar discussion about that because I'd love to see what data you have because, as researches and scientists, we're really interested in data. So you made a lot of statements there about quality of infrastructure, and if you have data that supports that, we'd love to get it. If not, we'd like to have a discussion about what is seen and what is not seen. One of them was you said a lot of ccTLDs are not signed. I think that is a judgement because there are a lot that are. So we can have a data discussion.

The other one was about not a technical issue at all really but the policy issue around how ccTLDs are managed. Now, ccTLDs do not have their policy set by ICANN or within ICANN, but the ccTLDs are country codes, and they have a different mechanism. So there is no mechanism for ICANN to go in and force particular policies in this area. It doesn't exist. What we do is we collaborate a lot—I mean a lot—with ccTLDs. And David can talk about the amount of work we do with ccTLDs.

So exactly forums like ICANN are places where you can come and discuss these kind of issues and discuss policy issues. The ccNSO is where a lot of the ccTLDs come together and work on all these kinds of

issues. They have a Tech Day at most ICANN meetings, if not all, where they discuss these issues.

So there is a lot of collaboration amongst the ccTLDs and with ICANN and especially some of my staff around improving things, but I think an audit for us requires the ownership of that policy process. And that policy process does not sit within ICANN.

So, no, there will not be, in the foreseeable future, a situation where ICANN can walk into a ccTLD registry and audit. And with the way the policy developed, one could argue that there should not be because it is not our remit. It is not our role.

Kim, I don't know if you have anything to add to that, or …

KIM DAVIES: Yeah. I think that was a good summary. I think it's just worth reemphasizing (because it might not be familiar to many of you here) the difference between a generic TLD (gTLD) and a country-code top-level domain. For generic top-level domains, much of the policymaking that happens at an ICANN meeting like this is around setting the rules and requirements of what's required to operate a gTLDs and the parameters within which they operate. And a significant part of ICANN's work is, once those rules are decided by the community, to implement those rules and then to monitor adherence to those rules. So ICANN has a Contractual Compliance department. Each operator of a gTLD needs to meet certain requirements to be able to continue operating it successfully. And if they don't meet that mark for an extended period of time, there are remedies available to that.

It sounds like you're seeking some kind of arrangement like that, possibly for ccTLDs, but for ccTLDs, it's quite a very different relationship. Back to the very beginning of the DNS, back in the 1980s, a decision was made—a decision that has been kept until now—that ccTLDs are really vested within their respective countries. ICANN's role is relatively limited: to find a trustee within the country that will operate the ccTLD for the public good within that country. And the concept is that within that country will be all the relevant oversite mechanisms to ensure that that operator stays accountable and does what is necessary. Obviously, it's a complicated world, any many different countries have many different mechanisms for that. Some are better than others. That is clear.

I think what ICANN can positively do through our technical engagement activities and things like that is to promote best practice to do capacity-building, to help inform ccTLD managers about what their obligations are and how to fulfill those obligations. It's such a powerful and fundamental component of ccTLDs that they are operated in the country, that the operators have not complete control but largely are responsible locally for how it's run. That means that our mission and our mandate is relatively limited when it comes to ccTLDs. Thank you.

SIRANUSH VARDANYAN: Thank you.

Do we have some [destruction] here?

Okay. We'll take one more question from here and then one remote and then we'll give the opportunity for Kim to do his presentation. And we will continue with [the candy game].

OLIVER RISTESKI: Hello, my name is Oliver. I come from Macedonia. I work in the Ministry of the Interior. As well, I'm a part of the Center for Security Research. My question is relating to that recently we were faced with receiving e-mails with fake bombs in public schools, airports, malls, and transport centers. It cost a lot of spending of resources for our ministry. Tracking of this crime is so low. And efficiency of exploring/investigating this crime is so low. Also, this issue is common for all the [inaudible] Balkans. Are there any possibilities for doing research with these issues?

JOHN CRAIN: Sounds like you're talking mostly about the phishing exploits, etc., and malware and things like that that are just abhorrent and are a part of our day-to-day life on our Internet. Yes, we can do research around that when it relates to the domain name system.

And I don't know, Samaneh, if you want to talk a little bit to some of the research we're doing.

SAMANEH TAJALI: Thank you for your question, Oliver, and thanks, John. So like John mentioned, this is a very day-to-day typical problem that most Internet users have. We at the moment in the SSR group are doing research on

it. It will be published soon: identifying methods or more efficient methods to classify phishing e-mails into different categories of spam, malware, etc. So keep looking at our OCTO docs or publications. We are planning to publish our methods. First you're going through academic publication, but once that's peer-reviewed, you are going to publish the methods. Maybe the methods is useful to be implemented in other areas, providers, operators, etc.

JOHN CRAIN: And there are other things that you can think about. Now, if you have a national cert, ensure that they are a member of FIRST, which is a body for certs around the world. ICANN itself is actually a member of the FIRST, which is the forum for instant responders. So get involved in that community. Make sure that your incident responders are in the incident response community because this is not a problem unique to anybody.

The other thing you can do long-term is invest in your universities in building up the talent and country to understand all these, whether it's research or incident response or even just good networking skills, etc., as in technical networking. That's another thing you can do.

Now, if you are really interested mainly in the public safety aspects of how the Internet is used and you're wondering how you can affect or be involved in policy in that realm, we have a Government Advisory Committee. It's a very important part of the ICANN process. And within that, they actually have a working group called the Public Safety Working Group. So if your government is participating in the GAC, and they have a specific interest in this area, then the Public Safety Working Group is something for them to look at and get involved in here.

Now, at ICANN we focus on something we call technical abuse or security threats that are related to the identifier system. So not all of the threats that you see on the Internet—in fact, many of the threats you see on the Internet—are not related to the work you do. But that particular subject is always a hot topic at ICANN. And at this moment, there are various things happening within the community. There are contract negotiations occurring around what it means to be a registry and registrar and what you need to do about DNS abuse. The current contract states that you have to receive reports and investigate them. Those are not the exact words in the contract, but I'm not a lawyer. But one of the things missing from our contractual language is that these people have to mitigate the abuse. And we are working at the bequest of the contracted parties—the registrars and the registrars. They came to us and said, "We want to add this to our contract, so we are obliged contractually to mitigate abuse." So that discussion is ongoing at the moment.

We do a lot of training. Samaneh and our group do a lot of research and publications in this area. So it is something that we're very, very interested in.

If you have law enforcement that would like to talk to us about education and outreach, we are happy to talk to them. We have people on our staff that spend a lot of time talking to law enforcement around the world. Our main remit is explaining to them how the ecosystem works, and sometimes it is also to do the introductions between them and others in the ecosystem, building trust, if you like, because that's very critical to our ability to do the work for everybody.

So come talk to us, and we can have a one-to-one discussion about maybe how we can help your ministry and your government get more involved.

SIRANUSH VARDANYAN: Thank you.

Can I request the tech team to have the IANA presentation up?

Meanwhile, I will ask the questions from remote participants. Romulo Chacin, ICANN76 NextGenner, would like to know how the different security threat mitigation projects and programs interact between them"—so between each other, I assume.

JOHN CRAIN: How long do we have? I mean, if you look at ICANN's core remit, if you look at our bylaws, if you look at the purpose of ICANN, it states very clearly that we have to worry about the security, the stability, and the resilience of the Internet, of the identifier systems. So that's not people's websites, etc., but it is the name that … Hello. Hello, neighbors. I'm hearing … Huh, I'm hearing voices.

So in some ways, it's core to everything we do. So everything interacts with security. Every time at ICANN as staff and also most of the time as community when we're looking at something, we always have that in the back of our minds. How does this affect security? How does this affect stability? So everything interacts.

Now, within our group—and I introduced you to a bunch of people within IROS—IANA is doing its job well, which they always do because

they're awesome, is critical to the security of the system and the stability of the system. We have to have good registration of identifiers. And then we do research and we do outreach and education. So that's what we do. But we also have, as Kim said, compliance to our contracts. We have contract negotiations. We have enablement of all of these policy discussions. And everything has an effect on the security and stability of the identifier systems because, when it comes down to it, that's our job. That's what we do.

SIRANUSH VARDANYAN: Thank you.

And Kim, if I can give the floor to you to introduce IANA's work, please.

KIM DAVIES: Certainly. So it seemed like a good opportunity, while we're having this discussion, just to do a quick tour through what the IANA functions are. It's something that you'll probably hear a lot during an ICANN meeting. And the term "IANA" is just thrown around, assuming that you know what it means. So this is just intended to be a relatively brief overview of what the IANA functions are comprised of. And hopefully that will be illuminating, too. We'll resume the questions after. So if anything comes along that you'd like us to elaborate on, please let us know.

So we talked a little bit about this already: IANA, the Internet Assigned Numbers Authority. Despite the name, we do more than just numbers. We do names, too. We do protocol parameters. We do all sorts of different identifiers.

In essence, it's one of the oldest institutions around on the Internet. Back in the very first years of the Internet, when it was a research project, when those first nodes were connected in the late 1960s and early 1970s, someone needed to keep records about what computers were connected to whom. And that role was played vey early on by a man named Jon Postel. He's the person on the right in the video next to Vint Cerf. And Jon Postel was the personal embodiment of IANA in the very beginning.

Later, IANA got its name and became sort of a name that was thrown around in the 1980s. IANA grew to be more than just one person. It became a team.

But ultimately, that was its original purpose back then and is still its purpose today: what are identifiers used for, and where is there an authoritative record of what those identifiers have been made to do?

So it was in the 1990s that it was recognized that the IANA functions in particular and management of the root zone really need some more formal structure than just an academic person (Jon Postel worked at a university) beyond what he could do individually and with his team. There were efforts throughout the '90s to formalize this, to recognize the commercialization of the Internet, the growth of the Internet, and the increasing demands on the IANA function.

ICANN was created to be the home of IANA. That was its original remit. In fact, before ICANN had a name, it was called the New IANA. And ICANN today still exists for that fundamental purpose. ICANN has other identifier remits beyond just the IANA, but IANA is still core to ICANN's mission.

So ICANN today is a department of ICANN, and it maintains registries (and I use "registries" here as a general sense—not domain registries but registries as in an official record) of the Internet's unique identifiers. Each of these registries has a different policy, so part of our team's work is to apply those policies depending on the type of identifier and the situation involved. So when you hear "IANA," it's referring to this allocation function, this official record-keeper function that's operated by the IANA department within ICANN.

So why do you need an official record keeper such as IANA for the Internet? Isn't the Internet sort of free from any centralized control? Computers talk to each other using technical protocols, and it's really important that those technical protocols are the same so computers understand one another. Whilst the content is transmitted over those protocols, those core protocols are things like TCP/IP, as one example.

They need to work the same way on every device for the network to just simply function, so a lot of the work that we do in IANA is not so much the protocols that you see, like domain names, but things that work below that in lower levels of your computer and in your networking device to ensure that the transmission between different Internet devices works, is accurate, that that file attachment that send is received at the other end in the correct format, and that, when you connect to service, you don't get a voice call instead of a website. Things like that. So all these identifiers have a particular purpose to aid that communication. And it's primarily used by software vendors. Software vendors use those IANA assignments to make sure that their software works with everyone else on the Internet.

So today the functions are performed by the IANA team. There's multiple different contracts. It's quite a complex mess of contracts, to be honest with you, but nonetheless, there's quite a lot of contracts that govern how the IANA functions are performed today.

Another term you might know or might hear this week is PTI. PTI is an affiliate of ICANN. Think of it like a subsidiary of ICANN that actually performs the IANA functions. For most intents and purposes, PTI is not an important distinction to make. One of the safeguards that were implemented in 2016 when the multistakeholder transition for ICANN happened was to put the IANA functions in a different organization to ICANN but an organization that ICANN controlled, and that is PTI. So you'll hear PTI. My advice is: don't worry too much about the term PTI. Just know that it is the formal legal name of the entity that runs the IANA functions.

Day-to-day operations? We function just like any other ICANN department. So we're about 16 people, and this is our bread and butter. This is what we do as our job.

So what are the IANA functions just in a little bit more detail? Typically, we divide them into three sections: protocol parameters, number resources, and domain names. This distinction is a little bit arbitrary. There's a bit of overlap between these segments. But for a high-level discussion about the IANA functions, it works quite well to split into these three areas.

The first one I'm going to focus on is protocol parameters because they're basically the most fundamental aspect of what we do. Protocol parameters. There are thousands of different types of protocol

parameters. There are hundreds of thousands, if not over a million, assignments of protocol parameters. They're numerous. There's many of them. 99% of them none of you have ever heard of. 98% of them I haven't even heard of. There's a lot. And a lot of them are used in very specific applications. Unless you're creating software to a do a very specific thing, you might not ever need to use one of these registries. But for the five, ten, or 50 people that work in a very specific industry that implements software around one of these unique identifier sets, the work that IANA does is invaluable. There's an index at IANA.org/protocols if you want to get a sense of the full list, but there's a lot of them there.

For protocol parameters, IANA plays a direct role in that implementors, which are often software vendors and protocol developers, come directly to IANA, talk to our team, and get the allocations they need from us directly. This is the key distinguisher from domain names and number resources that I'll get to in a moment because, generally speaking, people do not come to IANA to get a domain name. People do not come to IANA to get a numbers resource. Instead, they have these hierarchical allocation systems where there's middlemen. There's different people with different responsibilities. IANA just plays a small piece of the allocation story there. And part of the reason for that is there's a lot more policy to apply for number resources and domain names.

So where do these protocol parameter registries come from? The vast majority of them are developed in the IETF (Internet Engineering Task Force). This is the primary standardization body for the Internet. It's more where most Internet standardization happens—not all but most.

And when people develop Internet standards in the IETF, a component of that is developing IANA registries to go with those Internet standards.

You might have heard of RFCs. This is a document series that is where Internet standards are published. And many RFCs either create, refer to, or modify IANA registries. They include instructions on what IANA needs to do and the policies that it needs to enforce.

To talk a little about number resources, for those not familiar, number resources typically refer to three key things: Internet protocol version 4 addresses, Internet protocol version 6 addresses, and AS numbers. For those not familiar with IP addresses, there's these two flavors: v4 and v6. But these are unique numbers are that are assigned to every device on the Internet. Your laptop has one. Your phone has one. Your smart device at home as one. Your T.V. probably has one. Increasingly, many different things in the world have them, and it is the unique identifier that used to transmit from one device to another. At its heart, when a transmission is made over the Internet, every transmission known as a packet needs to have a "from" address and a "to" address. And the "from" and the "to" are IP addresses.

Because there is literally billions of these addresses, you need some way to aggregate them into big sets to make this kind of easy to handle so network engineers don't have to type in every single IP address individually. They way they do this is with Autonomous System numbers, or AS numbers. They way I like to think about AS numbers is they're kind of like postal codes of the Internet. Network providers will group big sets of IP addresses together under a single number—an AS number—and then, when they talk about where to traffic over the

Internet, they use AS numbers instead to make it a much more easy task.

So I talked about what these are. I will note that version 4 IP addresses- we're all out of. We gave out the last of the available IPv4 addresses some years ago. Regional Internet registries that assign them to networks are mostly out as well. So there's very little supply of IPv4, which is why you'll hear that there's a lot of initiative to move to IPv6, which has a lot more capacity for growth of the Internet.

So I just mentioned regional Internet registries. For those not familiar with the concept, I mentioned before that you don't not come directly to IANA for an IP address. What happens is you as an end user are automatically assigned an IP address by your network provider. They use a protocol, DHCP—another one of those protocols behind the scenes that IANA works on. DHCP allocates you an IP address individually for each device. Each network provider, whether it's your ISP or a hotel conference network, has a set of IP addresses that they share amongst the people in their facility or on their network.

Where do they get their blocks? Well, they go to a regional Internet registry. There are five regional Internet registries. LACNIC is the regional Internet registry for Mexico here. And for each of those, their bread and butter is assigning these AS numbers and IP addresses to network operators within their region. The RIRs, in turn, get their allocations from IANA.

Lastly, domain names. What's our role for domain names? I'll skip through this. So, DNS hierarchy-wise, the most critical piece of the domain namespace is the root zone. And that is an essential part of

what we do in IANA. You can see just below the root on this diagram the top-level domains. In turn, they assign labels before that, second-level domains, and so on and so forth.

So our primary responsibility within IANA is administration of the DNS root zone—again, this is the authoritative record of what is a top-level domain—and then all the technical information that goes with that and also administrative information, like who are the points of contact? What is the actual company that runs that TLD? Things like that. So we are the official recordkeeper of those facts. We receive requests from those operators to make updates and administrative changes to their TLDs. We do due diligence on certain types of requests. And then once IANA is satisfied that any changes to the DNS root are appropriate, we send those through for implementation in the DNS root servers.

I mentioned this earlier as a result of the questions, so I'll be quick on this, but we do manage this key-signing key, this central key that secures the DNS as well. We do that with key-signing ceremonies. The reason we do this in a very public fashion is to promote trust. We could do all of our work for DNSSEC and securing the Internet in private and just say, "Hey, we're ICANN. Trust us," but a better way to do it is to bring you all into the process, to give the community access, visibility. And we believe that better promotes trust because everyone can see with their own eyes. They can look at what they do, and security experts from around the world can look at what we do and collectively look at that and say, "Yes, it's being done in a secure and safe way. We can trust this system works."

Just some other functions we do in domain names as well. We do operate dot-int, one of the top-level domains. This is solely for intergovernmental treaty organizations. It's not available for general registration. We also operate dot-arpa. I'll summarize dot-arpa as technical plumbing. It's a domain you'll probably never see directly, but it is important to certain Internet operations. And we also operate a repository of label generation rule sets. This is where registries that operate internationalized domain names share and adhere to best practices.

So that sums up the scope of the IANA operations. Obviously, this is a very high-level description. But I just did want to finish by noting security. Actually, you know what? I'm going to skip that slide. Some other aspects of IANA.

I think underlying everything that we do is impartiality and neutrality. We're here to implement the policies as written. We can provide advice but in a neutral way. So that's part of what we do in our engagement here this week. We have a strong focus on performance. There's lots of SLAs that govern what we do. We're constantly measuring what we do. We're constantly reporting what we do. So that is key. We want to continuously improve, so that's another part of our work: continuous improvement. Part of that is having external third-party audits and generally having accountability of the community. There's a lot of oversight committees and so forth of IANA that you'll come to learn about in the ICANN space.

So in summary, IANA maintains registries of unique numbering systems. They're there to keep the Internet interoperating. Most IANA

registries are pretty straightforward. People come directly to IANA. You probably have never heard of them. They're pretty easy, but there are some complex, high-profile ones. We talked about the root zone. We talked about the key that protects the root zone. And for those, IANA is sort of the global root for those naming systems.

So that is the 10,000-ft. view of IANA. Thank you.

SIRANUSH VARDANYAN: Thank you, Kim. This was informative. And for our participants, this PowerPoint presentation is uploaded onto the ICANN76 website under this particular session's detail. So if you want to download that and use it, feel free to do it.

And we can take several more questions now. We do have 30 minutes allocated for that. So please don't be shy.

Firuz, yes, I know you are in turn. Please go ahead, Firuz. I see David? Yes. But we'll start …

FIRUZ AZIMOV: Hello. My name is Firuz. I'm an ICANN Fellow. And I was waiting and I have two questions already. My first question is about … As we mentioned earlier Meta's problem, I remember that there was also a problem with Meta about that Meta subnet. was announced by another ISP. And this happens usually. Within our country, we had this problem: our subnet allocated for DNS was announced by another ISP. And we lost the Internet not only for this subnet but for all our users. And my question is, does it [inaudible] a solution is to prevent this type of

problem. And every border router on the Internet must have an RPKI check enabled before installing a [route] in a routing table. And how can we prevent it and make stability in, as you mentioned, in lower layers(for example, in Layer 3)?

JOHN CRAIN: Okay, so this is another discussion about how we secure routing. What you're referring to is often referred to as a BGP hijacker.

I'm going to hand it over to David to talk about this a little bit.

DAVID HUBERMAN: So RPKI helps that issue to some extent. What's interesting is that the issue you just described happens every single day on the Internet, sometimes multiple times a day. Our friends at the Internet Society actually set up an observatory to look at these events, and they're measuring 500-1,000 of these events every single year. And these have been going on since the 1990s. This is nothing new. Some of this is malicious. Some of this is intended for someone who wants to create a mischief for some reason. A lot of it is accidental because, for many, many years, engineers building the Internet actually hand-typed configurations into routers. And we're humans, and we make typos. We make mistakes. And when you make a mistake in a router, that can be very bad. RPKI is designed to help with much of that but especially that second scenario, especially the human misconfiguration. RPKI helps a lot.

What I like about RPKI is doesn't require every router that speaks BGP to validate announcements. What it turns out as is it actually only

requires the largest transit networks in the world to do so because, when we share routing information from your ministry, from your ISP, to here at the ICANN meeting network here in Cancun to Facebook in California to something down in Venezuela or something, all of those packets will typically go through a fairly small number—about 800 or so—large Internet providers who provide transit for these packets. And it turns out that, if just those 800 or so providers validate and sign routes, anything that's invalid gets dropped there, and traffic doesn't get to where it's not supposed to be.

So one of the success stories of RPKI and secure routing in general over the last few years is 100% adoption for the 800 or so largest ISPs in the world to validate packets, which means, if you operate a network or if you regulate a series of networks, it's critically important that those networks issue the certificates, the ROAs (Route Origin Authorizations) for their routing prefixes to ensure that everybody can validate that.

To fully secure the channel, to fully secure communications, we need not just only RPKI. We also need to validate the path. A packet, when it leaves your device and goes to its destination and then comes back, goes through a series of intermediary networks, and we need to ensure that path is validated the whole time so that—what we call a man-in-the-middle attack—someone can't take that packet and start handling it when we don't authorize them to do that.

The IETF, the engineering community, has some solutions. We're continuing to develop and work on better solutions that everybody can implement. And that will be the next stage of our security journey in the routing security world.

SIRANUSH VARDANYAN: Thank you.

David, if we can go for … And then Nicolas. I know you have a question about IANA.

DAVID MONDRAGON: Hello, everyone. This Daniel from NIC Costa Rica, Senior Network Engineer. NIC Costa Rica is responsible for the TLD domains in Costa Rica. I have two questions. The first question is, is ICANN or IANA doing any efforts to force policies or technologies to use DNS or TLS instead of DNS-over-HTTPS? Because that might be a problem for most network engineers.

The second question is, what is IANA and ICANN's point of view about this issue from a political routing and security perspective?

JOHN CRAIN: So the first one is easy. The answer is no because it's not within our remit. We study these things. We measure them. We're interested in them. There's a lot of discussion in other areas around the effect of this. If you're doing research and you're looking at the DNS packets and you want to go into the packets, obviously you can't do that under [DAAR] and things like that. And you can have an argument. Is that good? Is that bad? I don't know the answer, so I'm just speaking from a personal perspective because there's always a tension between security and privacy in these kind of technologies.

So I don't think we have a particularly official stance on DoH. We've done some research on this.

And because Matt has been really quiet, and I want to see if he's still awake and he wants to talk to this.

MATT LARSON: I am. I'm awake down here. Yeah, we have done some research on DNS-over-HTTP and DNS-over-TLS. In fact, Paul Hoffman on the research team has contributed to those efforts from a standards perspective. So we've helped actually develop those standards.

Given the overall increasing interest, I'd say, in privacy, I think it's inevitable that we're going to see more and more deployment of those protocols.

At the same time, however, they're more computationally intensive and more network-intensive because normal DNS is simply one packet for a query and one packet for a reply. And maybe that happens over a TCP connection, in which case there are a few packets exchanged to set up and tear down that connection.

But once you start talking about adding cryptography to that, you're talking about increasingly complex interactions with more packets. And providers who answer a lot of DNS queries, like TLD operators and root server operators, are a little nervous about what that means for their infrastructure. If suddenly every query coming in is not just one packet over UDP but instead requires a connection to be set up and cryptographic validation to occur, that's a lot more intensive. And so

people who run critical infrastructure at scale have concerns and questions about that.

But I think, as an industry and as a society, that's where we're going. So I think it's inevitable that we'll see increased deployment of those protocols.

SIRANUSH VARDANYAN: Thank you.

And, Daniel, apologies. I called you David.

Nicolas? We'll take one more question from Nicolas, and then David will introduce the KINDNS program for all of us. Thank you.

NICOLAS FIUMARELLI: Thank you. I participated virtually in the last KSK rollover last week, I think. It's a question related to that but also related to the [inaudible] DNSSEC. Are there any ongoing efforts within the IETF to incorporate post-quantum cryptography into the DNSSEC protocol, especially regarding the administration of the root zone? And given there are already efforts to include post quantum algorithms in other protocols at the IETF, what challenges does the PTI team anticipate in implementing these new algorithms inside DNSSEC, and how do you plan to address these challenges for the security and stability of the DNS system? Thank you.

KIM DAVIES: Thanks for the question. So as of right now, we don't have any post-quantum cryptography initiatives actively on our radar, but we are doing some preparatory work to change the cryptographic algorithm in the root zone. So today we use RSA-SHA256. And we've never actually changed that algorithm. And it's unclear if changing the algorithm will be difficult or easy. So we actually spun up a community design team just in the last few weeks. They're meeting in two weeks in Yokohama to talk about this at length. And really the purpose of that design team is to work out how you even change the algorithm in the root zone, whether it's post-quantum cryptography or maybe it's just something else like an elliptic curve cryptography algorithm that will result in smaller packet sizes [and] other beneficial outcomes.

So we're really at that stage. I think it's premature to start thinking about post-quantum cryptography. It's definitely, I'd say, loosely on our radar.

But in terms of what activity is going on in that space, I'm probably going to hand it over to Matt to talk about research activities because definitely from where I sit operationally, I think post-quantum cryptography is more of a research activity at the moment.

MATT LARSON: Thanks, Kim. Thanks for the question. So this is a chance for me to refer to the OCTO document series that John mentioned a few years ago. So we've actually written document about this. I'm not in the Zoom room, so I can't paste the link, but it's called OCTO-031: Quantum Computing and the DNS. And it's exactly about this topic. Because post-quantum crypto gets increasing attention, OCTO commissioned a cryptographic

researcher—very well-renowned—to do research into post-quantum and to write a paper about that. So it's readable, but it's an intense paper. And so we did a more general version of it, and that's OCTO-031. And that gives our opinion on the state of the industry and what we have to worry about for post-quantum cryptography. And I think the answer is: we're a long, long way from needing to worry about post-quantum algorithms because we're a long, long way from a quantum computer that can even remotely be able to pose a threat to the algorithms we use for public key cryptography today.

So I think this is an example of that there's a lot of hype in the industry and people talk about it. And the sense that you could get from just reading trade publications is, "Oh, my! This is imminent, and the world is collapsing, and we all need to be ready!" And that doesn't mean that we don't have to be ready, but we have years, if not decades. So, really, that is our position: it's almost even too soon to be researching it. We have so much time because we are so far from having a quantum computer that could be a threat to today's cryptography.

SIRANUSH VARDANYAN: Thank you, Matt. The link has been posted in the chat in the Zoom space. So you open it and read the details in the document.

Meanwhile, I would like to give the floor to David to talk about the KINDNS project, please.

DAVID HUBERMAN: Thank you, Siranush. So I wanted to change the topic for just the few more minutes that we have remaining today, and I wanted to tell you

about something we're doing in ICANN to try and help improve the technical posture of the Internet.

I went out to dinner last night. I went to a restaurant with a friend and I had a really nice time. And while we were being served our dinner, the waiter did something that I think is the nightmare scenario for a waiter. He dumped my drink all over me while refilling my glass, completely soaking me. And when that happens, I think there's two or three different ways we can react as human beings. We can get all angry and go, "What?! What are you doing?!" and make a scene, and it's just difficult and awkward for everybody. And we could of sit there and not react. Or we can take the better approach, which is we can laugh and we can smile and we can say, "It's okay. You made a mistake. No worries, my friend." And we can take a bad situation and make it good.

Okay, so we did that last night, and the waiter was fine, and we laughed, and we're friends, and it's no big deal. It's fine. So why am I talking about this? Because we can do the same thing in the DNS. We can be kind, and we can make life better for everybody through taking certain acts, small acts, of kindness to each other.

ICANN has created a program called KINDNS. It's at a website, KINDNS.org. And the purpose of the initiative for all DNS operators, big and small, whether you're Google or Facebook, or whether you're a brand new small ISP in Macedonia … Whoever you are, there are steps you can take as a DNS operator to be more kind. And if everybody is more kind, the DNS itself can have a strengthened and improved technical posture.

So in this project, you are classified as the type of operator that you are. You run a small, private recursive resolver. You run an authoritative server that gives responses to DNS names and questions. Or perhaps you're a public resolver that you want everybody in the world to be able to use. And through the KINDNS project, you can take a self-assessment as an operator and see how you're doing, judged against a set of norms that the community—the ICANN and DNS technical community—have agreed that are a basic set of standards that everyone should adhere and, if everybody did adhere to it, the DNS would work better. It would be more secure and more stable. So you can test against this set of norms and see how you're doing, get a private result back to see where you are, and, where there are gaps, you have the opportunity to fill those.

And this is an effort that is modeled off of something that, again, our friends in the Internet Society did in routing security. They called it having good manners. We call it being kind. And through these types of initiatives, the entire community can work to make things better for everybody and do so with a very small series of steps that don't cost money, typically, and don't cost a whole lot of time. It just helps you understand where your network is and make small changes to improve that network and improve the DNS infrastructure so that everyone can benefit.

So that's KINDNS. So if you have a chance, when you have some free time, take a look at the KINDNS.org website. And you can see in just very plain words some of the community-accepted norms that we think everyone should adhere to.

And that's all I wanted to share with you. Thanks.

SIRANUSH VARDANYAN: Thank you, David.

We have a remote question from Mohamed Elnour Abdelhafez Fadul from ISOC Sudan. "Path validation is significant to the global routing table security. The BGPsec extension is introduced to eliminate this issue, but it faces difficulties regarding its deployability due to the huge resources consumed by BGPsec. Research is required to optimize the extension and make it deployable. What is the ICANN role in this matter?"

JOHN CRAIN: So there's sort of two roles we could play here. One is, of course, engagement, and the other, of course, participating in research.

So I'm going to hand it over to, I think, David. Do you want to take this one?

DAVID HUBERMAN: So it's a great question. Thank you. As I was saying earlier, the two paths to a secure routing infrastructure are RPKI and path validation. And as the question very rightly points out, we already have a solution. The IETF has already developed a solution called BGPsec—presumably BGP security, right? But as our friend notes, deploying BGPsec is not very realistic right now because the computational overhead for a router is so tremendous … We wouldn't break the Internet. No, we'd do something way, way worse. We'd make it slow.

So for ICANN, our participation in researching and participating in other solutions is, in some part, what Matt's team will do and other teams in ICANN do in terms of participating in the protocol standards development processes—namely I'm referring to the IETF here. When solutions come out we of course can measure the impact of those solutions. We can formally and scientifically measure it. We can empirically measure it through our conversations and our interactions with members of the community. And then we can also be a facilitator for discussions, especially more focused in the ICANN community with names and numbers, to see impacts, to see drivers, to see motivations on how some of these technologies can improve (or not) the situation on the ground.

JOHN CRAIN: Okay, thank you, David.

I do wonder, how many people in this room have actually ever participated in the Internet Engineering Task Force?

Oh, good. There's a few of you. If you're a technologist and you're interested in the protocols, that's a cool place to go. If you're not a geek, you'll be very confused when you get there. But for the geeky amongst us, the IETF is a really good thing.

And it's important to remember that—you're going to be shocked to hear this—ICANN does not run the Internet. ICANN does not develop the Internet. We do not develop all the protocols. So it is a partnership. It is a community of engineers and people using the Internet that actually

do this. So it's good to see people in the IETF and other forums and not just here.

I think, with that, we're closed? Or do we have more questions?

SIRANUSH VARDANYAN: We can take one more last question.

Yes, please? Afifa, am I seeing you?

Yeah. Afifa, please.

AFIFA ABBAS: Hello, everyone. This is Afifa. I'm a Fellowship mentor. It's been two years that I've been mentoring my Fellows. So one question that I really get asked very frequently by the Fellows is, where in ICANN, in terms of cybersecurity newcomers, can they get involved, where they can proudly say that they belong to this particular cybersecurity in ICANN. So being a mentor, I have a hard time answering this question because … So if you can name a few of the platforms so that can get involved. Because, being a mentor, I can say that there's a huge bunch coming on who are really interested in cybersecurity. And as you said, the ICANN Fellowship is all about including fresh blood. We don't want to lose them out, and I'm also sure that ICANN doesn't want this either. So how can we utilize their talent in terms of cybersecurity? Thank you.

JOHN CRAIN: Okay, thank you, Afifa. And hi. It's always good to see returning Fellows, especially when they become mentors. That's awesome. So that's an

interesting question because ICANN is not a cybersecurity forum, right? It's not what we do. But we do have a security track where things [inaudible] in that track within the ICANN agenda.

If you're looking for advice about where to get more involved in cybersecurity issues inside ICANN now, we have a committee called SSAC (Security and Stability Advisory Committee). You can apply for membership. They are looking for mostly seasoned security professionals there. So if you're coming as a Fellow, as a seasoned security specialist—because you know we do have people who have been in the industry for a while as Fellows—that is the place to look.

We have technical days. The ccNSO does a series of technical days where there's a lot of security discussions.

And of course, you can always come to us, and we can help you find other areas and people to talk to.

A lot of what is important at ICANN is not just what happens in the policy discussions. Remember, ICANN is a policy discussion forum. It's about policy for the identifiers, which is not only security and certainly not only cybersecurity. But the important thing that you do here is you interact with the people in the corridors and at events.

So if you have seen somebody that you want to meet—I don't know—that's in your field, be that cybersecurity or another area—always feel free to either talk to your mentors or come and find an ICANN staff member or frankly anybody in the community and say, "Hey, I'm really interesting in subject X, and I found this person that seems to be really well-versed in that. Can you introduce me?" because we will all do that.

This is about working together, bottom-up, as a community. And to do that, we actually have to form communities.

So that's the best advice I can give you. There is a security track, so look at that. Look at the ccTLD, the Tech Day. Talk to people from SSAC. Talk to people from RSSAC. That's the Root Server System Advisory Committee. If you're a ccTLD—anybody here from ccTLDs? I know there's a few. Hands up.

Do you do security?

Are you on the ccTLD security list?

So if you're in the ccNSO, they also have security things.

So there isn't a straightforward answer, which is why you struggle with telling them. [Send us] to other people. We will have a one-on-one discussion with you and see if we can figure out what actually suites you. The problem is, you used the term "cybersecurity," and it means so many things to different people. But we are happy to help you.

And I think Samaneh wants to say something, too. Go ahead.

SAMANEH TAJALI: One point to add to what John already said is it's an interesting question because we sometimes discuss this but not in a systematic way. We used to also have interns, together with … We did projects—smaller or bigger projects. We haven't talked about this internally, but we are … Anyways, as research teams, we do have projects and we do want to welcome outside ideas or operations within our own groups and outside. So if the mentees you have are interested in research and

doing projects, please feel free to send them our way, and we can have discussions and see how we can proceed with that.

SIRANUSH VARDANYAN: Thank you very much.

With that, I'd like to thank all our presenters—Matt, Samaneh, David, John, and Kim—for your time. I know you have a busy schedule, but thank you for taking the time to come and talk to us, to Fellows, to NextGenners. They are really interested in learning more.

And people here, our participants, you know these faces now. Whenever you see them in the corridors and you would like to ask any questions, please feel free to reach them and ask your questions.

And by concluding this session, I would like to say: be kind to each other. Thank you very much. And this meeting is adjourned. We can close the recording now. Thank you very much.

[END OF TRANSCRIPTION]