ICANN79 | CF – How it Works: IROS and IANA
Saturday, March 2, 2024 – 1:15 to 2:30 SJU

SIRANUSH VARDANYAN: Can I request Fellows and NextGeners come and take the front seats? Thank you. Please take your seats. We'll start in a minute.

Please start the recording. Thank you. Hello, everyone. Welcome back to the next session with Fellows and NextGeners. We will be covering during this session the technical aspect of ICANN, how it works, and we'll be speaking about two main components of how technically ICANN works. This is the IANA and IROS Team. They are here with us to introduce their work.

Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior. During the session, questions and comments submitted in the chat will be read aloud if put in the proper form. My colleague, Deborah Escalera, will be our remote manager for this session and to identify what is the proper way of asking questions.

Remember to state your name and the language you will speak in case you will be speaking in a language other than English. Speak clearly and at a reasonable pace to allow for accurate interpretation. And please make sure to mute all other devices when you are speaking. You may access all available features for the session in the Zoom toolbar. With that, let's start this session.

This is one of my favorite sessions, actually. I would like to give the floor to start the first part of the session to Adiel. Adiel, please explain

to us what this IROS means so everybody knows. And then continue with the explanation for the rest. The floor is yours.

ADIEL AKPLOGAN: Thank you very much, Siranush. I'm happy to be here and talk to the Fellows. It's always a pleasure for us to meet with the Fellows and talk about the other side of what ICANN do. So I'm going to take you quickly through IROS, which is the function of the department within ICANN that looks after the identifier operation and then security. It has a lot of research embedded into it, but more importantly, it also has the IANA function.

Is this working? No. Technology, right? Wonderful.

So IROS is the function within ICANN that looks at the technology side of the unique identifier management. It has two key functions within IROS. We have the OCTO department, the Office of the CTO, that is more into the research part by collecting data, analyzing those data, providing the community those analysis that can drive or inform policy discussion, but also involved a lot in capacity building around the unique identifier system, its operation, its security, involved with the abuse and law enforcement community as well, talking about how the notifier system are used on the file out there.

The other function under the IROS is the IANA function. You may have already heard about to IANA function which is one of the critical aspects of what ICANN's role is. The IANA delivers or implements policy that comes from the community to assign name, number, and protocol parameter to users out there. The IANA function, it's less to say that play a critical role into how the Internet work globally, and a

lot of their work will also be impacted by policy that are developed at venue like the ICANN meeting.

So we are going to take you through this. I am Adiel Akplogan. I'm the vice president for Technical Engagement at ICANN. I will be doing this today with Matt, who is the vice president for Research; Marilia, who is from IANA. We'll talk about the IANA function as well. Next.

So we'll start with the OCTO, the Office of the CTO department. It encompasses four key departments: the Operation department that is led by Steve Conte. He is not here at this meeting. But the Operation department is mainly the department that connects OCTO to the rest of the organization. They play liaison role with other departments when there is a thing to be done with them.

They also help organize events that are led by OCTO, particularly IDS. IDS is one of them. IDS is the ICANN DNS symposium where DNS experts gather once a year to talk about work that they're doing around the DNS.

They are also in charge of the ROW which is the Registry Operator Workshop, which is another workshop that is specialized beyond the ICANN meeting and targeted towards the registry operator specifically.

We also have the How It Works session. A few of them are happening this weekend. Tomorrow, specifically, we have few How It Works sessions focused on some of the programs that we have within OCTO, but also involved others from the ICANN community. So tomorrow, OCTO will be leading three How It Works sessions. One will be around the number. They talk about the number, will explain a little bit about the other side of ICANN mission beyond the name, which is the IP address. So, that is going to be led by the ASO. Then we have another one about the root server system, how it works. That is going to be led

by RSSAC. At the end, another one on KINDNS. KINDNS is an initiative that we have launched. There will be a How It Works session for that as well.

So the Operation department handles the logistics and the organization of all those sessions, but also plays another very important role in providing project management resources to OCTO in general.

The second department is the one I lead, which is the Technical Engagement department. The main function is to coordinate ICANN engagements with technical organization beyond ICANN, ensure that we have a coherent way of expressing and presenting ICANN technical mission and technical role. And we do that basically through capacity building, through cooperation agreement with other organizations, and working with them to make sure that DNS operation best practices, DNS security best practices are actually implemented.

The third function within the OCTO is the Security, Stability and Resiliency Research Team led by Samaneh. Samaneh is not here today. They lead the cyber security aspect of the unique identifier system in general. They provide expertise. They are researcher on the impact of the use of the unique identifier system on cybersecurity in general. They do research; they will provide tools that can help the community to better understand how the use of unique identifier system can impact the overall security and resiliency of the Internet in general.

The last but not least, the Research Team that has a little bit more wider scope because it provides analysis of research about the unique identifier system in general, how they are used, how they are evolving, what are the things, the path that we are seeing, and how those things

could impact ICANN mission or not, how they can impact the secure operation and stability of the Internet and the DNS particularly.

So those are the four key functions that are within the OCTO. We'll go through all of these in a little bit more detail. Each of us will talk about our department.

So we'll start with the Technical Engagement. The Technical Engagement, as I mentioned, has the responsibility to develop and sustain relationship with all the technical organizations in the ecosystem in general, and also help foster those relationships in order to ensure and maintain a secure and stable unique identifier system. This involves capacity building and also properly frames how ICANN can collaborate with all other organizations when it comes to the stability of the unique identifier system.

The Technical Engagement Team is also in charge of initiatives like KINDNS. If you are interested by KINDNS, which is a framework for DNS operation best practice, tomorrow there's going to be two hours How It Works session about that. You can come and learn a lot about KINDNS. For those who know the bits, if you know about MANRS, which is another framework for routing, KINDNS is the equivalent for the DNS. We're trying to promote that and help operators to adopt those best practices.

Within OCTO, the Technical Engagement Team has the particularity of being a regional team. We try to cover our engagement on technical matters from regional perspective for a simple reason that it allows us to be close to the needs of different regions. Different regions have different level of maturity when it comes to the unique identifier system, have different needs. And by having that regionalized

approach, it helps us to be closer to the community and those who need ICANN support.

So what we do, I already explained that. To track the technical capacity building track and outreach track that I mentioned, that is more engaging with different community and talking, explaining what ICANN mission is about, what they are doing may impact ICANN mission, and how they can do it well so that we all contribute to maintain a secure and resilient unique identifier system.

The second is a more wider engagement that includes the different agreements with partner leading initiatives that can help the unique identifier system to work better, support regional community, working with different regional organizations like regional NOG, local NOG, or even the RIR on technical matters, support some of the ICANN community or constituency or advisory group that are very technical focused as well into promoting what they're doing, or organizing joint activity with them to talk more about what they are doing. We are also involved in this specifically in Africa, very involved in supporting the CDA initiative, which is the Coalition for Digital Africa, by leading the track that are related to DNSSEC development, for instance, or ccTLD capacity development. Those are areas of the CDA that are led by my team.

As I mentioned, it is a regional team. I put here the team that's covered different regions for North America. We have David Huberman. He's not here. He's based in Washington, and cover North America. In Latin America region, we have Nicolas Antoniello. And he's here, Nicolas. He covers Latin America region. So if you are from Latin America and you are looking for anything related to capacity building outreach or formation, Nicolas is your guide. Very active in the region, supporting

ISP and DNS operators. In Africa, we have Yazid and Simon. They cover Africa and Middle East, provide training, capacity building, and support to operators. In Asia Pacific, we have Champika, who is there. We still have Europe and a second person to hire. So those positions are still open. Europe, we are almost there. But if you are interested or know people who can join and provide added value to what we are doing in Asia Pacific region, that is still open. There is one additional role within the Technical Engagement Team, which is the safety and law enforcement engagement. That is covered by Carlos Alvarez. He has a more global scope for his role, and he engage more specifically with law enforcement, with community that do research, investigation around how uniquely identifiers are used to abuse the user, the Internet, etc.

So those are the team and myself. We will be here throughout the week. If you want to learn a little bit more about what we do, particularly in capacity building, feel free to contact of course myself or Nicolas. That's it for the Technical Engagement. I will leave the floor to Matt to take us through the SSR Research activities.

MATT LARSON: Thank you, Adiel. I'm Matt Larson. I am the vice president of Research. I'm going to talk about the two sections of OCTO that are related to research. So Adiel already touched on these briefly, I'll go into a little more detail.

The first of those is the Security, Stability and Resiliency Research. And that's led by my colleague, Dr. Samaneh Tajalizadehkhoob. That team focuses on, as you might guess, from the name, security, stability and resiliency. So we do have two research teams in OCTO. Samaneh's

team tends to focus more on the SSR aspects of identifiers. And the team that I run, which I'll talk about next, focuses more generally on the identifier system. That being said, we kind of operate as one big research team and certainly are all colleagues. Sometimes it's sort of tough to figure out where a particular topic will land, one group or the other might handle it. So this team focuses more on academic level papers. Right now, the team is two people, soon to be three. And they both have PhDs and are used to researching in an academic context. So the SSR Team has a great deal of rigor in their research. They have, for example, papers accepted by conferences.

Let me talk about some of their specific activities, you may have heard of some of these. They have created, initially, the Domain Abuse Activity Reporting system or DAAR. That has since been updated to a second version. So if you come to Tech Day this week, you'll hear more about that. There's a project called DNSTICR that works on collecting information about security threats from the domain name system. I don't need to read all of these research projects to you. You can read the slide just as well. But you can see based on these topics that they do focus on the security and stability angle. And as you can see, they've written papers that have been accepted at prominent academic venues.

So then, as I said, I lead the more general research team. Our job is to provide trusted and verifiable information to the Internet community about the system of unique identifiers. So we work a lot with the community. We work in standards areas that we work with the Internet Engineering Task Force to develop standards related to identifiers. That's an important component of what we do.

We have access to a lot of interesting data. We have access to the data from the ICANN managed root server. ICANN operates one of the 13 root server identities, and that's a wonderful set of data that we use to do our research. We also have access to all of the gTLD zone files, so all of the files from the various registries. That is also a very valuable source of data.

So root server traffic research is an important component of what we do. You may have heard about the name Collision Assessment Project or NCAP. That's going to be meeting this week. That project is near winding up with the publication of its study. But that's something that the Research Team has been heavily involved in.

Then I represent ICANN Org on RSSAC, the Root Server System Advisory Committee, and all of the root server operators and some other folks are on RSSAC. They provide advice about the root server system to the ICANN Board.

So here are some of the research activities that my group does. We have a long-running project called Identifier Technology Health Indicators. And the idea is if you want to know about the health of the unique identifier system, you could measure it at any given point. But if you had measurements over time, you would be able to see trends. So that's what ITHI is. We have various measurements that we measure over time and make them available to do research on.

We do a lot of work related to the DNS infrastructure, authoritative servers and resolvers. I already mentioned root servers. So things like where are they located, how are they distributed?

On the Internet numbering side, we do research related to RPKI, the Resource Public Key Infrastructure. For example, we've looked at how much of DNS critical infrastructure is covered by these Route Origin

Authorizations that are the way that RPKI authenticates network blocks.

An example of our IETF work or working standards community is something called DNSSEC error reporting. This is a document that my colleague Roy Arends and I are working through the IETF. DNSSEC is the domain name security extensions. And this is an extension to that protocol that would allow errors to be reported and get back to the originator of the data so that, ideally, errors can be discovered and repaired more quickly.

We also take some of the data that we have access to and we sort of mix it up and republish it as some interesting datasets. One of those is called the DNS Core. Another one, we have over 10 years of measurements related to TLDs. So we can do interesting studies over time on that, like, for example, tracking how the different TLDs use different DNSSEC keys and how they change or roll over those keys.

Then, as I mentioned, the ICANN manage through server data. ICANN Managed Root Server. Instance is a wonderful source of data that we use all the time.

Then one more important thing that we do is all of OCTO publishes technical documents in something we call the OCTO document series. This started in 2019. And to date, we've published 38 documents. These are some recent examples. They are on all aspects of the unique identifier system. Some are more technical than others, some are longer, some are shorter. But what we found was, several years ago, OCTO had things to say but we didn't have a formal way to say it. So that led to the OCTO document series, and it's really been a great resource, we think, for the community and it's been great for us because it's very clear when we have something to say what we do. We

put it down in an OCTO document. And you have the link there to the URL that has all the documents.

So where can you find the OCTO Team and what we do? Well, in addition to the OCTO document, which is a good way to track the projects that we're working on, we also write entries on the ICANN blog, and then speaking engagements. For example, Adiel mentioned the How It Works sessions. That's OCTO engaging at an ICANN meeting. Adiel's team, Technical Engagement Team, engages all over the world. And we also present at various technical conferences and meetings.

That is my last slide. So that's the end of the OCTO portion of IROS that we're talking about. Why don't I turn it over to my colleague, Marilia Hirano, who will talk about IANA?

MARILIA HIRANO: Hello. It's good to see some familiar faces that I've been at NASIG 24 with a lot of you. So welcome to ICANN79.

SIRANUSH VARDANYAN: Marilia, I'm sorry. Can we have the next slide up? Yeah. Thank you.

MARILIA HIRANO: Yes, the IANA slides. I've been seeing them trickle in, and it's really good to see you here. My name is Marilia Hirano. I am a director of Strategic Programs for the IANA Team. Today I'm going to be presenting a little bit of what is IANA. You guys heard about it. For those of you who were at NASIG last week, we talked about a lot of the topics, IANA was brought up. So it's good that you're here. Now, you'll

hear a little bit about what it is and what we do in the performance of the IANA functions.

So what are the IANA functions? The IANA, it's the record keeper for the unique names and numbers. Matt was talking about the unique identifier system. IANA, we predate ICANN, actually. ICANN was established in 1998 to be the home of the IANA functions. When we talk about the unique identifiers, they include the protocol parameters, Internet numbers, and the domain names. I'll go over them in a bit. So what we do is we maintain these records and that is according to the policies that are adopted by the community. So we do not implement policy. Sorry. We do implement policy, we do not set policy in IANA. Very important point.

Here you see in the picture Jon Postel. If you haven't heard of him, he was IANA, basically. He used to write down the records in his little notebook. These grew. Fast forward to today, there's a team of 20 people who are in charge of managing the IANA functions.

Why do they exist? Why do the IANA functions exist? For the Internet to interoperate globally, we coordinate the Internet's unique identifier systems. Otherwise, it wouldn't operate. That's in a nutshell. If the Internet connected devices, they don't use the same system of identifiers to talk to one another, then it wouldn't speak that common language, right? It wouldn't work.

Then the authoritative registries are used by vendors, service providers, businesses, applications, and others to expand the use of the Internet. A lot of the work that IANA does, for example, on the protocol parameters side, it's not going to be seen or used or accessed by the average Internet users. It's mostly software implementer. So it's on the technical standards. I'll go into the—did I go back? Sorry.

All right, so the core IANA functions, so you can have an overview of what's each of the IANA functions. That's what we do to deliver each of those. Starting with protocol parameters, it's basically used everywhere. But, again, the end user won't be the ones accessing this. Most protocol parameter visibility is limited to software implementers. And the Internet Engineering Task Force, they're the ones who develop the standards that will define protocol parameters systems. What IANA does, we receive and evaluate the requests that come from, let's say, software implementers to create new registries and to add new values to the registries. We also maintain and publish the registry data. We provide advice on upcoming standards. Also, we work closely with the IETF. Every RFC or request for comment, it's an IETF document that defines the standards, it has a section that is called the IANA considerations, and that's where we collaborate with them providing the input into that document. So that's protocol parameters.

IETF operates a little bit like ICANN. They have three conferences a year all over the world. They are each in a different region. Matt's very involved in that area, too. So if you're interested, the next one is in Brisbane, Australia in a couple of weeks. So you can look that one up.

Then we have Number Resources, which are specialized forms of protocol parameters. So we have the IP addresses, and this might be more familiar to the end user. What IANA does, we allocate the Number Resources, so these IP addresses, to Regional Internet Registries, which are they will then delegate it to your Internet service provider. So we don't assign these numbers directly to the end users. It goes to the Regional Internet Registries. There's one in North America, and then Europe, Middle East, Asia. They are the ones who

assign it to the ISPs. We have some specialized allocations, though, that are made directly by IANA, but that's not common.

So we're talking about IPv4 and IPv6 addresses. If you want to be more educated on this, Adiel mentioned earlier in his presentation that they're having a How It Works session specifically on numbers. So if you want to learn more about this space, join us tomorrow, I believe at 10:30. So if you have the availability to attend that, it's a very interesting presentation.

Then the most notable function is the Domain Names which are a lot of the ICANN meeting is focused on. It's managing the DNS root zone which defines the top-level domains. So like the Number Resources, the domain space is hierarchically delegated, and we are only responsible for the top-level domain, so the uppermost level of allocations.

What do we do to in this space? Again, we receive and evaluate the root zone change requests, and we evaluate them against policies and operational requirements. We don't set those policies, we implement the policies. So things like assignment and transfers of TLDs. So a country code domain or generic top-level domain, we assign and we transfer those domains. We also do routine maintenance for name servers and other technical elements that are required for domain to operate. Points of contact. So all of these domains are managed by an organization. These organizations will assign an administrative contact, a technical contact, and they come to us whenever these people change. Like people leave organizations, they come to organizations, so we process those requests as well. Then transmitting these changes for implementation in the root zone and root servers to

make sure that everything continues to operate in the root zone. We don't want the domain to not be accurate. So that's the domain space.

I like this slide just to make it clear that the IANA, what we do, we create the registries based on policies from the community. We do not create nor do we interpret the policy. We maintain existing registries. We allocate Number Resources to the RIRs and we publish all registries for general public use.

What we do not do, as I said, besides not creating and interpreting policy, we don't determine what can be a domain name. That's not our remit. And we don't choose what the TLD managers will be.

So that's the IANA functions in a nutshell. What's the oversight? What are our accountabilities mechanism? The IANA functions are performed by the Public Technical Identifiers, PTI. PTI is a nonprofit organization that was created in 2016 as a result of the IANA stewardship transition, and it is an affiliate of ICANN. So we are a separate entity, although ICANN as its sole member, so PTI hires us, me and my team, the IANA staff, but we do work under the umbrella of ICANN.

PTI has a Board. It's a five-member board of directors. Two of those are NomCom appointees. Right now, this is Anupam Agrawal and Tobias Sattler. Those are the two NomCom appointees. And then we have three ICANN staff members who are on the PTI Board: Kim Davies, Jia-Rong Low, and Xavier Calvez. So that comprises the PTI Board.

As I said, we are a team of 20 people who are performing these functions that I just went over. Our team is broken down into three main departments: Operations, Strategic Programs, and Technical Services, with the Operations team being responsible for the change

request for evaluating and implementing the policy work according to the request that come through. Strategic Programs department is my team. We're responsible for project management, budget, risk, audits, and other governance-related initiatives. Then Technical Services, it's our Engineering Team, as well as our Cryptographic Business Operations Team, which I'll touch a little bit on at the end. So that comprises the IANA staff.

Then where does ICANN fit in? We are all here at the ICANN meeting. ICANN is responsible for the IANA function. So ICANN oversees the work that PTI does through contracts. So ICANN oversees our performance. ICANN also provides shared resources. So we sit in the ICANN facility. We are mostly based in Los Angeles. At the ICANN headquarters, we share the Legal department, the IT department, the HR, the Finance. We all work together with those resources. We don't have our own HR, Finance, etc.

ICANN provides all the funding to PTI. It also supports additional accountability mechanisms. There's a group called the Customer Standing Committee that have appointees from the ccNSO, the GNSO. They provide that oversight to the IANA Naming Function. So for the domain name portion, that green piece of that pie, they oversee that section. So we do still operate under ICANN even though it's just a separate entity.

I mentioned contract. So every function, so the Names, the Numbers, and then the Protocol Parameters, they have different accountability mechanisms through contract. So with the IETF, we have a Memorandum of Understanding, and it's between ICANN and the IETF. But they subcontract for PTI to provide those services.

The Numbers, we have a Service Level Agreement between ICANN and RIRs, also subcontracted for us to perform the numbers function.

Then lastly, the domain name oversight is by ICANN, but it's governed by the naming contract, which is between ICANN and PTI. And as I mentioned, the CSC, the Customer Standing Committee, we report to them on a monthly basis. They are an oversight body for us.

Each function also has service level expectations defined that we report against. So for the IETF, we have to report to them every month. We have KPIs that we have to meet. These reports are all published on our website. You can look in iana.org, you'll see all of the reports dating back 10, 15, almost 20 years. Around 70 measurement categories to the CSC for the naming functions, we report to them, and performance reporting to the Numbering Committee for IP address and AS number allocations. These figures are reviewed through various processes. As I said, monthly reports. We have regular meetings and dialogue with the IETF leadership. We attend all of the three meetings. If you are going to be more on the technical areas of ICANN, the IETF meetings, you'll see us there. We have a Help Desk where we see customers face to face. We also report to the RIRs and we have an annual IANA Review Committee process through the Numbers community, too. So we have several accountability mechanisms that we report to our oversight bodies.

Besides that, we conduct third party information security audits. We need to make sure our systems are operating through best practices and technologies. We have internal audits that checks and balances from our operational processes and business processes. We have surveys. We have contingency and continuity plans that are tested annually. The results of that are also posted on our website.

Everything is very transparent. A lot of our work, most of our work is all public/published. Structured project management framework and we have regular engagement with the community. You'll see us in all three ICANN meetings, the RIR meetings, the IETF meetings, as I said, and also at different industry meetings, the IDS, as Matt mentioned, and then different events that we attend throughout the world.

Then I'm going touch on other notable activities on the domain side. The .int registry. So .int domain is used for registering organizations established by international treaties, so between or among national governments. It's a mouthful. So it started in 1988. And historically, it also included some non-treaty purposes, but not anymore since 2000. We have approximately 200 domains registered, so it's a small registry with very few legitimate requests per month. So Operations Team will process many people wanting to have a .int domain, but the eligibility criteria is very strict. And a lot of the ones that apply are not eligible. If you have access to the PDF, I put the links there if you're interested in what the criteria is and then some organizations—

SIRANUSH VARDANYAN: Three minutes notice, Marilia.

MARILIA HIRANO: Okay. Some organizations that have that domain. We also maintain the .arpa registry. So that's just an Internet infrastructure. It's just used for that purpose. It is and more of an IETF oversight. But we do work there. And I put links if you want to learn more about the .arpa registry. Same thing with the Label Generation Rulesets. So that's the formerly known as IDN tables. I know a lot of you are interested in that space,

too. So I added a lot of links to my presentation in case you want to dig deeper into this. It contains some codes and associated eligibility rules for which strings are permitted for registration within a TLD policy. So usually it's language, and this is Thai, Japanese, Urdu, or script bound like Latin, Cyrillic. So it became a Contractual Compliance requirement for the gTLD operators, but not ccTLD. They need to adhere to these IDN guidelines. Before the transition, we didn't have Service Level Agreements to do this work, but we do now. So that's relating to internationalized domains.

Then lastly, we manage the root signing key. This is part of the root zone related function. We manage the key signing key, which is the trust anchor used to secure the DNS. We have an auditable process for performing these key signing ceremonies and we use members of the community as key participants. I'm not going to talk too much about it because I want you to watch it in a more fun way than having all of us talk about it. So why don't we go straight to the video?

VIDEO: Please center your eyes in the mirror. Please move a little back from the camera. Sorry, we cannot confirm your identity.

We've been hearing a strange tale about seven people who have fragments of some kind of master key to switch off or restart the Internet. They're back together in L.A. for a key ceremony. So we're going to follow them to find out who they are and what this key actually does.

We've arrived in Los Angeles, home of amazing cityscapes, palm tree lined streets, and ICANN, one of the bodies that run the Internet. This is Rick Lamb, a savvy senior program manager at ICANN, the Internet

Corporation for Assigned Names and Numbers, which basically assigns web addresses. The California-based organization is technically a not-for-profit, but it has one of the biggest jobs in governing the Internet to manage the Domain Name System or DNS.

As far as who put ICANN in charge of all this, that's a really good question. It's the community. It's the people that have put ICANN charge.

But what exactly is DNS? When you type a web address into your browser, your computer looks in an online phonebook of sorts to see where to go. This is called a domain name system. It's been made more secure. It's going to be signed so that no one can trick people into going to the wrong place. At the heart of this new system lies one master key. That key is controlled by seven smartcards locked in one of two high security deposit boxes, one on the East Coast, one on the West. The keys to those boxes are scattered around the world in the hands of two groups of seven online security experts.

How do we pick these people? We have Russians, we have Chinese, we have people from Burkina Faso, we have somebody from Trinidad, and they're all technical experts. So we publish the criteria on the ICANN website, said if you're interested, apply.

The idea behind this, they say, is to make sure that no one person or company or even government can get control of the key.

So what happens if this master key to the Internet gets lost or stolen? Does the whole thing have to shut down? Are we back to an era of carrier pigeons and Morse code? With a push of a button, the words are on their way to a couple in Missouri.

Actually, it's not quite that dramatic, but we're going to take you inside the secure data center in El Segundo, California.

The ceremony takes place here in this data center. ICANN has full control over a secure compartmentalized information facility. This is a high security room designed to be able to store even the most sensitive classified information. Getting into the data center involves a series of security precautions reminiscent of a Bond film on security guards, biometric hand and iris scans, secret pins, and smartcards. Accessing the ceremony room is even trickier. Only a select few can enter at once, and everyone must properly sign in in the secured lobby on mantrap before moving forward. Needless to say, the space is tight. Once inside, copies of the script are handed out. This is a series of more than 100 actions to complete during the ceremony. Everything is recorded to the minute using GMT time.

For consistency, we're told, the ceremonies should go like this. The ICANN staff and key holders get their equipment from the secure safes. They wire everything up and activate the machine that will renew the key. They type in the code to renew the key, and then lock everything back up.

First, everything goes to plan. But that run of luck doesn't last forever. Someone slams the safe door and triggers a seismic sensor which locks the key holders to the Internet in a small cage. The only way out is to trigger an evacuation. After more than half an hour, that plan has worked and the ceremony is back on. The assembled crowd applauds as the new key is generated and passed to Tomofumi Okubo, an ICANN crypto officer, to transmit for use. The job is done for another three months.

So that's the ceremony. A little bit of high security, a little bit of computer repair, a little bit of theater, and a little bit of chaos. Sounds a lot like the Internet to me.

MARILIA HIRANO: That's my last slide. I want to leave some time for questions. We do have ceremony experts here, too, if somebody wants to stay later and ask questions. He's a former key holder here sitting next to me. So John has joined us, too. So if you want to ask questions, go ahead.

SIRANUSH VARDANYAN: I would like to introduce ICANN CTO, which is technology officer. I know technology officer, a senior.

JOHN CRAIN: I'm the senior vice president and chief technology officer. But don't worry about me. Let's get to the question.

SIRANUSH VARDANYAN: Chief technology officer. I always forget chief. But thank you for coming, John. And please, the floor is yours.

JOHN CRAIN: No, let's get questions. Let's open up the floor.

SIRANUSH VARDANYAN: We do have the first question coming from our Zoom. So that's the way to put your questions. You will be the first one, Hafiz Farooq. I hope he's here as well. So he's asking, "Is IANA completely self-reliant to perform its three key functions or dependent on external contractors and third-party service providers?"

MARILIA HIRANO: We do have vendors, third party providers that help us augment our resources. But I would say like 90% of the work is performed by the 20 of us on the team.

SIRANUSH VARDANYAN: Yes, and then we'll move. Yes, Abraham, please.

ABRAHAM SELBY: Hello. Thank you very much. My name is Abraham Selby, ICANN79 Fellow, for the record. I'm speaking in my own capacity. I've been thinking about IANA work, and today I'm very happy to see this presentation and that. I have been part of committee in my country, and there is a lot of conversation going on about the country code top-level domain names in Ghana. Now, I want to know. I have two questions. I want to know first, who is mandated to manage such country code domain name within a country? Is that the government or the private sector? And two, if maybe the country code top-level domain names was being managed by a private organization, what is the transition or change from maybe that organization to the government? Thank you very much.

JOHN CRAIN: John Crain, CTO, I've been at ICANN for a long time. It's actually quite complex. So the way the ccTLDs were originally given out was basically by John Postel often to whoever was building network into a country. Garner, there's a gentleman there, Professor [Quaner], who's been doing this for many, many years. And there is discussion ongoing

now about how do you transfer that role into a new custodian, new facilitator, whatever you want to call it. So that's an internal discussion inside the country. Now, the government obviously has a role. But it's not purely the government. It's also needs to be the community and it needs to be a form of consensus. Now, it's not like you can just take a ccTLD and say today it's going to be one person, and then tomorrow is going to be the next person, right? It's a piece of infrastructure that the country relies on. So it has to be a clear process. It has to be agreed upon first within the country.

Now, the IANA folks—and I think you saw that in the slides—they do not make those decisions. We do not make a decision at ICANN or IANA what a country code is. That's an ISO thing, a different body. And we do not make the decision on who gets to own it. So what will happen typically is there will be a process, there'll be in-country discussions, they will often come to a conclusion, and then they will pass that forward to the IANA. And then the IANA will make sure that there's actually some level of consensus. Often it will be ICANN's government engagement people who will go talk to the governments, etc.

So what we will often hear is—somebody will come to us and say, "We need to run this. It needs moving now. ICANN is not making the decision and pulling it away from the other person." Well, we don't make those decisions. It is a complicated scenario because… I don't know if you heard that video, but they said, "This is one of the organizations that run the Internet." Well, we don't run the Internet. Nobody runs the Internet. Nobody gets to make these decisions for a country. So I wish it was a straightforward "go talk to this person," but it's not. You have to build a consensus in the country. I know they're working hard on that now.

SIRANUSH VARDANYAN: Actually, there was a follow-up, to some extent, question. "Which body in ICANN gets to determine what can be a domain name? As you mentioned, we are not dealing with this. Is there anybody?"

JOHN CRAIN: It depends what you mean. There are different elements of what can constitute a name within the DNS, right? So there are technical limitations, letter, digit, hyphen. But there are also all kinds of policy considerations. So that's the community. That is the ICANN bottom-up multistakeholder community. So there are lists of things that cannot be names, and there are rules around what can be names. For example, what can and cannot constitute the IDN. Part of that is technical, the xn dash, dash, which is on the wire, and part of it is policy. So the ICANN community makes the policy.

SIRANUSH VARDANYAN: Thank you. Pranav, and then Shanelle.

PRANAV BHASKAR TIWARI: Greetings. I'm Pranav Tiwari, an ICANN79 Fellow from India, for the record speaking in my personal capacity. Thank you to all the speakers. The presentation was quite detailed, and I learned a lot. I was particularly intrigued by ICANN manage root service. And my question is is there a person or a dedicated session where I can seek inputs on technical, financial, and geopolitical considerations around establishment of IMRS clusters?

JOHN CRAIN: Did you want to specifically know about IMRS? Or do you want to know about root servers in general?

PRANAV BHASKAR TIWARI: Both of them, actually, because there's been a demand in India for IMRS clusters recently, along with parliamentary expectations in that regard. So understanding that ecosystem and what are the policy considerations for establishing it would be helpful.

JOHN CRAIN: All right. So it's a complex question. And it's not a complex question. It's both. So if you go to dns.icann.org, obviously, we use a really cold domain name for the page, you'll see the criteria for hosting a IMRS instance, which is just a singular machine. Now, those are extremely—I won't say extremely. Those are fairly easy to have deployed within your networks by a piece of machinery, work with the engineers, make sure it gets installed correctly. You have one of those, you have DNS resolution. It's important to realize that the service you get—because you mentioned specifically a cluster, and an instance is exactly the same, right? Name service just answers names. So whether you have a cluster or an instance, you will get exactly the same answer.

Now, we're also looking at deploying clusters. And we're actually talking to people in India, of all places, about how we deploy one of those. Those are much more complicated mainly because they're much more expensive. So a cluster will typically be something like half a rack or a rack with the actual expensive part is, of course, the fiber and the bandwidth. We have multiple of those, and we're not the only

ones who have these. Other operators have them, which is why I asked that question. And we're in discussions about that. I don't think there's been a solid decision yet. That's actually not my role making that decision. I am part of the discussion.

So it's basically ask. Go to that dns.icann.org question now. In every region, we have engagement folks. Our Global Stakeholder Engagement folks, you can talk to them, they can help you find all the information. But a cluster, the way to look at it as an instance, is a fairly low investment. You could probably put 100 of those or 200 of those into a country for the price you can put a cluster in. But they serve slightly different technical purposes in slightly different scenarios. I'm happy to talk offline.

PRANAV BHASKAR TIWARI: Thank you.

SIRANUSH VARDANYAN: Shanelle, please go ahead. Adiel, you want to add something?

ADIEL AKPLOGAN: Yeah. Just to clarify something. You mentioned geopolitical consideration. It's a very loaded word because we are talking about technical aspects, and geopolitical consideration doesn't really come into the decision. Because what matters for ICANN and the IANA is the stable operation of the Internet globally, right? That's what's the most important. And those are the considerations that are going to be taken into account.

SIRANUSH VARDANYAN: Actually, while, Adiel, your on the mic, there was a question. You mentioned that you don't have a person in Europe. Does it mean that there is no work taking place in Europe?

ADIEL AKPLOGAN: Yeah. They are good. They don't need us. No. As I mentioned, as you can see in the graph, we have that in dotted line, we are hiring somebody. Actually, we are in the process of finalizing that. Very soon we'll have somebody in Europe, just that the process is on the way.

SIRANUSH VARDANYAN: But the Internet is working in Europe.

ADIEL AKPLOGAN: Of course.

SIRANUSH VARDANYAN: Shanelle, please go ahead.

SHANELLE MCPHERSON: My name is Shanelle McPherson. I am an ICANN79 Fellow, and I'm speaking in my own capacity. Mr. John Crain, it is my pleasure to finally meet you, sir. I remember you invited me to dinner in ICANN76. I hope it's not too late. My question is how accurate is the report on DAAR? Because I know that there are [captures], the TLDs and the gTLDs that are abusing our domain system. That report is perhaps pulled from crowdsourcing, spam filtration, honeypots, and you get

your reports from third parties. Now, what happens when you really get those reports? What happens to those remain? I'm sure they're a part of some blocklist, but what's the underlying factor of that? Well, that's one.

Then two, I would like to know, could engagement in different areas, because the last report that was pulled, well, I recognize pulling was from May 2022. And there were so many countries within that still was not involved in DNSSEC. So I wanted to know if there is an existing report with some updates that you guys can provide, as well as from the engagement side of things. How can I get engaged in providing updates on these inquiries within the Caribbean region? Those are my questions, really.

Oh, there's another one, Mr. John Crain, before you go. Do you ever think there is going to be a time where we can perhaps mitigate domain names from inception from being abused? Thank you.

JOHN CRAIN: Okay. Just a short question. Let's start with the registration blocklist. It's important to realize that DAAR, despite its unfortunate naming, is actually measuring the reputation of namespaces. It's not actually measuring instances of abuse because it's taking what people are saying about names. Now, these are well known reputation blocklists. We just issued a paper recently—I think it's 37 or 36. 37? Thank you—which talks exactly about how you identify and choose these blocklists. Because there is actually a little bit of a science to it but it's not well documented. This is a question we get a lot. So we've actually issued a methodology for doing that and how we do that.

Now we are about to, at this meeting, talk about something called Domain Metrica. Domain Metrica is a system that will replace DAAR and will add over the years a lot more measurements and functionality. So we have other projects that do things like gather evidence of abuse. We just issued another paper that was looking at a different type of abuse feed, which is where people send in unsolicited e-mails. So we've also developed a methodology using machine learning for looking at large scale streams of mail and differentiating abuse types within that e-mail. So we have a lot of research between Matt's and Samaneh's groups. We have a lot of research in this area.

There are different places for DNSSEC data, then our place is dnssec.org, and we also help fund another project out of one of the universities that's measuring that. We have internally been building some tools to gather more of that data. Adiel's team has been looking at that on the sort of country-specific level. That will probably at some point become part of Domain Metrica or it will become part of the Internet health identifier. So once that's finished, that will be published and will be much more up to date. So there's a lot of work going in the background here.

Will we ever be able to prevent abuse at its inception? Yes and no. So there are a lot of projects out there trying to identify names that are likely to be used in an abusive manner and there are different ways different registries are handling, though there's no policy in this area, just to be clear. So there are tools out there that, for example, cause delay in the resolution of the name. So they don't let it get put into the zone until they do extra checks because the name has reached some threshold. So there's been a lot of research in this area in Europe and

other places. But the Minority Report movie, it's like that, we're probably never going to get there.

So there's been a lot of talk about dealing with abuse after the fact. So when it becomes recognized, because often you can't tell whether name is going to be abusive unless it is. So there's been advances in the community around that, including new contractual clauses, etc. So, obviously, DNS abuses are very important part of what happens on the ecosystem. It's not the only abuse. And of course, the Internet reflects society. So there will always be bad people on the Internet. We can only do our bits. The community does its bit, sets policy. I suspect there'll be a lot more discussions over the next year or two about how that policy evolves. But that will be the community and not just as we are the researchers and the bringers of—I'm not going to say truth, but the bringers of data.

SIRANUSH VARDANYAN: Thank you. We only have five minutes to go. So we'll take the question from a gentleman and then come back to Russell. Thank you, Matt, for pointing out to the publications. There was a question on it. So please go ahead.

MICHAEL PALAGE: Michael Palage for the record. Quick question, John. With regard to the .int and .arpa top-level domains, has there been a decision made within IANA in which countries in the EU they will be registering with under the new NIS2 requirements? And if not, how will that evaluation and decision be made?

JOHN CRAIN: I don't know if that's even in front of the lawyers yet. So the answer's no, but I don't know where it is in the process. Obviously, we follow those things. So you'd have to ask one of the lawyers.

MICHAEL PALAGE: Thank you.

SIRANUSH VARDANYAN: Russell, please go ahead.

RUSSELL DEKA HARADA: Thank you. My name is Russell Deka Harada. I'm director of ICT, PNG University of Technology from South Pacific. Also I'm ICANN79 Fellow. This is my first time making a question both online and in person. So very simple. I'm working for university. We need to make a capacity building, but no one in my country teach about the DNSSEC. So how can ICANN/IANA assist our country to make our capacity building, especially young youth? Thank you.

ADIEL AKPLOGAN: Thank you for asking. You are in the right place. We'll be more than happy to work with you on that. In fact, this week, Nicolas just concluded a very successful training here for university students, specifically on the DNS, and helping them to understand, etc. And your observation is valid, not only in your country, but it's globally. It's something that we have observed. What we're trying to do is to work with the stakeholder with the community in those countries. So if you're having these, talk to us, Dr. Nicolas, he will be more than happy

to help. And if he cannot do it, somebody in your region that cover your region will be able to jump in and help. This is valid for everyone. We want to engage with the academic community on these topics. If you can host this kind of training, let us know.

SIRANUSH VARDANYAN: Also work with Xavier to connect. I think Xavier is not here, but he met already Xavier. So he has worked with him to make this connection, and this happened.

Last question, last opportunity for anyone here. If not, then I just want to thank your team, John, and for everyone being here. This is one of the most important and interesting topics. I see the feedback coming all the time that Fellows and NextGeners, especially those who are first timers, it's very important for them to know where to start. So thank you for being so open. Thank you for coming and agreeing to run these presentations for our groups. With that, the meeting is adjourned. Thank you very much.

[END OF TRANSCRIPTION]