MARRAKECH – GAC PSWG and ASO / NRO Workshop
Tuesday, March 08, 2016 – 12:30 to 14:00 WET
ICANN55 | Marrakech, Morocco

UNIDENTIFIED FEMALE: March 8th, 2016, 12:30 P.M to 14:00. ICANN55. Crystal room. GAC PSWG and ASO/NRO Workshop.

ALICE MUNYUA: Good afternoon, everyone. Thank you for [staying]. We're just about to start the joint workshop. This is the Number Resource Organization and the GAC Public Safety Working Group. You're all very welcome.

We'll have a very quick introduction of the people sitting with me so you know who they are. I'll start with myself. My name is Alice Munyua, Africa Union Commission and Chair of the GAC Public Safety Working Group.

BOBBY FLAIM: Hi there. I'm Bobby Flaim from the Federal Bureau of Investigation in the United States.

PAUL RENDEK: Good afternoon, everyone. My name is Paul Rendek, and I'm the Director of External Relations for the RIPE NCC, which is the

Regional Internet Registry for Europe, Russia, Central Asia, and the Middle East.

LESLIE NOBILE: Hello. My name is Leslie Nobile. I'm the Senior Director of Global Registry Knowledge at the American Registry for Internet Numbers.

CRAIG NG: Good afternoon. My name is Craig Ng. I'm the General Counsel for APNIC. APNIC is the Regional Internet Registry for Asia-Pacific. Part of my role is to engagement with law enforcement agencies in our region.

MADHVI GOKOOL: Good afternoon. I'm Madhvi Gokool, Registration Service Manager at AFRINIC. Thank you.

ALICE MUNYUA: Thank you very much, and welcome, everyone. The agenda is up there. I think everybody can see it. We don't have much time, but we're going to start with a joint introduction, a very quick introduction of what the GAC Public Safety Working Group is and the NRO, and then go through an overview of how public safety agencies and law enforcement agencies use IP WHOIS, an overview from the [RIRs] and their members and on policies and practices concerning IP WHOIS, and then a discussion and next steps to discuss how we're going to take this forward.

I don't know if you have any comments on the agenda. Yes?

UNIDENTIFIED MALE: Yeah. Sorry. I was just going to ask you to speak into the mic because I can't hear you.

ALICE MUNYUA: Speak to the mic. Yes. I'm going to start by giving a very quick overview of what the GAC Public Safety Working Group is. As you're all aware, the GAC Operating Principle 27 provides for the creation of committees or working groups to address certain matters that affect public policy issues.

This particular one was created in February 2015 during the Singapore meeting, and its objectives are cooperating with ICANN advisory committees and supporting organizations and the ICANN community to ensure multistakeholder support in advancing public safety policies, recommendations, and advice.

We also assess and ensure that the DNS registrations are not used to propagate unlawful activity. We support public safety organizations and law enforcement agencies to investigate, prevent, and disrupt unlawful activity in the DNS, and also participate in ICANN working groups and study groups, PDPs, to promote shared understanding of the potential effects such groups' work and recommendations will have on public safety. The most recent one is with the GNSO PDPs.

Also, we are continuously assessing ICANN's responsiveness and mechanisms to develop and enforce our contractual obligations with registries and registrars, as well as addressing work streams and policies and studies that are brought to us at ICANN that affect public safety.

In a nutshell, those are the objectives of the GAC Public Safety Working Group. I'll hand over the mic to Paul to introduce the NRO. Paul?

OSCAR ROBLES: Sorry. My apologies for being late. I was stuck in another meeting. I'm Oscar Robles. I'm the CEO of LACNIC, the Regional Internet Registry for Latin America and the Caribbean, some of the Caribbean territories. This year, I am the NRO NC Chairman. NRO is the Number Resource Organization, which is a group of the five RIRs together. Welcome for [inaudible]. Thank you for inviting us to this session. We are interested to hear your concerns or your questions and see what can we do to address those concerns. Thank you.

ALICE MUNYUA: You're welcome, Oscar. Thank you very much for collaborating with us. We look forward to working together. Paul?

PAUL RENDEK: Thank you, Alice. I'm going to give a quick introduction to the Regional Internet Registries. I understand that we probably have varying understandings of what Regional Internet Registries actually do, so I'm going to walk us through maybe a 101 on the registry system here.

How do I move the slide?

ALICE MUNYUA: Just [inaudible]

PAUL RENDEK: Oh, there we go – oh. One up, please. There we go. What is an RIR? I'm going to read this, actually, because it is a nice definition. I think it needs to be read out loud. A Regional Internet Registry manages the allocation and registration of Internet number resources in a particular region of the world and maintains a unique registry of all IP numbers issued. These resources are IPv4, IPv6, address space, and autonomous system numbers.

Next slide, please. Regional Internet Registries. Currently there are five Regional Internet Registries. We are represented, all of us here, on this panel.

UNIDENTIFIED MALE: [inaudible]

PAUL RENDEK: I've actually listed down the establishment of when these registries were established. If you take a look at each one of them, I will walk you through here. We have the RIPE NCC, which is the oldest Regional Internet Registry, established in 1992, which is quite some time ago. The RIPE NCC covers, as I mentioned, Europe, Eastern Europe, Russia, Central Asia, and the Middle East.

The next registry that came on board was APNIC, which was formed in 1993. They cover the Asia-Pacific region. Then after that we have ARIN, the American Registry for Internet Numbers, which you can see Canada, America, and parts of the Caribbean that they cover.

After that, we see LACNIC, which covers Latin America and also parts of the Caribbean. It also covers Central America as well. Then AFRINIC, which was established in 2005.

I've listed these establishment dates because, actually, the way that these registries came about was quite natural. These regions weren't just selected and divided. They were based on the way communities came together and wanted to have the registry formed.

It actually probably also shows the development of where the Internet was happening. Actually, before the registry systems, all the numbers came out of the United States of America. Their registry was not the first registry coming about because they still had a legacy provider that was providing the space in the United States.

Next slide, please. RIR structure and services. The RIRs have a number of services and activities that they provide in their region based on what their membership and their community needs from them. Overall, the ones that are overarching and bring us together that we have in common are the following.

The structures are not-for-profit membership-based organizations, 100% community funded for fees. There are fees for the service provided by the Regional Internet Registry. They are open, bottom-up, and inclusive. Anyone can participate and anyone can become a member.

The policies are developed by the communities within the Regional Internet Registries. The processes are open. They're transparent, inclusive, and they are documented. So this is the structures that we all have in common.

As far as core services that we share, of course, the distribution and registration of Internet number resources, the IPv4 and IPv6 and the ASNs. We maintain a directory of services, including WHOIS and routing registries.

We also provide reverse DNS. The RIRs register only reverse delegations and are not involved in forward domain delegation at all. Reverse delegations allows applications to map a domain name from an IP address.

We also facilitate the policy development process. It's very important to note here that the RIRs themselves do not develop policies. These policies are developed by the communities. We publish the policy documents. We maintain the mailing lists, where the discussions takes place, and we also facilitate the meetings that bring together the people that actually conduct the policy development process. This is done by physical meetings and also remote participation. Then there are mailing list discussions that follow from this, as I've listed here.

We also all conduct outreach and training to our members, community, and most recently, to other stakeholders that are coming on board. So we do do a lot of trainings also with governments, with law enforcement, and other intergovernmental organizations.

Next slide, please. What is the NRO? The NRO was actually established in October of 2003, and it is actually formed together by an MOU of all the five Regional Internet Registries. It is a very lightweight organization. It's an unincorporated association.

We use the NRO when we want to actually come together and show you a concerted view of the RIR systems. We feel it's an easy way for people to just access all the RIRs together. So we use the Number Resource Organization for this.

The mission of the NRO is really to provide this coordinated Internet number registry system out there to the whole world. We promote the bottom-up and open and inclusive policy development process in Internet governance, and we also actually coordinate and support joint activities in the RIRs. So there are various groups inside of each RIR where we come together and we work on NRO-specific or kind of global projects together.

But the most important function of the NRO is that it fulfills the role of the ICANN Address Supporting Organization, or ASO.

Next slide, please. Where do we fit into the whole ICANN environment? If you look here, you see we've listed it in red here, the ASO. We fit underneath one of the supporting inside of ICANN. So this is where the Regional Internet Registries fall within ICANN.

Next slide, please. On the Internet, you are nothing but an IP address. When we look at what we look like in the Internet, you probably see these lovely machines that we all carry in front of us. You see the lovely person here, and you see all these domain names floating around.

Next slide, please. Sorry.

UNIDENTIFIED FEMALE: That didn't work.

PAUL RENDEK: Yeah, that didn't work. Can we just back up for a moment, please? I apologize. Actually, this slide was supposed to remove the person and the domain names, and underneath that, there are IP addresses. So the Internet actually doesn't view any one person or any one machine as the way we are sitting here in this room. It views you as an IP address, simply transferring data within the network.

Next slide, please. What is an IP address? Again, I will read this definition out. It is a unique identifier for a computer or a device on an IP network that facilitates moving data between networks. Every device directly connected to the Internet needs to have a unique IP address, and therefore we have these five Regional Internet Registries.

Next slide, please. IP addresses are not domain names. This is something that does get confused quite often, so I've actually identified here the difference between an IP address and a domain name. An IP address, an identifier, it's very computer-friendly. It's a unique number that identifies any device on the Internet, and it's used for routing. So it's actually used for moving information or packets across an internetwork from a source to a destination. That is what it does.

Domain name. They're very people-friendly. It maps a host name to a unique IP address, and it's a means of storing and retrieving information about hosts, host names, and IP addresses in a distributed database.

Next slide, please. And that was just a quick introduction to the RIR system and where we fall into this environment. Thank you.

ALICE MUNYUA: Thank you very much. I think we'll have the presentations presented and then hold for questions at the end. I'd like to invite Bobby to give us an overview of public safety agencies and how law enforcement uses IP WHOIS.

BOBBY FLAIM: Okay. Thank you, Alice. I just wanted to point out for those of you in the room that we do have other international law enforcement here. We have Interpol here; [inaudible]. We have Europol; Greg. We have the European Commission; [inaudible] from Holland. We also have the United States Drug Enforcement Administration and the Federal Trade Commission. We also have our good friend from Switzerland, Adrian Koster, and we also have the International Association Chiefs of Chiefs of Police, just so you know it's a very international, broad-based effort. So I just wanted to acknowledge them in the room.

Thank you very much to all of the Regional Internet Registries who have taken the time to come and speak with us and present and hold this discussion. We have been working with the Regional Internet Registries collectively and individually for about the past ten years. It's been an absolutely fantastic relationship, one that we really prize and one to – the show goes on. We want to ensure that that continues. That's why we have been able to hold these very frank discussions.

Our relationship has gone back ten years, where we have actually participated. It was very slow-going at first because we were quite unsure how they worked. But they were very, very kind in taking us in, showing us how policies work, how the membership works, how things are done, and how to be very effective. That's why we're really here, again, today: because we want to be effective and we want to work very closely with them to ensure that we both have and can achieve the desired results.

I just wanted to say that and give you a little bit of a history to let you know that this is not something new. This is a position of strength in which we have valued the relationship and have worked for a very, very long time.

Going to the issue at hand, which is the WHOIS and in particular the IP WHOIS, because, if you heard in Paul's presentation, IP is actually where all the Internet traffic goes through. The DNS is a level on top of it, so it's human-friendly and people can access it more easily, but the IP traffic is actually very, very important. The Regional Internet Registries, in doing what they do, is actually very key and very, very important.

That being said, international law enforcement always looks to the IP WHOIS because that is where traffic is being derived from. That's where the crime is occurring. If that's the case, it's going to be an important tool in all of our investigations, whether it's a child exploitation case, whether it's a kidnapping, whether it's a bank robbery. If an IP address is used in any way during the commission of any of those crimes, therefore it becomes a piece of digital evidence, and we need to find out who that piece of digital evidence belongs to.

A very simple way you can think of it is if someone calls in a bomb threat on the telephone. You want to be able to trace the telephone call, who was on the telephone call at the time so we can actually find out who that person was.

Same thing with an IP address. We are trying to find out who the criminal was using that IP address at the very, very specific time. Therefore, we have to use the IP WHOIS to determine which organization that we need to go to to get that information.

Generally, in the United States, it's what's called an Internet Service Provider – Comcast, Verizon, so on and so forth. In Europe and the rest of the world, they're sometimes also referred as a Local Internet Registry, or sometimes an organization, anyone who has gone to one of the Regional Internet Registries to seek out and have obtained an IP block.

Therefore, we need to go to that organization who has or is in charge of that IP block because they have received that allocation from the Regional Internet Registry to go with them with legal process. This is an important piece of the equation – legal process – to determine who was using that IP address at the time. Therefore, knowing exactly who to go to at that very specific time is critical.

The problem that we're running into, however, is that, because the IP WHOIS is so vast, with so many organizations and so many people responsible for it, it isn't accurate the way we need it to be accurate to get that information through legal process as quickly as possible. That's where we're really running into the problem.

It isn't so much with the first allocation because the Regional Internet Registries themselves have done a very good job in ensuring that that information is accurate. The problem comes when those larger IP blocks are assigned.

In other words, I would go to the ARIN region from Leslie and I would get a big IP block, and I decide that I'm going to assign part of my IP block to Alice. Alice gives part of her IP block to Paul, and so on and so forth, so that, by the time we get to Leslie or Craig at the end, we're not quite sure who actually has that IP block and who we need to serve that legal process to. That is very key, and that is very essential. That is why we need the IP WHOIS to be very, very accurate. We need to go to the right person at the right time.

That is really the heart of the matter. We all use it, insofar as all different international law enforcement agencies, and that's why we need it to be accurate.

Now, what we're hoping to accomplish with the Regional Internet Registries is to work with them. They are the experts. They are the technical experts. They know their membership, and they can help us to ensure that we reach a mutually beneficial solution. You want to incentivize the membership, the community, so that really it's in all of our best interests, not just law enforcement, but also other public safety agencies, consumer protection, health agencies, the abuse, operational purity. We want to ensure that the Internet is safe and secure, and this is a benefit to all of us, not just strictly public safety agencies.

It's also a benefit to the Regional Internet Registries and the other Internet Service Providers as well. Everyone wants to know basically who has that IP address legitimately. It's not being subject to an abuse or a nefarious activity.

So that is our goal in working with the Regional Internet Registries here today. We just want to get the dialogue started. We know that we have to go to them, to their particular meetings, where they have them in their regions, and we have done that. I myself have gone to, I would say, 80%, 90% of ARIN meetings. I've actually gone to each one of the other Regional Internet Registries meetings at least once, and so have my colleagues internationally as well. So we know we have to be there. We have to participate, and we have to work with the Regional Internet Registries. This discussion is to get that ball rolling, how we can do that, and how we can be effective.

I'll just end with saying that we have already starting doing that. I know in the ARIN region we have the ARIN Government Working Group. RIPE has the Government Roundtable, in which they have afforded governments the opportunity to meet and discuss with them one-to-one some of the issues, and also to educate us on what's going on with the Regional Internet Registries.

I will end there. I'm looking forward to Leslie's presentation. Then we can have the discussion after that. Thank you.

PAUL RENDEK: Thank you very much, Bobby. Bobby, you're right, actually. There's been a lot of work that's been put into actually forging the relationships between the communities and the LEA community. I think probably about five or six years ago, the word "LEA" wasn't such a great word inside of the RIR communities, but we have come a long way from that point, actually. We have worked as registries to actually bring the law enforcement in and show them how they would come and work with the community.

It has been very positive to date, and I'm happy to see that we do have a lot of law enforcement – for instance, I can speak for the RIPE NCC community meetings that we have. We do have quite a number of law enforcement that come in, and I can see today they feel like they're just an integrated part of the community. They're there. They've made their relations. I think this is the kind of positive cooperation that we need to see moving forward.

We're going to concentrate next on a presentation that's going to take a look at WHOIS and data accuracy across the RIRs because Bobby has mentioned that this is one of the areas that of course is maybe one of the tools that law enforcement uses. It's something that I think we've worked very hard to make sure that law enforcement has a good understanding of what is WHOIS, what they can get from this, and what it is not, also, and what it doesn't actually deliver. We have spent some time on trainings in this area, and I think we do need to do a lot more in the capacity-building area.

We are very open to this, so I'm happy that Leslie has put together this wonderful presentation on WHOIS and data accuracy across the RIR. Leslie?

LESLIE NOBILE: Okay. Hello, everyone. Okay, I'll just jump right in since Paul told you what the title is. I'm actually going to talk about what WHOIS is and what its purpose is, and then talk about data accuracy processes, practices, and policies across the RIR system.

I wanted to just talk some terms initially, just to throw these out there because Bobby mentioned ISP and I'm going to mention other things. You've probably heard some of these terms and may not know what they mean.

An ISP is an Internet Service Provider. They are allocated address space by an RIR for the purposes of providing connectivity and address space to their downstream customers. When an RIR allocates space to an ISP, that means they can take that space and further sub-delegate to their downstream customers. So allocation is a different term than assignment, which we'll talk about in the next bullet.

An end user, that's an organization that is assigned addresses by an RIR, and that's for use exclusively within their own internal networks. The assignment stays with that end user, so if you are looking in WHOIS and you can see that it's an end user organization, which it's typically defined in the WHOIS, that assignment will not be further sub-delegated. It will stay there, so, as law enforcement, you would never have to go further than that one end user organization to look for the address space.

A local internet registry, it's a term used in some of the RIR regions to describe an ISP member. It's interchangeable with an ISP.

Legacy space. This is interesting. These are number resources that were issued prior to the establishment of the RIR system. Paul made brief mention of this. Before the RIRs came into existence, IP numbers and domain names were actually issued under U.S. government contract, and that was done from the '80s until '92, '93, when the RIR system started forming, when the Internet started forming, and when the domain names flipped from the IP addresses.

Legacy numbers were issued directly to a customer with no contract. They would come in and say they have a need, and we would issue address space to them. So there was no contract, which means there were no terms and conditions.

Currently, that legacy space is maintained in all the RIR's databases. We inherited the database from the Internet previously, and we maintained that address space.

Most of the RIRs allow limited services to legacy space holders. They can maintain and update their data without contract, without fees, but they don't have access to some of our more advanced services.

This legacy space has been a target for hijackings and criminality. A lot of the space is not routed. It hasn't been updated in years. So the criminals look for that, and then they come in and they do route hijackings and they start spamming with it, or they do other things. There's lots of things they're doing with that space.

UNIDENTIFIED MALE: Slow down, Leslie.

LESLIE NOBILE: Oh, sorry.

UNIDENTIFIED MALE: For the interpreters.

LESLIE NOBILE: Thank you. Sorry I speak fast. I always do this. Okay. I'll go slower. Anyways, they are targets for hijackings and criminality.

What is WHOIS? Oh, I'm going by my own slides and I forgot it's right in front on me. My apologies.

UNIDENTIFIED MALE: Next slide [inaudible]

LESLIE NOBILE: Can you do next slide? Thank you. It's clicking. WHOIS is a general purpose registry directory service. It is not a database. It is a registry directory service.

Click, please. It is used by various types of registries. It is used by the number resource registries. That is the RIRs. Bobby referred to it as IP WHOIS. We just call it WHOIS. It is used by the Domain Name Registries (DNRs). That is a very different WHOIS. And it is used by routing registries, and that is where routing policy is collected and displayed.

Can you click, please? Additionally, WHOIS service differs in usage and content depending on the type of registry. Obviously, domain name registries are very different than number registries, and routing registries are very different than either domain or number registries.

But even within the RIR system, our WHOIS usage and content differ slightly. Some of the RIRs actually include routing policy in their WHOIS displays, and some of the RIRs do not, so there are even differences in WHOIS across the RIR system itself.

What information does an RIR WHOIS include? Typically, it includes registration information about IP addresses and autonomous system numbers that the RIRs are issuing to customers. It includes information about that legacy space I mentioned. So we all maintain those legacy records, the IP addresses and autonomous system numbers, that were issued prior to the establishment of the RIRs.

All of the RIRs include the original registration date of that resource. So if you are looking in WHOIS to find something, you will see the original registration date. Most of the WHOIS data actually includes the last updated date as well, so you can see when an organization came in and made an update to the record.

It also includes information about the organizations that hold the resources and about the points of contact that are associated with the resources or with the organizations that are registered.

Additionally, it includes customer reassignment information I described, from ISPs to their downstream customers. When they're allocated space, they're also further subdelegating that space to their customers, and they do put those customer reassignments into the WHOIS database.

Additionally, routing information. As I mentioned, some of the RIRs include routing information. AFRINIC, APNIC, and RIPE NCC have a very different display than ARIN and LACNIC. ARIN and

LACNIC do not include routing information, but the other three registries do.

Can you click, please? Lastly, the WHOIS includes referential information. This is important. If you are looking for an IP address in the ARIN database, for example, and you don't see it, ARIN will have a referral to the authoritative RIR. We will point you to the RIR that actually is authoritative for that IP address block. We don't have any other information, but we will point you to the right RIR so you know where to go look for it.

Again, there's slight differences in WHOIS output. In the ARIN region, we have something called an RWHOIS server. We're going to put a referential link in the organization record if an ISP has chosen to use a Referral WHOIS server. Basically, they set up their own WHOIS server, and they put all of their customer reassignments into that WHOIS server. So if law enforcement were looking for a downstream customer of an upstream ISP, in the ARIN region, they would see a link saying, "This organization is using this RWHOIS server, and here's how you get there. So you'd have to go look further at the RWHOIS server if you wanted customer information.

Next, please. What information is not in an RIR WHOIS? There is some confusion sometimes, and I so many times have heard people say they look for the domain name in the RIR WHOIS. We have no information about domain names in the RIR WHOIS.

There are certain end user customer reassignments that do not show up in WHOIS. I know that sometimes foils law enforcement. I know it can be frustrating.

I mentioned already that some customer reassignments are going to be in the RWHOIS server, but there's certain policies that each RIR has that dictates how you show your reassignments. Some of the very smallest customer reassignments do not show up in the RIR WHOIS, and that's per the RIR policies. I know of at least four of the RIRs that have policies that allow the smallest reassignments to not be public.

There are some other customer reassignments that don't show up at all, and that is because the RIR has a privacy policy that allows the organization to choose whether to make their reassignments publically available or not publically available. They still have to submit the data to the RIR, so the RIR has the information, but they cannot display it publically.

This is an interesting one, and this is one that often confuses people, law enforcement, and even our own communities. The RIR WHOIS does not necessarily have the accurate geographic location of the network or the end user customer.

There is a reason behind this. The main purpose? WHOIS was designed to record registered users or assignees of an Internet resource. That's the main purpose. It's a unique registry showing who has what Internet resource. It doesn't necessarily show where they're geographically located. It typically has an address, but that can just be an address of a main headquarters, or it could be the address of an old customer, but the ISP changed and reassigned this space to a new customer and didn't let us know. It really depends. But that is not the main purpose. Accurate geographic location is not the main purpose of WHOIS. It is a recording of who is assigned resources.

Next slide.

UNIDENTIFIED MALE: Keep it slow.

LESLIE NOBILE: Okay. I thought I was slow. Some WHOIS tips. Basically this is just a summary of what we just talked about with maybe a little bit of additional information. Regarding data accuracy, it's the responsibility of the registrant to update their information and their customer information. So they tell us what they're going to put in the database. They send us the information via automated processes or via old-fashioned templates. It's their responsibility to keep that data updated. The RIRs do not chase after their customers to get updated information. Typically we don't do that.

The legacy space is rarely updated. As I mentioned, there's no contractual obligation, so there's no term or condition that says they must maintain that data. A lot of it is not being used or it's being used by researchers, and it's used occasionally or it's routed or it's not routed because it's used on a private network.

A lot of the legacy space holders got their space in the 1980s/very early 1990s, and they don't really feel the connection with the RIRs. They don't have much of a relationship, but I can tell you that all five of the RIRs have reached to their legacy spaceholders, trying to bring them into the fold, trying to educate them about what the RIR is doing and basically about their data. We're giving them options to become members, to get further services, etc., etc. So we have reached out to our legacy spaceholders.

As I mentioned, again, not all customer reassignments are in WHOIS. I talked about that in the previous slide. Sorry.

As law enforcement, if you do need data that's not shown in the WHOIS database – for example, I know with law enforcement, at least with ARIN, a lot of times they need financial transactional information. That gives them a lot of information about who they're tracking.

That is information that's private between the RIR and the customer, so you might need a court order or some type of legal process to obtain additional information that's not made publically available on WHOIS. We'd be happy to give it to you. We have it, but we typically need that court order or some type of legal process to give you additional information.

Next slide, please. Now that we all know what WHOIS is and its purpose, we'll move into WHOIS accuracy requirements. We're going to talk about three different areas as far as data accuracy requirements. We're going to talk about those required by a contract, a service or membership agreement that we have with our customers, because there are terms and conditions in there regarding accuracy.

We're going to talk about policies that require data accuracy across the registry system, and we're going to talk about an RIR's internal business practices, what we've put in place to make sure that we're getting accurate data and that it is maintained.

I put together these matrixes, and there is lot of information. I'm sorry. They're really crowded. You'll have this information later if you want to actually review it more thoroughly.

I'm mostly going to talk about the similarities because, as you can see, there's a lot of similarities in our contracts. We call them registration services agreements or membership agreements, and all five of the RIRs have those when they issue resources to their members. We set certain terms and conditions that they all must comply with.

The top thing you see with all five of the RIRs is every organization that gets resources from us must comply with all policies. They cannot violate policies. They must comply with all policies. Most of the RIRs require some accuracy regarding registration information, but not all of them do. But most of the contracts do require that accurate information is given to the RIR.

Next slide, please. What are the repercussions for contractual noncompliance? This is where we actually are all in solidarity. All of our registration services agreements and membership agreements say the same thing. If you violate the terms and conditions of the contract, the RIR will suspend services. We will not provide services to you. We will terminate the membership or registration agreement, and in most cases, the resources.

Sometimes there's a variance. You'll see that there's a number of days that some RIRs allow, but we will all terminate, just depending on our internal process. Then we will typically revoke those resources. If things are not rectified, we will take those resources back.

Next slide, please. We're going to talk now about data accuracy requirements per policy. What are the Regional Internet Registry policies that require organizations to maintain their data and provide us with accurate data?

Again, the thing that's consistent – policies vary based on regions, so there's slight variances. We actually have a policy matrix that we put out. It is maintained on the NRO website, and it's a comparison of all five of the RIRs and their policies. It's very brief. It's really easy to understand. If you're more interested, if you want more information about policy differences, that's where you can find it.

But the one thing that all five of the RIRs do require is that all customer assignments are put into the database. They have to be registered in WHOIS. If they are going to take space and give it to someone else, they have to let us know. That is a requirement of all five RIRs.

There are some other variances. We have other policies that require accurate points of contact or annual validation, but it depends on the registry.

Next slide, please. The repercussions for policy noncompliance. Again, this is really similar across all the RIRs. We do the same thing. If you violate the policy, we essentially suspend services. We will not provide services, and we will certainly not provide additional resources to you until you come into compliance, and in some cases, some of the RIRs will actually terminate the membership or registration agreement.

Next slide. Thanks. Data accuracy requirements per business practice. So this is what the RIRs do. These are internal business practices that we've all developed individually, but it turns out that we have some of the exact same things that we're doing. It's because we've learned over the years that we have to do this.

ARIN was hit very early on in 1999/2000. Everything was built on trust, right? The Internet was built on trust. It was bottom-up. It was community-oriented. So if someone said they were an organization and they needed resources, we just put them in the database, didn't check, and registered them, and then we issued them the resources.

But we found out early on that there was a lot of falsified information being given to us, a lot of lying, a lot of organizations making things up to get additional space and sometimes doing some bad things with them.

One of the things we did was we required that any organization coming into the region has to have a legal presence in the region. They have to be legally registered to do business. All five of the RIRs have that exact same requirement at this point. So we're all vetting our organizations to make sure they're real, they're accurate, and they're doing business in our regions. That's the one thing that's consistent across as an internal business process. There's a few variances that you'll see, but I just wanted to highlight that particular one.

What are the repercussions for business practice noncompliance? This is similar to violation of the contract, actually. This is pretty consistent. If you come in and you don't vet and you're not a legally registered organization, none of us will provide you membership. We will not register you in our database. We will not provide you any services. You actually have to be legally registered, and that is the one consistent thing we all do. You can't get in unless you show us and demonstrate you're a legally registered entity.

Next slide, please. We're at the end. So that is all I have on WHOIS.

UNIDENTIFIED MALE: [inaudible]

LESLIE NOBILE: Alice will.

ALICE MUNYUA: Thank you very much, Leslie. I think now we'll open it up for questions, but before we do that, I'll let the Chair of the NRO speak. Oscar, please.

OSCAR ROBLES: Thank you, Alice. Just two clarifications. One important difference with the traditional phone directory services or White Pages is that WHOIS services are not intended to provide information on individuals or end users of a specific IP address.

This service was created to indicate who is the organization in charge of allocate or assign that big block of IP addresses to the end users. This is relevant information because when we talk about accuracies or inaccuracies, it depends on what someone is looking for because if we are looking for information on individuals, obviously we won't find that information, and that would be a big difference with our expectations. That's related with Bobby's comment about the inaccuracy because there are so many of the institutions responsible.

I would love to see factual information because if there's something we can do, I think that our community would be more than willing to try to improve that performance of this query service. Thank you.

ALICE MUNYUA: Thank you very much. Just to let you all know, we have some sandwiches and drinks at the left of the room, providing lunch. The floor is now open for any questions and discussions or clarifications. Yes, please? Let us know your name and organization. Thank you. Then [inaudible]

UNIDENTIFIED MALE: Good evening, everybody. I prefer to talk in Arabic if you don't mind. So, please…

[inaudible] Okay. Good evening, everybody. [inaudible] I'm from Palestine and from the Communication and Information Technology. I am originally a member from WHOIS [inaudible] of WHOIS in ICANN, and also I am working in a new gTLD. According to the geographic position or location of Palestine, I am a member in [inaudible], and based on my experience about the [IRS], it is easily and if any problem happen, anybody can reach me out. At the beginning, I would like to thank all of you and therefore all the work that you are doing.

Now I have a question to Mr. Bobby. A while ago, somebody mentioned that because of some of the conflicts in policies between RIR, there is no enough information about the users. My question is if there is any possibility for this information to be available? How we can get this information? If there is no way to get this information based on the policies the RIRs are using or adopting, what can we do?

The other question is in – please, Paul. Everybody knows that the origin of the IPs in IANA, no matter where the location is. As a committee, what are your expectations and the results of this committee? Everybody knows that the governments and the committees – because this is looked at from two different point of views. The first one is the Internet as a network open to all, and from the side of the privacy. There are limitations about these privacies.

Also, I think that there is something to be addressed between two parties, between people who are in charge of privacy and human rights, and also who are experts in DNS and the industry of DNS.

BOBBY FLAIM: Okay. I think I understand your question to be, how can we work to improve the WHOIS inaccuracy? Is that correct?

UNIDENTIFIED MALE: Mm-hmm.

BOBBY FLAIM: Well, that's an excellent question because that's one of the things that we're trying to do here. I think we may need to look at several things. Number one, we want to see how we can, like I said earlier, incentivize the membership, the organizations, the ISPs, that make up the membership and the community of Regional Internet Registries to properly record the WHOIS so that we know who to go to to find that specific IP address and when it was being used.

Oscar made an excellent point. The point is not to find specifically the end user and get their information. The point is to go to the organization that has that allocation or assignment so that we can serve them with a court order to exactly determine when that IP address was being used and who was using it.

What we're trying to do with improving the accuracy of WHOIS is to develop policies, procedures, commonality within the Regional Internet Registry to ensure that the membership is putting in the accurate information with those assignments.

I hope that answers your question because the bottom line is we're working to develop stronger policies as an incentive to ensure that the accuracy is there.

PAUL RENDEK: How would you do that?

BOBBY FLAIM: How would we do that? We would do it by working with the RIRs and proposing new policies, globally coordinated policies across all of the Regional Internet Registries. And working with the community to make sure that that policy will be agreed upon and that they actually will comply with it and actually will actually do it.

PAUL RENDEK: Yeah. Make it a procedure.

BOBBY FLAIM: Right. Make it a procedure that can be followed through because a policy that isn't followed through is useless. It won't do anyone any good to have it on paper but not actually be enacted. There's no action behind it. So that's what we are trying to do. We are trying to stimulate action to ensure that people are physically going into the WHOIS database and putting in the accurate information as is appropriate.

PAUL RENDEK: Maybe the second [inaudible] thank you very much for your question. I'm going to attempt to answer the second part of your question as I understand it.

Speaking from the RIPE NCC, because everyone has a slightly different legislative process in their area of operation, where we are, we are an organization that operates underneath Dutch law. So we do have certain privacy protection rules that come from the European Union or from the Netherlands itself. We definitely follow what comes from the Netherlands.

Some of the work that we've done that might answer your question a bit is that we've worked actually with law enforcement over the last couple of years to document and make sure that we have as refined a process as we can get for law enforcement to approach the RIPE NCC to get information from its registration database, not the WHOIS, because that's open.

We have another database that's behind, obviously, a wall that is not publically available. We've done a lot of work in drafting the documents, seeing how we can shorten the process of how a subpoena would be given to us and what is the corporate governance we would follow as an organization to be able to provide that information.

If we're looking at the RIPE NCC – I cannot speak for all the registries; everybody can comment, of course, on what they're doing – in our area, we're probably as far as we can go in refining this process with the speed of which we would be able to provide the data we have to provide when we are supplied with a court order.

But we have to comply with the Netherlands legislation of the privacy on the data for anything that we would have. So WHOIS? Obviously public, but there is the information that is in there in registration database.

ALICE MUNYUA: Craig, you wanted to respond?

CRAIG NG: Thanks, Alice. Thank you, [inaudible]. What I do want to say is that, in addition to what Oscar and Paul has said, each of the RIRs have processes in place and programs in place to look at improving WHOIS accuracy. So quite apart from any policy changes right now, I think in each of the RIRs there are actions being taken, whether it be a community discussion that might develop into a policy or business practices. We are very conscious about the accuracy of WHOIS.

The other point I want to make is, I think to reinforce what Leslie has said, right at the heart of it, at the beginning of the allocation process, certainly from APNIC – and I am absolutely sure that each of the RIRs do as well – we put in a lot of effort to make sure that the entities applying for resources actually exist and they are who they say they are.

So it's not like domain names, where applications happen very quickly online without verification in the IP world because the allocations are actually large and involved. So we actually take a lot of steps to verify the corporate existence and the identity of the people behind them.

In addition to that, we certainly have contact information that we verify yearly by different means. In APNIC's case, for example, the account needs to be renewed every year. The message is sent to the e-mail address that we hold for the contact, so that we do actually have a contact that works in order for that account to be renewed. So there are a number of measures that are in place.

ALICE MUNYUA: Oh, you want to add?

PAUL RENDEK: Yeah. Thank you. Thanks, Craig. Actually, if I can just summary this, because you asked Bobby the first question of how would we get involved in this, I'm going to drop the gloves and give it to you very clearly on how you can actually do this.

You need to actually participate in the community policy development processes if you want to make a change. You cannot simply come to any one of the RIRs and say, "We as law enforcement want you to have this procedure in line." We can't act on that. We actually can only follow the procedures that are built in the policies for things such as maybe making new policies on WHOIS accuracy.

So, as Craig said – he's very right – we all have WHOIS accuracy discussions inside our communities. The way you can make a change is that you need to get involved in that. You need to understand what you're actually needing or what you're wanting to solve. You need to come with a proposal and put that proposal into the policy development process and have the discussion inside the community.

Hopefully, your policy proposal will be accepted. If it is accepted and people do understand what you're trying to achieve – and I think that, in general, the communities do understand that law enforcement has real concerns. We are as concerned about the security and stability of the Internet as you are. We're all in the same line there. So if that was to happen and your policy goes forward, it would then become a procedure, and we would have to follow that. Therefore, we would make all of our members follow that. That's just the line of how you would do this.

Again, I understand that it's probably something that wouldn't come natural to a law enforcement agency to say, "Oh, yes. We're just going to become a part of this community and follow this process."

But actually, it has worked in the past. In fact, Bobby has managed to change policy in ARIN. I watched him do it. So it is very possible.

We are here as RIRs to work with you, to help you understand how you would inject something that could effectively change policy around this. That's important to note.

ALICE MUNYUA: Thank you, Paul. I have [Indonesia] and then Europol's Greg. [Indonesia], please.

UNIDENTIFIED MALE: Thank you. Just curious to know about the IP numbers and the security. Sorry if my question looks a bit stupid because I'm not very well aware of this.

You mentioned in your presentation that everybody is an IP number, including me. Including my handheld. It's an IP number.

Now, I would like to ask the FBI: how will you identify the person if they are using dynamic IP numbers, using Wi-Fi, like in this room, and they are using, say, a slightly cheaper handheld with a [hot] e-mail number, [inaudible] number from GSMA? And using a prepaid, [pilfered] card which is already on. [inaudible] [available] many countries.

How can you identify that one? There's several hundred people in this [inaudible], for example. Thank you.

PAUL RENDEK: I was going to make a joke, but I won't. No. To use the WHOIS, whether it's for domain names or IP addresses, it's just one tool. It's just a triage tool. It leads us to one of the organizations that we can get further information from. It is not the be-all-end-all. It's not the one-stop shopping. It is not the identifier. Once you have an IP address, it is not the identifier, but it leads us in the direction, just like when we go to an Internet service provider and we're like, "Okay. Who was using this IP address at the time?" So it depends on how the ISP themselves have configured and if they can actually tell us that information.

Now, here you've made a good point. We're all using kind of we'll assume one IP address. It's all NATed and networked. We're all using one IP address. There's 100 of us in the room. How do we determine who was using that IP address at the time to use it to commit a crime? How do we know?

Well, we would know that everyone's in the room, and then what we would have to do is we would have to go on an investigation. We would have to use the old methods of Sherlock Holmes. We would have to interview people. We would have to see if there were cameras in the room. We have to see if anyone twitched the wrong way. We would have to do all different types of things.

So when we come and we're saying IP addresses are important, they're important but they're not conclusive. They are very important as a first step in investigation. If we don't even have that first step to get to at least the beginning – or let's just use this room as an example. If we couldn't even find this room and we're going from room to room to room to room to room, we're wasting precious time. We have to know that this is the location and this is where we need to start our further investigation and go into those old-fashioned methods of interviewing and other physical types of evidence.

But you're absolutely correct, and I don't want to give the illusion that this is one-stop shopping and this is where it all begins and ends because it's not. It's just one part of the process. We always try to stress that. It's one tool, one part of the process, but an important one.

I hope that answers your question.

UNIDENTIFIED MALE: Very good.

ALICE MUNYUA: Europol?

GREGORY MOUNIER: Hello. Gregory from Europol. Thank you so much for your presentation, both of you. They were super interesting, very helpful. I'm really glad to see that there is such a robust corpus of policies and accuracy and requirement and contractual obligations. That's all great.

But the feedback I get from the investigators is that, when they're after an IP address that is being used for malicious activities, most of the time that IP address has not been allocated by one of your members. It has been allocated by somebody down the chain in a smaller ISP or something.

As far as I understood what Leslie said, it's the registrant's responsibility to have accurate information, to put accurate information in the WHOIS.

So now my question is, what type of advice could you give us, the law enforcement community, to try to achieve the same accuracy requirement that your members have down the chain and to be sure that our investigators, whenever they're looking for an IP address and they go a local ISP, they get accurate information?

Like in the case of RIPE, for instance, our investigator would go to KPN, which is a massive Internet service provider and member of RIPE. Of course the information will be accurate. That's no problem, but KPN has given a block of IPs to others and they resell, resell, resell, and that's the main problem.

What's your advice for us to try to extend the scope of the accuracy requirements down the chain, almost to the end ISP user? Thank you.

PAUL RENDEK: Go ahead.

LESLIE NOBILE: Okay. Hi. I can answer this partially. I'm not sure I can actually give you the right advice, but I can tell you that, in our contracts, at least the ARIN contract – I'm not sure about the others; they can comment – but our contract requires the upstream ISP to maintain the data of their customers and their customers' customers. Our policy also requires the exact same thing. It's expected that if they are issuing from this top level, each level has to comply with the exact same policy, which is to update the RIR.

What we've seen with reallocations? They can go down, at least in the ARIN region, as far as five levels. We've seen five levels down of reallocations, and we've actually seen them in the database. So some do comply. Some do not comply.

The way we've traditionally stopped them or caught them and enforced that rule is, when they come back for additional address space, we review their assignments. We say, "What did you do with your last blocks? Tell us." Then we choose some of their customers and we get very specific.

If they don't comply and they don't have that information and it's not publically available in WHOIS or RWHOIS, we deny them services. We will not issue further resources.

This has become a problem with IPv6. The IPv6 blocks we're issuing are very large. Most of the ISPs are never coming back to ARIN for additional resources or to any of the RIRs, only the largest. So that customer reassignment information, while I'm seeing it in the ARIN region and I think it's in other regions, it's not consistent the way it was. We no longer have a hammer. We no longer can stop them.

So unless we're physically going after them and proactively identifying this, we don't have that hammer that we did. The only thing I can advise is I think, in the globally-coordinated policy arena, if you are going to consider a globally-coordinated policy, you want to put the hammer. You need the repercussions.

You also need, as Bobby said, to incentivize the membership. I don't know if that's a carrot or a stick, as we say. I'm not sure you'd want to do, but I really think you all need to put your heads together when you do consider a globally-coordinated policy and work with us. We'll help you.

But I think that's really the only way. I don't know if anyone else has a comment, but…

MADHVI GOKOOL: Just to add to what Leslie said, at AFRINIC, we do have our members who can sub-locate their customers who are ISPs. This is an exercise that we've started recently. We audit these what we call sub-locations – when they come back from resources, though. We don't do audits regularly, but when they come back for additional resources, we do make the audits.

What we have also had to do, which is resource-intensive, is to actually make our members understand the need to further register the customer assignments and that they have to transmit this information to comply with the policies that we have already to these customers who are also ISPs. It's not an easy task, I must say.

ALICE MUNYUA: Thank you. I have [inaudible], and then FBI. Eranga, not Bobby.

UNIDENTIFIED MALE: My name is [inaudible]. I'm with the GAC. When it comes to Facebook and [inaudible] pages, do you have a good cooperation? Because people really can see the IP [inaudible]. They will have to deliver the IP address after. So you need the time. Do you have a direct access or cooperation with them?

BOBBY FLAIM: Let me make sure that I understand your question. For Facebook, you're trying to go back to something that's occurred on Facebook –

UNIDENTIFIED MALE: If someone has a fake account on Facebook and…

BOBBY FLAIM: Yeah. That's a little bit of an issue because then you're talking about a content provider. Therefore, a lot of that becomes very tricky.

PAUL RENDEK: You need a court order?

BOBBY FLAIM: Yeah. You would need a court order, but you'd also have to go to the service provider to see where that originally was coming from. A lot of times, that's even tricky because you have to log source ports and you have to have some specific times. That becomes exceedingly tricky, and that's a very big challenge for us as well.

I can go into more about carrier-grade NATs and source ports. Craig wants to add something.

CRAIG NG: Hello. In relation to the content providers – and this is in my interaction with them wearing the law enforcement sort of engagement hat – I know a lot of them.

Google, Facebook, and Microsoft are very, very conscious about this. What they have done is incorporated into their terms of service, in their contract with their subscribers, the ability to reveal information to law enforcement.

Now, they all differ slightly, but they have the ability to disclose their information to law enforcement agencies, depending upon their different processes.

So each of Facebook, Google, Twitter, and Microsoft have very established practices dealing with law enforcement agencies. I know Facebook, for example, has a whole team dedicated to law enforcement interaction. So if it is Facebook, I can actually give you the contact person for that. From my understanding, they do work very closely in relation to that.

UNIDENTIFIED MALE: Okay.

ALICE MUNYUA: Eranga, and then [inaudible] the European Commission.

ERANGA SAMARARANTHA: Sure. Thank you for the presentation. I found it very helpful. I have two questions. One relates to the answer you gave to the previous question, just in general about forming globally-adopted policies, and more specifically, procedurally I guess, how we can implement that and what role the NRO has to that and if it's something that needs to done at each RIR or if the NRO plays a role in a more large RIR-wide policy formulation process.

The second I think may relate to ARIN. I thought your discussion of RWHOIS was very interesting. If you could speak a little bit more about that, if you could correct me if I'm wrong, if that's a service that only ARIN has, and if so – it seems that it's something that we'd be interested in – if it's possible to expand that to other RIRs? Thank you.

LESLIE NOBILE: I'm actually going to briefly describe how a globally-coordinated policy works, and I'm going to describe how an RIR policy works. It's a very simple process.

As we mentioned, it's open to anyone. Everyone is a community member. Any one of you can submit a policy in any of the regions. You don't have to be a member. So you're just a community member.

It's developed bottom-up, so you propose it and the RIR staffs will implement it. Each RIR has its own community-developed policies based on the needs of the region, but if you're talking about a globally-coordinated policy, it's the same principles. Anyone can do it.

What it requires is you as an individual or as individuals working together with community members if you need guidance. In each of the regions, there's people that are policy experts. There's also staff that can help guide you. We can't make policy, but we can help you because we know what it is you need.

So you want take that same policy and propose it in each region. Each one of the RIRs has their policy development process listed on their webpage. It's detailed on how it's done. It mostly involves submitting policy text to an e-mail address. Then that gets publicized on a policy mailing list. That gets discussed by the community. If there is a consensus reached, it gets adopted.

With a globally-coordinated policy, you want to take the same text to each community. It has to be submitted to each RIR individually. The same people can do it. Then that's what gets discussed.

There's no guarantees that a globally-coordinated policy is going to be adopted in every region. In some, it could be adopted in two out of the five regions. It can be difficult, but that's why I suggest working with community members because they're the ones that know how it works and they can guide you. We can tell you which community members in each community. Each one of us can tell you who your best bets would be and where you're going to have the most success and the most help from community members.

That's what the globally-coordinated policy would be. It's slightly different in that it gets taken to each region. Does that answer your question about globally-coordinated –? Okay.

The question about RWHOIS. It's kind of interesting. Our WHOIS was developed by our engineers way back in the DDN-NIC days. It was just a service for organizations in the ARIN community.

I don't think any of the other RIRs have ever even talked about it. I don't really know the situation in the other regions. It could certainly be used anywhere. It's just a tool. It's an open-source tool that anyone can use, but I don't know where the interest lies there, and I think that's something that would be brought to the community probably by a policy.

PAUL RENDEK: It would be a database working group policy.

LESLIE NOBILE: Yeah. I think that's probably how it would have to go if you were going to implement it or institute it somewhere else. Does that help? Did I answer that? Anything else?

ERANGA SAMARARANTHA: Yeah. Could you just speak a little bit more about RWHOIS as a tool [inaudible]?

LESLIE NOBILE: I don't know a whole lot about it. From a technical standpoint, I know what happens. I don't know how they actually set it up. They stand up their own RWHOIS server, and then the requirement in the ARIN region is that it's always on so that anybody from the public can come to ARIN's WHOIS database, look at the organization record, see the link to the Referral WHOIS server – it's right there – and you click on it. You're supposed to see any customer reassignment that is in the database.

It's the same policy requirement. You must register your customer reassignments, whether that be in WHOIS or in your own RWHOIS server. It's the same requirement for both.

As I said, our policy requires the RWHOIS server to be on 24 hours a day, always on, and we have a system that trolls the

RWHOIS servers to make sure they're on. If they're not, we notify them and we say, "You have to make that public. Turn it on."

So that's pretty much all I know.

ALICE MUNYUA: Okay. I'm afraid we're running out of time, but we'll allow the European Commission one last question.

UNIDENTIFIED MALE: Thank you, Alice. [inaudible], European Commission. I have a question based on the presentation from Leslie, but before asking the question, I want to indicate, indeed, our appreciation for this dialogue with Regional Internet Registries. We greatly appreciate that.

My question. Leslie, you mentioned that, regarding end user reassignments, that some small customers may not show up in WHOIS and that there are at least four Regional Internet Registries that have a policy on that. You stressed the commonalities between policies, but of course, there are also differences, for example, in relation to this, I suppose.

Because that's something that would really appreciate, that would be really helpful for this development of global policies, do you have some kind of evaluation, some kind of figures as well, on the influence of the differences of those policies on the accuracy of WHOIS information?

For example, the fact that four of the Regional Internet Registries do allow these small customers not to get reassigned – does that really influence the accuracy? Does that have a consequence? Do you have that information? Do you compare that amongst Regional Internet Registries?

LESLIE NOBILE: I'll answer the last question first. We do not compare information amongst ourselves, the registries, on that.

The policy basically says, if you have this certain size of a reassignment to a customer – a /29 or a /30 in IPv4 – you don't have to put that in the public WHOIS, but you still have to report it to the RIR. So we still have a flat file with that information, at least in the three out of the five regions. I think three of us have that policy. We still get that data, so if we came to us, we could give that data to you. We still maintain it, so it's still the same accuracy. It's just not public.

We haven't done any comparisons on that, though. I don't know if I've answered your question. Maybe you can help me a little.

UNIDENTIFIED MALE: If you want to develop policies, of course, you need facts, so you need to collect data. You need to collect statistics. In order to find the best practices amongst Regional Internet Registries, it would be really useful if you would be able to show us some statistics among the use or the abuse of WHOIS or IP addresses, and then compare that amongst Regional Internet Registries.

LESLIE NOBILE: That's a good question, and that is something that you can send to us. All of us would be happy to comply with requests for statistics. If we can get the data for you, we will get the data for you. That's just something you can ask any of us for that through a formal e-mail or informal e-mail. We are happy to provide data.

ALICE MUNYUA: Thank you very much. Very interesting discussions, but we have to wrap up. I'll give Paul and Bobby the mic to give us very quickly what the next steps should be, and then I'll invite the Chair of the NRO for the last words. But first, Bobby, then Paul.

BOBBY FLAIM: Thank you very much. I won't say very much. I think that this was a great introduction, and I think we just need to work with the RIRs to actually maybe meet again or certainly come to their meetings, but maybe meet again and hold maybe a special session to delve into some of the technicalities and the procedures on how we can be very specific on how we do this and how we could work with them.

Thank you all for speaking with us. Always a pleasure, and thank you again.

ALICE MUNYUA: Paul?

PAUL RENDEK: Yes. I'd like to echo what Bobby is saying. It's a great pleasure. We do have good relations with the LEAs. We would like to keep that momentum going forward.

I think two areas where we could look at in the future that brings us together and can bring something positive out of working together is taking a look at maybe what we can do. If you would like to get involved in the policy development process, I think taking that to another step is probably something that would be very interesting for the PSWG moving forward.

A second thing would be training. We've worked with a lot of law enforcement. I know that we've worked with Europol. We've given trainings there. We've given them at various LEAs across our service region. We have an understanding of what are the issues and what people are looking for there, so we do have some materials on maybe how to help you mine the WHOIS data and probably be that first step in helping you with your carrying on with your investigations so that you don't get stuck somewhere in the WHOIS.

They have been very positive, and we're happy to share them and continue those. So we would like, of course, then to hear the feedback from the LEA community that you would like to go forward with something like this with us, and we will provide.

Thank you very much for this opportunity.

ALICE MUNYUA: Okay. On behalf of the Public Safety Working Group, I would like to thank the NRO, and especially the Chair, and give Oscar the last word. Oscar, please.

OSCAR ROBLES: Thank you. Thank you very much for this opportunity to listen to these kinds of concerns. We are always open to know what things we could try to go further.

Please feel welcome to attend any of our meetings and present these kinds of concerns because it is not only to give you the information – which sometimes we may have it, sometimes we may not – but also in the case there's one proposal to change this, you have to have the support from the community. So we would like to have you. Please don't be shy to show up in our meetings and start talking with the rest of the community.

Thank you very much.

ALICE MUNYUA: You're all welcome to sandwiches and drinks on the left side of the room.

[END OF TRANSCRIPTION]