Note: This text is the result of live transcription work conducted by professional transcriptionists for the purpose of creating an aid for participants in this ARIN meeting. It is currently unedited and has not been proofread or corrected. It should not be relied upon for purposes of verbatim citation of the meeting proceedings. Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible statements made during the meeting or transcription errors. It is posted as an aid in understanding the proceedings at the meeting but should not be treated as an authoritative record. A clean and proofread transcript, that has been edited for accuracy to match the audio/video recording of the meeting, will be published approximately 10 business days following the close of an ARIN meeting as part of the formal meeting report.

APRIL 29, 2025, 9:00 AM EST

-oOo-

Opening and Announcements

Hollis Kara: Welcome to ARIN 55, Day 2. I'd like to start off in the room with a thank you to our elected volunteers from the Advisory Council, the Board of Trustees and the NRO Number Council. Can I get a round of applause, making sure everybody is awake. Thank you volunteers.

(Applause.)

We'll breeze through this quickly. Folks joining us online who maybe weren't with us yesterday, do take advantage of the Q&A and raising-hand option in order to submit comments or statements during Q&A periods.

Please also take advantage of the chat, but understand any questions that you put in chat are not going to make it here onto the floor in the room. So do use Q&A and raising your hand during those periods, and remember to lead off with your name and affiliation. Thank you.

Really excited to see such great online participation yesterday. Let's see if we can keep that energy up.

Virtual help desk is open. If you're having any issues, our real, live ARIN staff person will be there until 9:30 and again at the lunch break. I think Jason is on the desk. Thank you, Jason.

If Zoom disconnects, once again, try to reconnect. If that doesn't work, head over to the livestream for information about what's happening. And if that's down, just hang in there. We will be sending you an email as soon as the meeting is available to reconnect.

But hopefully we've had a great network so far. I'm very confident, knock wood -- everybody knock wood, if you can find any -- that things will remain in good shape today.

In person, again, feel free to join the Zoom. That link is in the event hub on the ARIN 55 site. But if you do, please make sure you're disconnected from audio and your devices are muted. But you're free to hop in and chat with the virtual attendees if you would like.

And when we open the microphones for questions, remember, again, lead with your name and affiliation. And please try to speak slowly and clearly for the benefit of the transcript.

Wi-Fi information. Hopefully everybody's on the network, but if you're having a challenge, please talk to the registration desk out in the hall.

Slides are available online for all of today's presentations, and live transcript and webcast are available as well. You can access those from the ARIN 55 website or directly from the ARIN 55 Meeting Materials page.

What's on the agenda today? We've got a lot of updates. The thing I like about Tuesdays, or the second day of the spring ARIN meeting, is it's really all about ARIN accountability. We do still have a policy block, and we'll be talking about policy. But remember, we are a member-based, nonprofit organization. So what we do we do for you.

And part of that is informing you how we are using the resources to benefit you as a community and make sure you're up to date on the work that is happening inside of ARIN at the times we're not here at the meeting.

So we're going to be hearing from engineering, information security, routing security, a little bit of a deep dive into how ARIN manages its trust anchor, IPv4 transfer services. Take a break, recalibrate.

We'll come in and we'll have an update on our outreach and Fellowship Program as well as hearing from our grant recipients. We have our current grants ongoing, and we have reports from both of those programs so you can hear what they're doing.

Then we'll shift gears and we'll have updates from all of our Fellow RIRs, hear what's happening in the other regions.

Then we'll take a break for lunch, come back at 1:30. Mark your calendars. That will be our second policy block of this meeting. We've got four policies on the docket to talk about today.

When that wraps up, we will have an update from our chief experience officer and then from our registry integrity and oversight team lead. Take another quick break.

Come back and talk about what's happening with ARIN agreements, with data accuracy, our outreach and engagement strategy for 2025 -- take a little bit more of a deep dive into that. And then close out the day with an Open Microphone. So lots of good stuff happening.

Note that if we do find we need more time for the policy discussions today, we will adjust the schedule accordingly, and that could result in some presentations that are on the agenda today being slid back to Wednesday, potentially.

Not too worried about that happening, but feel free to -- we're here to talk policy. So if there's things to talk about, take advantage of the opportunity while we're here in the room.

Again, just a reminder, standards of behavior. You all checked the box when you registered. Hopefully you gave it a look over. I think everything's been going well. Just remember, we're all here with the same goals in mind and to treat everybody with courtesy and respect.

If there is an issue, we do have a reporting framework for that. And you can always reach out to Stacy in the back of the room. She is here to help with facilitating discussion about any issues.

All right. More audience participation. Let's take a second and thank our Network Sponsor, Spectrum. Can I get a round of applause.

(Applause.)

Our Webcast Sponsor, Google, let's hear it for them.

(Applause.)

Our Platinum Sponsor, AWS.

(Applause.)

And our Silver Sponsor, IPXO.

(Applause.)

And then last but not least, before we start in with presentations, I want to take just a second. For those of you who are maybe longtime members of the ARIN community, this day may stand out for you.

In 2013, on this day we lost our good friend and colleague Bob Stratton, our former CFO. I really firmly believe that his impact on the organization is still felt in our organizational values. And he was the heart of the community for quite a while. He did a lot more than taking care of the books.

So for those who remember or those who don't, if I could have just a round of applause in memory of Bob.

(Applause.)

All right. With that, I'd like to welcome our chief technology officer, Mark Kosters, up to the stage to give us an engineering update. And, yes, he's been informed the clock is running.

Engineering Update

Mark Kosters: So I think I've been told to be prompt. There it goes, 14 minutes and 56 seconds. That's what I have to go ahead and do this presentation. I'm actually going to be a little quicker than that.

This presentation and the following presentations are all kind of interrelated. So what you hear from me, you'll hear a follow-on from Christian. You'll hear a follow-on from Brad. Then I'm going to talk a little bit more. Let's go ahead and get started.

Here's the agenda. I'm going to talk about the services that we offer, very briefly. Statistics, so you can see how we're doing. Seeing if we're going up to the right, going down to the left, whatever.

Let's see. Software releases and improvements. Core services. Here's the services that we offer. We have an added something and we've removed something. Has anyone noticed the removal of the FTP protocol from our repertoire?

Were there people using it at the end? Absolutely. I don't know why. But I hope they've moved on. So I think people set up contacts from the early 1950s and left them there. Anyway, it goes on and on and on.

It was retired 31 of March, and it is gone. Yes, Louie.

Louie Lee: Louie Lee, Google Fiber, and this is Louie's hat. I assume you have the IP addresses of those that were still doing FTP. If only there was a way to look them up.

Mark Kosters: I did.

(Laughter.)

What was interesting is that we looked at sort of interesting hosts that were actually pulling from and talked to a number of them as well. So it wasn't just, let it go. We actually were fairly active in making sure that it was -- when it was retired, that there would be no surprise. And I suspect there was no surprise.

Here's our internal support. And actually I want to highlight one thing here. You see ARIN Online, our staff interface; security and performance monitoring, which most people have; cloud-based tools that we use for a bunch of different opportunities within house; various development and testing environments -- and we have lots of them.

Email. So email, we had hosted exchange for a long time. We have now moved to Exchange Online. So our corporate email is in the cloud. So thanks to Frankie and Pete and many others, this is something -- it's really hard to move something that's in flight and moving along lines, but we actually went ahead and did that. And we are now fully on Exchange Online.

And I don't know who got it first, it was ARIN Online or Exchange Online. But anyways, I think we were first.

Analytics. We use infrastructure tools like Jira, Confluence, build agents, et cetera. Most organizations do that. And of course our financial systems.

Services that we can simplify. Here's the next one that we can start thinking about. We have four directory services that do the same thing. Normally it's really three, but there's a fourth one we added here, and that's RWhois.

So we have Whois, which has a predominant amount of traffic going to it. We have RWhois, which was a way of doing reassignments locally, so you can actually do things there. But there's still referrals. It's actually built into the Whois client now.

There's Whois-RWS, which is actually one of the ancestors -- or actually it's a parent of RDAP, which is the industry standard and the way that we're going to go for directory services in the future.

So this is something that we're teasing right now. And there's most likely going to be a consultation later this year talking about how we can actually retire two of these, RWhois and Whois-RWS, and see what the community thinks and how it should go forward.

Statistics. ARIN Online. I'm continually amazed with the number of people that come in every year. We consistently get 15,000 new accounts every year. Amazing.

ARIN Online logins, cumulative. We have lots of people that do one and done. I'll note that many of these things are actually -- I need to retune this for next time and actually take out the people that are locked because they don't have 2FA on there. That's an improvement I'll make for the next time.

You'll see this number dramatically change, but there's a lot of people that don't have 2FA on their accounts or MFA, multi-factor authentication, on their accounts. And we lock them, but now we have a lot of people that continually use ARIN Online, a lot of power users that actually use ARIN Online.

Multi-factor authentication. You can see that TOTP is going a little bit faster than SMS now, which is interesting. It's good to see. FIDO2, still fairly small and will probably continue to be that way.

Whois and Whois-RWS. I like to show this slide because Whois has been there forever, and it was built in a time when there was only v4. And actually it's the next slide. I'm sorry I'm going to get to it in a minute.

Here you see that Whois, we had a peak of almost 6500 queries per second. That has come down some. Whois-RWS has seen 1000 queries per second and continually grows.

Now here's the one I was wanting to talk about, v4 and v6. RDAP is actually a fairly recent protocol and has had an opportunity to be developed in a time where there's both stacks available, both v4 and v6. And what's interesting here is that we're starting to see a slight uptick in the amount of traffic that's sourced v6, which is interesting to me.

You can see that RDAP is actually increasing in use as well.

RRDP, you can see it's fairly consistent on the people that use to pull-fetch our repositories via HTTPS protocol.

RSYNC, fairly consistent as well. It's a little bit more -- goes up and down a little bit more. This is of interest to me. It's much less than RRDP, but it's one that I look at because this consumes a fair bit of CPU on our boxes.

DNS, it's fairly consistent. It's by far our most heavily trafficked site, our service that we offer, which is not all that surprising.

And now let's talk about releases and improvements. Public, we have RPKI and IRR integration that we put out. We have ASPA preparation that we've done. And it's actually available on our OTE environment, and Brad's going to be talking about that more in the future. We have numerous bug fixes that we put out.

Internal, we've been working on tech debt. Continue to do so with financial controls. Ongoing, we have SOC 2 audits, which is something that is always underway; PCI audits that we go through; and availability enhancements to our provisioning systems.

System improvements, continuing to move to Kubernetes. Moving to KubeVirt VMs for -- under OKE, which is a Red Hat product, for our public-facing sites. And continually consolidating our monitoring into Prometheus away from Sensu.

Now, for something that was alluded to in Nancy's presentation yesterday, one of the big things we're doing is we're moving to a new data center. Our current data center is substandard. What I really like is someone came to our office, and we gave them a tour of our data center, and it was done by a contractor that maybe didn't quite know what they were doing in an HVAC way. I don't know. But we've had lots of issues with HVAC over the years. So much so I think a couple of us are now certified AC technicians.

We've also had problems with leaks on the roof, and it's not fun having water coming in, dripping on your UPS, for example. Does not work out well.

So it's something that we're looking forward to, moving to a colo and removing the site from the equation.

The objectives are, one, to reduce technical debt. As we move this, we're actually changing our environments running our entire infrastructure under Kubernetes, which will in turn allow us to be more highly available. And to do so, we're actually moving mostly new equipment into our new data center as well.

There's a few select devices that we're moving from site to site, but we're mostly going to throw all the things in the new site, turn it on, turn the old site off, and remove that old equipment that's been there for a long time.

One of the things that's kind of cool about this is the database. The database is now running under Kubernetes. For me, being an old-school database guy, this is kind of scary. So here is the sort of crown jewel of ARIN, you could say, that's running under Kubernetes.

And we had a very innovative solution working under Postgres before, and we moved to an even more innovative solution, so much so that it's worked out really well. We had a lot of middleware support from our support vendor, and it's quite innovative.

And there's going to be a talk at the Red Hat conference here in Boston in May talking about this work that we've done here. It's actually pretty cool to see this work underway.

Here's our planned public enhancements. ROA aggregation, which actually means we can edit our ROAs as opposed to adding and deleting them.

Routing intelligence for RPKI, where we will actually allow you to see, much like RIPE and APNIC do now, allow you to see what routes you effect by the ROAs that you put in or present.

Internal improvements. We're looking at creating staff efficiencies for our internal tools.

RDAP enhancements. This is something that's ongoing. It's creating parity between Whois, Whois-RWS and RDAP. And there's all kinds of protocols and conformist standards that we're looking for, to do, so that no matter which regional registry you go to, you will expect the same results. So you do the same query, you'll get the same results -- of course, for region-specific data.

This is something that's ongoing, and there's going to be more here. And we're actually putting a lot of standards work, and we've talked about this before with geofeeds, and actually integrating some RPKI information as well so that you can do a Whois-like feature using RDAP to find out information, who the contact is for that particular ROA, et cetera, whose organization is associated with that ROA. It's something we're looking forward to coming to the table with.

And that's it, and I have two and a half minutes.

Hollis Kara: Good job, Mark. Anybody has questions for Mark, please approach the microphones. Folks online, please start typing. We've got one in the queue online. Mark, it's up to you. Do you want to take a virtual question first or start on the floor?

Mark Kosters: Let's start with the virtual today.

Beverly Hicks: Matthew Cowen, unaffiliated: "Are there any plans to deprecate 2FA by SMS given its questionable security for that job?"

Mark Kosters: This is sort of a common question. The community, if this is something that -- it's a pretty popular type of service. So I would say that this is something we could look to in the future, but not at the moment.

Louie Lee: Louie Lee, Google Fiber. Again, this is Louie's hat. To follow on the 2FA piece, maybe you make it not the first option for SMS. Make it like you have to click through for further options, just to get people thinking about something else first.

Mark Kosters: Good point, Louie. I like that.

Louie Lee: The actual question I came to ask, have the various departments given you a list of places in their processes where it's a manual step that provides a chance of human error that maybe you can help automate in order to reduce that chance?

I've heard that there's a fear that somebody might accidentally take a route down just because of a typing error. So I hope that it's been prioritized for you in some way.

Richard Jimmerson: Thank you very much, Louie. This is Richard Jimmerson, chief operation officer. John Sweeting and his Customer Experience team, there's specifically a team inside the organization that is studying that problem. They've been studying it over the last year. They continue to do that.

And it lands as development projects on our 18-month schedule. We have things scheduled on there now doing exactly the things you're describing. So we're focusing on that pretty heavily.

Louie Lee: Fantastic, thank you.

Hollis Kara: Wonderful, come to the other side.

Andrew Dul: Andrew Dul, 8 Continents Networks. Mark, you mentioned the term "innovative" with regards to the database multiple times. That got me scared, thinking highly customized and very hard to support.

Mark Kosters: Not in this case. One of the things -- I totally understand what you're saying. And actually I share some of those concerns and shared some of those concerns with the team as we were building this. But we went through extensive tests. We went through extensive tests on, okay, let's take this down. Let's take down the database this way. Let's take down the database that way and see how it comes up. And actually it came through with flying colors.

So this is something that, yes, Kubernetes running this stuff is definitely interesting. Having support with our third-party vendor has actually been a real asset, making sure we're good. But we're not first to the marketplace here on this.

This is something that we've been taking our time with. And trust me, I'm a very conservative person, and this is going about it in a very conservative way.

Andrew Dul: Are you guys offline copying into a vault at some point as part of your process still?

Mark Kosters: Yes, we take backups continually, and we actually put things off to tape old school, once a day.

Kevin Blumberg: Kevin Blumberg, The Wire. A couple of rapid fires. You pick which ones you want to answer.

(Laughter.)

Singular data center?

Mark Kosters: Multiple.

Kevin Blumberg: Multiple. Geographically diverse?

Mark Kosters: Yes.

Kevin Blumberg: Thank you. Put legacy, deprecated, whatever, next to SMS. Start doing that with anything that you plan to phase out in the next five years.

RWhois, stop calling it RWhois. Call it legacy -- sorry, your Whois. Yeah. Arrr.

(Laughter.)

Just start letting people know well in advance that you're planning to deprecate and get rid of these technologies.

Email lists, as old as the thing that you got rid of, FTP. So it's great you're working on some new stuff there. Come up with better technology for us to collaborate as a community. Yes, it can use email as the basis, but most people have moved to hybrid environments for that.

And lastly, congratulations on the new move. Sorry about your water leaks and all of that. I think everybody -- I've heard from many people, move it to somebody else's problem. It's great you've moved it to colo. I've got news for you: You'll have water leaks in the colo. Move it to somewhere else. Get it out of your bailiwick. Get it into the cloud like you did with email. Maybe that's your first foray into the cloud is getting your email there. Get the stuff out of your own responsibility.

Mark Kosters: Thank you, Kevin.

Atefah Mohseni: Atefah Mohseni, ARIN Fellow. I'm curious, how do you measure ROI, return of investment, in some of the new deployments like RPKI service, and if you have any monetization plan for them?

Mark Kosters: Interesting. So actually this is part of our core mission. So it's not really -- it's a little bit different, and it's probably a better question for John Sweeting, I think, than me in terms of -- on dealing with this. But it's part of our core mission and one of the things we support, along with our other fellow RIRs in making this go.

So there's not really a monetization thing. I mean, you all pay membership fees. And as part of that membership fee that you have, you have access to these services.

John Sweeting: John Sweeting, chief experience officer. I'll add to what Mark said. There are some services we have to provide, and the way we provide them, the return on investment is how well we provide them to the community that the community feels they're getting the return on the investment on what we're doing.

And if they feel they're not, then they tell us about it by, hey, you need to make better services. And that's really the way we look at our return on the investment, is how well we can satisfy and the value we can give to you, the community.

Mark Kosters: Thank you, John.

Chris Woodfield: Chris Woodfield, ARIN AC. Yesterday, in the Financial Report, there was a mention of software and infrastructure costs coming in below budget, and I believe there was a mention of less spend on software licenses driving that. Did this status under migration factor in that as well?

Mark Kosters: No, it didn't. It was a combination of what we thought the price would be and what we were able to negotiate to, for example. It was sort of our primary factor.

And in other things, we're either deferred or we were pleasantly surprised by what we found out.

Chris Woodfield: Okay, thank you.

Louie Lee: Louie Lee, Google Fiber, Louie's hat. As a community member, I might say I find value in RPKI not being charged as a separate service, to keep the bar really low so that more adoption can happen.

Mark Kosters: Great. Thank you.

Hollis Kara: All right. Do we have anything further online? Got a "no" from the riser. Seeing nothing from the room, I think we're done. Thank you, Mark.

(Applause.)

All right. Thank you. Thank you. Next up, Christian Johnson, ARIN's chief information security officer, to give us an Information Security Update.

Information Security Update

Christian Johnson: Good morning. My name is Christian Johnson. I'm the chief information officer here at ARIN. I'm going to be giving the Information Security Update.

I'm going to move through the first part of this brief at a fair clip. Obviously if there are any questions we'll field them. There's a particular slide towards the end I want to spend a little time on, talk through a couple of points that -- and you'll hear it as I

go through it -- definitely tying in with a number of things that Mark brought up that were brought up yesterday during the finance discussion.

So this is the overview. I think I've used this several times now, but I do like to touch on this again because it really does sort of encapsulate the methodology that we approach things here at ARIN. It's a focus on the basics, doing the basics well.

I think in a previous ARIN meeting I actually threw out a statistic or a quote or something from somewhere that the majority of organizations that have problems with security are way out in front of themselves. They're not spending time doing the basics, things that are really less interesting than attending vendor conferences where they're selling the newest AI security technology and things of that nature.

We're spending time doing the basics here at ARIN. I say that not as a pat on my own back. This is actually intended to be a pat on the back of everyone who is sitting on Mark's team in engineering who I'm continually impressed with -- this is my pat on their back -- I'm continually impressed in every meeting and conversation we have that security is a part of those discussions. I'm not bringing up the topics; they're bringing up the topics.

I think that you, as a community, should be aware that, from my perspective, that's pretty impressive. And it's sort of baked in, to use an old security term, it's baked in to the organization. I'm just really impressed with that; I have been in the three years that I've been here, and continue to be.

So we were talking a lot about moving to Kubernetes. We were talking a lot about going into a new data center, moving out of the one that we have on site.

So this speaks to a number of the things, like maintaining an up-to-date security-minded infrastructure, reducing tech debt.

Some of the things that we're also doing that don't get talked about a lot, but they're in the press a lot, is ensuring our vendor or third-party security, the vendors that we use, being very deliberate about considering who we're going to use and continuing to review vendors that we use.

Sensitizing our users, our staff towards policies and training. The stuff that normally is considered very boring, ground-level security stuff is required.

I'm looking at the -- I'm on the wrong slide. There's the slide I'm actually talking to. Thanks, John. John, the only one that mentioned anything. Thank you, John. I'm looking at the slide ahead.

John Sweeting: That's a lot of words for that slide.

Christian Johnson: Fair enough. We've done a lot of work, and we'll talk about it, enhancing our reporting capabilities within the organization. That is primarily focused around email capabilities.

It was something I touched on in the past. I'll have more about that, more of a follow-on to that sort of evidence based on how that's actually improving the organization.

Spend a lot of time going over vulnerabilities, trying to identify and remove threats. And that plays out again when we get to talking about the roadmap items, the long-term planning that Mark was talking about, things of that nature.

And we do. Sort of with all of this, we're conducting lots of recovery and response drills. We do biannual -- sorry, not biannual -- semiannual, so once in the spring and once in the fall, we are conducting continuity recovery and incident response drills. That's with our technical staff, where we're actually going through and responding to incidents and things that they would see happening within the infrastructure.

So a quick review of the compliance initiatives that we're going through. Should have switched these -- PCI should have been first; it would be a little easier to talk to.

PCI, obviously, as a recap, is required based on the fact that we take card payments. The scope of PCI DSS is on ARIN Online, the payment card environment within ARIN Online, and the overall organizational controls that we have for security.

The SOC 2 certification that we do is around specifically the organization, yes, but SOC 2 allows you to be a little more specific as to which services you want to certify, or if you're a commercial organization, which products you might want to certify for market.

In this case, it's RPKI in the organization. Both of those compliance frameworks that the audit periods that we have, the monitoring periods that we have are a 12-month period, and they run from October 1st through the end of month for the following September.

For PCI, last year we had a whole new PCI version that was put in front of us that had a good number of changes to the framework we adjusted earlier on in the year. And there were a number of controls that took place at the beginning of 2025.

We were actually aware of them in 2024 because PCI, if they do anything, they do a great job of outlining as optional controls in a given year things that will become mandatory. So all the stuff that became mandatory as in new controls for 2025 were known about in 2024 and we had already put them in place.

SOC 2, we remain compliant on both. As I said, the scope of SOC 2 is around RPKI. We are working towards ARIN Online being a part of our SOC 2 audit program so that when we do a SOC 2 audit, when we do SOC 2 certification, we will be, in the future, certifying both RPKI and ARIN Online.

I will say briefly that we had, a couple of years back, forecast that we were going to do this a little bit earlier. We had a change in payment-card vendors. That sort of bumped up in our priority list when we needed to implement PCI. And so that sort of wiggled into our priority list.

And with the data center move and the migration to Kubernetes, we really needed to hold on the ARIN Online push into SOC 2 because -- has everyone seen the diagram? Project managers love to talk about this diagram where you have the Venn diagram with the three circles and it's cost and it's personnel and it's time, and you have to have all three to get a project done. If you have a lot of one, you can sort of skimp on others to get something done.

In this case, the dollars and the people and the time to get both of those projects done -- the migration to Kubernetes and preparing the infrastructure for SOC 2 -- it was all the same people, all the same money and all the same time. And there was no realistic way to try and do those in parallel.

The great thing that I will say -- and, again, this is another kudos to the engineering team -- is that as they're doing this -- and I have conversations with them about the migration to Kubernetes and about the data center that's being stood up, being worked -- they're having conversations with me around security. And they are building into that migration the requirements that we need for SOC 2.

It's not going to be as when I came on board in 2021 and we had this really initial lift that we had to get going and we had to build some inertia on SOC 2 because we weren't having those conversations previously to an extent. Not to say there weren't security conversations, but the compliance and the SOC 2 framework conversations weren't taking place at the level that we are required to do when you're sort of in the middle of it year in, year out.

Kudos to the engineering team for doing those things quite proactively and bringing me the updates instead of me having to ask for them on a regular basis.

So here's some general stuff. This may seem a little bit boring, and I apologize. The updated security training. This is almost an identical bullet from October, I think, with one exception, and that is the last bullet I changed 2024 to 2025. The reason it's even in here is because last year we got a new learning-management system, as I briefed last year.

And what we did is we moved the training from our old LMS over to the new LMS to sort of save time, save energy as we were trying to move things forward in that direction.

This year, we're working with our training team, and they're completely revising the training content itself in the new LMS. So we're going through a cycle right now where we're trying to improve the security training for our staff and move it forward.

With the expanded email reporting, this was also something I reported last year. And the reason it's on here is because of the last bullet. So now everybody is going to go straight to the last bullet and read that while I'm trying to explain the backstory.

We previously only had an automated reporting button in our email for Windows systems. And what we did was we had to wait. We were waiting on the vendor to change the way that they had their button working for SaaS systems.

And when that was finally made available and we completed the migration to Exchange Online -- I will not refer to it as EOL again because EOL means something different to different people, but Exchange Online -- we immediately fielded that and got the button pushed out to all of the users.

And again the reason is, the last bullet that is included, what we saw prior to that, where we had only Windows users and we had people manually reporting suspicious emails that were coming into the organization, we were hitting a quarter of -- we were getting about 25 percent of the organization was reporting that they had seen a suspicious email.

I knew there was going to be an increase. I will say, having been in an organization that used to do this regularly in standing up programs for clients and corporations, hundreds of thousands of employees, large, that's a fantastic number to have 25 percent of your organization reporting that they saw a suspicious email come in.

We're at 50 percent now, where the button just makes it too easy for people to report, and they're doing it consistently. This isn't just a one-off. This is six months of consistent 50 percent, or just slightly less than 50 percent, reporting. So that's a kudos that goes out to all of our staff and the people who are receiving those and reporting back that they're getting those.

Why is that important big picture? Because it develops a reflex. There's sort of an analogy that I've used in different areas where you can learn how to throw a baseball by going on YouTube and watching lots of videos about how to throw a baseball.

But I guarantee, if you spend a month having somebody watch YouTube videos and you put a baseball in their hand, it's going to look awkward. They're probably not going to be able to throw as well as watching the video.

So you can take somebody and you can do the fundamental security training that we're talking about, but until you put the button in the ribbon and you ask people to report when they're getting the phishing emails, it's not going to work out as smoothly as you would hope that it would. And it's only through the monthly exercises that we continue to run and making reporting yet easier for our staff that we're starting to see some of the fruits of that effort.

So that's some of the drills, some of the exercises we do, or the phishing exercises that run regularly. We've also expanded our internal technical drills and training. That's what I was talking about earlier, running those twice a year.

One focused on cyber incident response. So cyberattacks, effectively, of varying natures. And we're able to get a couple in each session with the staff that are participating in that.

And then at the end of the year we're focusing more on disaster recovery and business continuity-type exercises and drills.

So this is what I wanted to touch on. I want to say that it was ARIN 52, it may have been ARIN 53, someone came to the microphone and they said, basically, ARIN should consider removing outdated services for the sake of cybersecurity.

It's a great point. We actually had additional conversation around that earlier. I think it was the end of January. I'll be corrected if I'm wrong, I know. At the end of January, I believe it was, we removed a bunch of outdated, cryptographic ciphers that were on our public pages, our public resources.

Then, as was discussed at the end of March, FTP was taken down. Between the two of those, we actually were able to get rid of a number of security vulnerabilities that were being accepted up to that point because it was important to keep those services available.

And so that was of great benefit to the organization, security-wise, if nothing else.

I see the results every quarter when I run the external security scans for PCI. We see it every month when we're running the internal scans for PCI and SOC 2. And we've seen a number of those vulnerabilities just evaporate, disappear because of those being removed.

Again, the migration to Kubernetes and the subsequent data center move are also going to play into that into a very large extent because, as a part of that, we are updating systems and even some of our processes to facilitate the new environment.

It's going to be of great benefit. I'm a great beneficiary of all the work that Mark is doing on the engineering side. Security is truly going to benefit from that.

So I always like to put this out, the information security webpage at ARIN.net. We have our SOC 3 report that is effectively the publicly available summary SOC 2 report, their numbering. There's no one in the room from PCI, right? Their numbering system is whacky.

The SOC 1 report has to do with financials, SOC 2 is security, and SOC 3 is a summary security report. Whoever is doing that, I think, got laid off at some point.

That being said, our SOC 3 report, again, the summary security report is available. It's hanging off the website. We can do that. That's what the SOC 3 report was created for.

So you can go in or your organization can go in, and you can download that report, sort of self-service, if you will, that information, because when I said that we are going through and looking at our vendors, our third-party relationships, and we're doing assessments and we're trying to be deliberate about who we are developing those vendor-client relationships with to support the infrastructure, systems, et cetera, obviously all of our customers have, to varying extents have, responsibilities around that as well.

And so that's one of the reasons that we put that out there. We regularly get information requests -- and I've put this out before, too, as a nice little foot

stomper -- is that we get those requests saying they can't renew our contract with ARIN until you provide us a bunch of security information or you complete a questionnaire.

What we're finding in a lot of instances is that you have dedicated security staff -- this happens a lot in the larger organizations -- you have dedicated security staff who now that security team actually has a vendor security team within it, right? So they are dedicated to doing this mission and reaching out to their critical vendors.

And ARIN very frequently is considered a critical vendor, if you have an Internet presence of any type. And they're reaching out to us without your knowledge, without your visibility as the POC on an account.

And so what we're trying to do is we're trying to point them to the information security page so that they can self-service that information. The SOC 3 report is available there. In many cases that is sufficient.

In some cases we're needing to loop the POC into the conversations so that they're aware that maybe there is a team that doesn't find that information sufficient and they're still asking for more information from us. And usually that is able to resolve most everything.

And in some cases it's not, and we're having to have more deliberate conversations with people around what they actually need.

This is folks doing their job. I can respect and appreciate that. Everybody's trying to accomplish their mission and do what they're assigned to do. We want to facilitate that to the greatest extent that we can.

We do have a handful of customers, though. And if we were expected to spend hours for each customer filling out a tailored and custom questionnaire, we would probably have to change our mission statement or hire a whole bunch more people. Frankly, I don't want to be in that business.

And with that, I will open it up for questions and comments. That's all I have at this time.

Hollis Kara: Thank you, Christian. If anybody has a question or comment, please approach the microphone or begin typing.

Hey, it's Kevin. Hi, Kevin.

Kevin Blumberg: Kevin Blumberg, The Wire. Thank you for deprecating crap.

(Laughter.)

While it may be of use, the reality is, especially for ARIN's mission, you have to be at your A game, not dealing with applications, protocols, et cetera, that should have been retired out years ago. So, thank you.

One thing that is important is consistency. Keep doing this. Keep pushing the envelope. Keep letting people know: In three months we're turning this off; in three months, we're upgrading this; in three months, in three months, in three months. Keep doing that.

Because doing it one-off, people think it's a one-off. I really believe ARIN should always be at its A game when it comes to security. And unfortunately that means you can't service everybody. So that's the first thing.

And consistency is great. Our customers, from my own company, value -- rather knowing that we're doing this consistently.

The second thing is, in relation to the SOC compliance and the vendor requests, we're seeing a huge uptick ourselves in those types of things.

Bill the living crap out of it for them. I'm sorry, you've got your SOC 3. If they need more, you've got additional plans. I don't need to pay as a member individually for a limited number of companies that are unwilling to accept the work that you have done.

So if they need more than that SOC 3 report, move them to a value-added plan that gives them that one-on-one attention and "like" that they need. But don't make all of us pay for somebody who is asking for that. Thank you.

Christian Johnson: Excellent points. Thank you. Please.

John Sweeting: John Sweeting, chief experience officer. Kevin, I just want you to know that Joe Westover and his team work very closely with Christian to try to push these people away. And one of the ways we do that, as Christian noted, we tell them, look, we need to get an Ask ARIN ticket from your contact at ARIN to ask us to do this and make sure they know you're threatening to return their resources to us if we don't do it.

And one of the other things that Joe does tell them is, hey, if you want this special kind of service, you can pony up $5,000 and be a PSP.

Hollis Kara: We've got one more question from the floor.

Roman Tatarnikov: Roman Tatarnikov, with IntLos consulting company. I wanted to follow up, it's less of a question but more of a comment, on Kevin's comment for Mark's presentation. And right now, with Christian here talking security, I figured it would be the best place.

So when Kevin mentioned that it's best to move to the cloud and to make sure that the data center doesn't leak anymore and so on, I just wanted to remind that maybe it's best not to use just a single cloud and only the cloud. But use a multi-cloud solution and use some on-prem equipment as well in the data centers, just for the sake of information security as in BCP, business continuity, and so on. I know it's going to cost more, but it's critical for what ARIN does.

John Sweeting: John Sweeting. I have to clarify. I fell into the trap of talking ARIN-speak. PSP is the ARIN Premier Support Plan. It's a $5,000 annual fee that you get a lot of special attention as well as a personal analyst, white glove, tickets go to the front. And anything else that you might need is like a security form filled out. Thank you.

Hollis Kara: Thanks, John.

Do we have anything online? Nothing online. One more from the floor, if we could.

Atefah Mohseni: Atefah Mohseni, ARIN Fellow. Just a general comment. I think in information security, generally the initiative is already active. So I wonder if you have any discussions or initiatives that are proactively preparing for more advanced cyber threats with the recent advances in AI.

Christian Johnson: So AI is on everyone's lips, as was machine learning, as was a number of things that came in prior to that. There's certainly some unique attributes to our current AI environment that did not exist previously.

There's a lot of plug and play that's going on when we start talking about advanced cybersecurity or advanced cyber threats that we're seeing discussed within the environment, within the community.

It's not so much the advanced threats that we're seeing; it's the facilitation of fundamental and basic threat vectors that are being exploited through the use of AI. So the development of tools, the collection of tools and things of that nature.

Or a really great one that I've seen people talk about a good bit is the use of AI chatbot, for example, doing SMS attacks, using a chatbot with AI to be able to get information into social engineers so that you don't have to do it. You can actually have a chatbot bot who's attacking a thousand targets at one time, for example.

We're monitoring a lot of things that are going on as these threats mature. This isn't unique just to AI. We're looking at a number of threats that are doing this. The tough thing about cybersecurity -- in some cases, computer and technology and networking services in general -- is we take advantage of new advances in technology as they come up, and we apply them in very unique and very original ways.

So there are a lot of what you would imagine to be pretty straightforward and expected vectors that are being taken advantage of with AI, for example.

And what is most interesting -- there are a lot of vendors who already have product suites that counter all of these known threats or anticipated threats. What's most interesting to me are the vectors that are coming to life that are not what all of the security experts had forums about six months ago to inform the community to be on the lookout for. It's the new stuff. That's what I find most interesting.

And so, to your original question, we are looking at those. We're trying to track those. They happen at such a fast rate that it's almost impossible to keep track of them. Some of them will come to life, and they will be the next hot thing; in 10 years, expect this to be the only way people do things, and within six months they will have disappeared.

There is a grain of salt that you have to keep an eye on on with some of the things.

We're very conservative within the organization, technology-wise, with implementing fad-type solutions and to spend a lot of money on solutions that don't have a solid basis for providing value to the organization. I think that's being a responsible steward of the community's trust in us and funds. We'll continue to do so in the future.

But to your question, we do look at those. I take time out of every single week to try and look at those type of things and to see where we are, sort of do a check-in with some of those things to see whether or not they're advancing or declining.

Hope that answered your question. Anything else?

Hollis Kara: I think that wraps us up. Thank you, Christian.

(Applause.)

All right, don't worry, Brad, you'll still get your 15 minutes.

Brad Gorman, come on down. We have our director of customer technical services, Mr. Gorman, giving us an update on routing security.

ROUTING SECURITY UPDATE.

Brad Gorman: I guess I'll close out the trifecta of talking about security here this morning. As the role with the routing security product owner here inside of ARIN, it's definitely a subject that is very important to me.

So we're going to get started talking about routing security. I'm going to look a little bit at the global footprint and current state of RPKI, give some more detailed information in ARIN with how RPKI's working within our organizations and our community.

I'm going to talk about a few of the new features we've released, things upcoming. I'll also provide a short update on the NRO RPKI Working Group that we established to put a common or similar RPKI face to the entire RIR community.

So let's take a look at the numbers as far as where they're growing globally. So over the last five years, there's been a large uptake in the use of RPKI and covering resources by creating Route Origin Authorizations or ROAs.

The chart that I've got up on the screen basically support that. But, hey, more and more people from organizations are making the statements. And as you can tell, v4 and v6 are trending in exactly the same direction, which is definitely a good thing to see.

Within the global RPKI community, there are a few things that we have been able to establish as the key factors or some of the factors into this uptake.

Certainly continued outreach and education that provided through the RIRs or through the general community in standards bodies that are bringing the usefulness, that are explaining the usefulness of RPKI and how it works and what needs to be done.

There have been requirements from service providers or connectivity providers that mandate, hey, you need to make these statements before you can finish signing up for service with us.

The question is, is what the community is starting to see, is there a plateau that's coming? And there is some belief that we have hit the low-hanging fruit, but in fact it's the big factors, the largest groups of resource holders.

We know that our job moving forward is going to be more and more detailed and reaching out to the smaller organizations and smaller resource holders to come online and start using RPKI.

So within ARIN, we can see this accelerated growth of organizations that have adopted and taken advantage or starting to take advantage of our RPKI services. A lot of it has been attributed to internally as the efforts that were being made to get organizations to sign agreements, get under the fee cap or the LRSA fee cap that has really boosted the pool of available customers or resource holders to start using RPKI. Again, I spoke about service providers making it a requirement to sign up and create ROAs.

And there has been a lot of work assisting the US government in their plans and requirements to start developing or establishing RPKI platform or deployments and covering their resources using the services.

I just want to review, there are three RPKI services available through ARIN, the hosted RPKI service, which is akin to the easy button. ARIN will serve as the trust anchor --

From the floor: You're one slide behind.

Brad Gorman: Goodness. There we go.

Services provided by ARIN. The hosted RPKI service is a way to get started using RPKI. All of the lift of running a trust anchor, which is a requirement of the RIR, running the certificate authority, maintaining the cryptographic components and running the high availability group repository and publication idc repository. It lessens the requirement on the user. You just need to make statements on the resources you hold.

And there are also tools that ARIN provides to the customers that sign up for hosted RPKI.

The next component or service is delegated RPKI. It's kind of the flipside of the same coin for organizations who want to have cryptographic control, who want to maintain the A repository and keep hold of where their ROAs are created or other components inside the RPKI run.

And it is more resource-intensive in the way that you need to have human resources and technological resources available to run a delegated service. But one of the third pieces that ARIN does offer is a repository publication service.

So for organizations that choose to keep that control of the cryptographic components and hold in that need may be an internal requirement. But they don't want to run that repository service with a high uptime requirement. We have a repository publication service that's available to those customers, and they can offload that hard piece on to them.

So inside of ARIN, this is another way of showing that hosted RPKI services are the service of choice by a very wide margin. Greater than 90 percent of customers use hosted RPKI services. And, in fact, that is mirrored across the entire RIR ecosystem. Hosted RPKI is by far the first choice. And it's not just small organizations; it's large organizations as well that have chosen to do that.

The small percentage of delegated customers that are online with ARIN using that, more than half of them have chosen to use the repository service.

So for those delegated customers it's a popular thing to select and a benefit that they see coming from ARIN as what we're providing has value add.

Here, I've broken down some of the different entity types and the levels of adoption and coverage for their resources, breaking it down by government, educational resource and otherwise commercial or individual users of or holders of resources.

The numbers are still lower than we all would like to see in the community. Continuing education and then pushing the benefits of RPKI will get some of these numbers up.

One of the things you might notice is, as far as coverage of resources with ROAs, by far the largest group is the commercial groups. We attribute that to the commercial use and commercial groups that have RPKI enabled and using them are the ones with the largest pools of addresses. So that's what looks like and comes into what that large percentage represents based, or as compared to the other entity types.

I wanted to put this chart up to show that, the ARIN community isn't just North America. It is the Caribbean community that we support as well. And at the bottom of the list, very nearly at the bottom of the list, the percentage of organizations inside of those large pieces of the ARIN community, the adoption rate is pretty low. Makes me sad. That's what I like to see, the numbers to be higher than that.

Certainly within Canada and the United States, there are larger numbers of organizations. There's much larger blocks of resources that are assigned.

But the only way that the real benefits out of using any routing security product or RPKI, it is you have to start using and sign up to cover your resources and make the feature more of a benefit and more available and more useful to the entire global community.

Here it's just a representation of the number of resources within the ARIN pool. We have about 1.67, 1.66 billion IP addresses in the registry covered by ARIN.

A fair 60-plus percentage of them, 65 percent of them, are under an eligible to use RPKI services. And amongst those there are still 750-plus number of resources, IP resources identified that are covered by ROAs inside of the global ecosystem of RPKI.

So the numbers are good and the numbers are increasing. But the push and the desire is always to bring these numbers further up.

Like the other chart, but a little bit better in perspective, the number of resources that are in fact covered by the countries and territories within the ARIN region, the US and Canada are kind of in the middle.

But as I said before, the number of resources in our two countries far outpace what is in other places within our region. So 60 percent, 62 percent coverage is good, but it's not great. So again, I'm promoting, recommend, come to me and I will educate or give you a cool new pen. Please, sign up and start using RPKI services.

Some of the new releases and the developments that are on page, on line, we are about to deploy a ROA edit feature. Prior to now, the only way that a resource holder could make changes to a ROA that had already been created was to delete it and recreate it.

There is always a chance of something undesirable happening when you do that. So with a ROA edit feature, as we're deploying it, the customer will be able to go in and modify the contents, the prefixes that are inside the ROA so that there is much less of a potential impact and almost reduce the possibility of an unintentional, undesirable effect by deleting a ROA.

Mark alluded to it, and we at ARIN and within the greater RIR community, we're starting to look at what the next object in the RPKI and the next promising knob that we'll have. It's the Autonomous System Provider Authorization, or ASPA.

The ASPA, within the standards community in the IETF, ASPA is not yet standardized, but there are three drafts that are well along the way. And the component and the portion that the RIRs are responsible for is pretty baked, or we're not expecting any changes to come.

What we've done is we're enabling inside of our test environment in OTE, the ability for our customers to come in and use our UI in ARIN Online or the API to get your practice with, understand how your tools are going to work, start building your tools, so that when it does become a standard, you'll be ready to go and start taking advantage of what an ASPA does and can do in concert with the ROA and using RPKI.

Another feature that is on our roadmap that we will be deploying as we move through our developmental [rollout] and the prioritization of features and tools, is we're going to have an option for users who have resources that have either been reallocated or reassigned from the direct resource holder and allow them to make RPKI decisions for the resources.

Currently only direct resource holders can do such a thing. There have been many asks, suggestions from our community or direct interface with me or others inside the wider networking community that this was something that was wanted and needed, and we're going to be offering this in the future.

I had mentioned there was a group inside the NRO, an RPKI Working Group. I'll do my best to go through what is a simple presentation for our project manager, product manager within that group. She has given it many times. This is a first for me, so please forgive.

In this community, in 2024, we had a very big push out to the community to say, hey, what do you need from the RIRs in general? How can we make it easier for you to use RPKI? How can we make it a more common experience with a multinational organization that's using RPKI?

So we did this questionnaire. We conducted individual interviews. We went through and we started talking about how could documentation be in play and make this truly become a reality and work towards this, bringing together a common feel for customers who have multiple resources, multiple RIRs. Asked for better reporting and monitoring and measurement uptake and usage.

And another thing would be keeping -- we are well involved and up to date and constantly interacting with the technical community to make sure that as RPKI

continues being, with new standards being turned up and authoring new drafts that are coming out to make us be successful and be able to offer those products to the global community.

We took all that feedback, and for this year our goals are continuing progressing towards having a overall transparent picture that we're presenting to the global community from the NRO -- not only the ability to monitor and see, but the robustness in our data, making sure that we are maintaining and upkeeping an infrastructure that will be stable and accessible and useful for anyone who wants to use these products.

We talked about the consistency of the experience and coming out and giving regular communications in different regions around the world about the work and the activity that we're doing.

To be successful, not only are we working to pull on the information that we received so far last year and as we plan our development moving forward, we still need to hear from you.

As things evolve and are modified, we want to make sure that we continue to hear, continue to listen. And the only way we do that is you need to reach out to us. And there is a -- the funnel with which that comes into us is the email alias, the email box down at the bottom.

Please reach out. We're listening and we're working to deliver what you want to see out of the collaboration with all the RIRs with this working group. So take it, please, move forward and do that work. We're listening.

And then self-promotion here. Within ARIN and the features that you'd like to have, the easiest way to get a hold of me and the team, when I'm out, there are people back at home base that are listening to our email box. So take advantage of this email if you have suggestions or questions or gripes, whatever you want, use this and communicate that with us. And we will certainly reach back out to you and listen and try to accommodate. And your input drives development inside of ARIN. Please take advantage of that.

Hollis Kara: Thank you, Brad. Queues for ther microphone are open. So please come on down if you have a question for Brad. Same online, begin typing. Do we have a virtual? Go ahead, Bev.

Beverly Hicks: Altie Jackson, ARIN Fellow: "Brad, we in Jamaica we need the RPKI training you promised. We'll get those numbers up to 100 percent."

Brad Gorman: Altie is part of the Caribbean community. The outreach organization inside the Caribbean is called CaribNOG. They hold their own semi-annual meetings to attract that customer base and come in and provide knowledge and assistance.

Yes, Altie and I had spoken in the past. And we're working on that. Thanks Altie. Chris.

Chris Woodfield. Chris Woodfield, ARIN AC. I'm curious what techniques, tools are available to test the extent of RPKI validation. Testing the propagation of the (indiscernible) routes needs to be a technique the (indiscernible). Wondering if there's any other tools available to do that.

Beverly Hicks: Can you repeat the question so the online people can hear.

Brad Gorman: Yes, Chris Woodfield asked the question, what early other monitoring or performance calculations of the RPKI service and how any resource holders' presence looks like to the outside world.

Within ARIN, another development effort that we're looking at is providing current state of what a resource holder's announcements and how their ROAs are impacting or otherwise presenting that RPKI validity data which you're trying to get to.

Really in the community, there are a vast number of third-party RPKI tools that will answer and provide and generate more questions in your mind and things you want to look for in the future about how your presence and your footprint looks like and how it is presented and understood by people in the outside world, in the Internet.

Matthew Wilder: Matthew Wilder, Telus. My question is what is your strategy or what strategies do you have planned to reach the 85 percent or so Orgs that don't yet have RPKI or are using those services yet with ARIN? Is it going to be putting it front and center in ARIN Online so that when you log in it's, like, request RPKI and get all set up? What have you got going on?

Brad Gorman: That's actually a great suggestion. It's something that when you do put it in the face of anyone who comes in, either they know what is going on and it's, like, a harsh reminder, hey, I need to go do this, or will prompt that initial, hey, what does this mean? Why is it there?

Make that as a suggestion using our suggestions portal or certainly we're in the room and I'm hearing that right now. We'll definitely take that into consideration. But I like it.

Kevin Blumberg: Kevin Blumberg, Toronto Internet Exchange. We've been doing a lot of work in this area, looking at RPKI valids from our own customers, peers. It's important.

We want to get to the point of, if an Internet exchange is giving a route to others, we want to make sure it's valid. So this is a keen interest to us as a shared fabric to be able to do that.

We have minor insights that may be helpful. The first is, it's not quantity that matters, it's quality. What we're seeing is a high uptick of low-quality, high-number. So a whole bunch of residential subscribers, 10 million residential subscribers will be signed. All of the businesses that have actual infrastructure and that you're actually hitting won't be.

So it's definitely a quality-versus-quantity issue. And you are right. We have now hit the peak. And it is now a much harder game to get the next group of people on Board. And there's only one way to do it: Opt out not opt in.

I'm sorry, we need to take it to the next level, give notice and opt everybody into RPKI that doesn't have it, that we've got a legitimate, easy-to-do record.

And if they want to opt out of it, that's great. But on a certain date you've got an Origin AS. You know what it is. You can see that the update is live. It's not going to have an impact to them. Go.

We're never going to get to 100 percent. We're never going to get to 95 percent if we are chasing after unknown POC entries from 15 years ago.

Brad Gorman: So you had two questions, comments in there. I'll try to address them both.

Absolutely, the accuracy of information that a resource holder makes when they create their ROA is key. It's just like any other thing, that the information that you present on your resources to the outside world, that's your information, and you need to be aware of what you're saying and what the potential impact is.

Setting up RPKI is easy, but there are plenty of best practices and lessons learned that are out there that assist people who are doing this for the first time or even as

moving along that you need to be aware of. And on the ARIN web pages there is in the RPKI FAQ a list of the current IETF best practices and other lessons learned that people can review and hopefully will find helpful.

To the second part off that is a suggestion. Within the global RPKI community, it is opt in. I mean, there's no way today that we can come and mandate our member organization to do something like that. It has to come from you. So go ahead and do that and we can talk about it further.

Hollis Kara: One more from the floor, then one virtual, then we'll move on to our next presentation.

Alison Wood: Thank you. Alison Wood, state of Oregon, huge RPKI advocate. In response to Chris' question, Cisco Systems acquired a tool called ThousandEyes. ThousandEyes is a huge monitoring tool, but they use RPKI validation. They do show it in the routes. It's fantastic, and I would be happy to demo it for you or for anyone else who would like to see it.

Brad Gorman: That's great. Thank you, Alison.

Hollis Kara: We will go to the virtual. And I'm sorry, I can't take any more from the floor right now. We'll come back to it. Save it for Open Mic this afternoon, that would be great. Let's take our virtual attendees.

Beverly Hicks: Richard Desjardine from Hay Communications: "Discovering that hosted RPKI was included in our subscription during NANOG last fall was a game changer in getting our organization using ROAs and RPKI. Please continue to communicate that included service."

Want more?

Hollis Kara: Please just keep going.

Beverly Hicks: Matthew Cowen, unaffiliated: "Are the figures provided only for ARIN resources? I suspect the French West Indies' figures would be different given that they use a lot of RIPE resources through telcos like Orange and Free.

Brad Gorman: In the Caribbean, there is a split coverage area between LACNIC and ARIN. But, yes, there are territories that have more traditional ties back to Europe.

And in those cases, those resources have to be, statements have to be made about them in the RIPE interface rather than the ARIN interface. Yes, the numbers I did present are ARIN's numbers, resources within our organization.

Beverly Hicks: The last question from Brandon Knutson, VPS: "Do you support FCC rulemaking BGP security initiative to push the requirement to enforce Internet service providers to enforce BGP with RPKI? This may help get to 100 percent within the US."

Brad Gorman: With regard to decisions being made in government agencies or otherwise departments, you really have to defer to what they're doing in the RPKI. ARIN doesn't have any official stance on what's going on.

Hollis Kara: Thank you, Brad.

Brad Gorman: If anyone has additional questions, stop me in the hall.

Hollis Kara: He's here all week.

(Applause.)

Before we move ahead I want to point out a slight change in the batting order. We'll go ahead and bring Mark up. Where did Mark go? There he is. We'll fit in this next presentation before the break on ARIN's RPKI trust anchor.

We are going to slot the transfer update for later this afternoon after the policy blocks and some of the other things that are on the agenda because we have folks coming in online to participate in those as virtual presenters. So we need to stay on schedule for that.

Robert Seastrom: I have a question for Hollis before Mark goes on. Or just an observation.

Rob Seastrom, ARIN Board of Trustees, speaking on my own behalf. We have been really great and on time and short on awkward pauses, which means that we are below quota for bad jokes.

So I have a question for you. Have you ever tried eating a clock?

Hollis Kara: No, R.S., I have not.

Robert Seastrom: It's really time-consuming especially if you go for seconds.

(Laughter.)

(Applause.)

Hollis Kara: Thank you for that intervention. Moving right ahead, Mark, over to you.

Mark Kosters: Actually, I was going to do a grandpa joke, because I'm actually a grandpa now. But I decided I'm not going to do that after -- so let's go ahead and move on.

But I do have a question for the audience because this next talk is also going to be on RPKI.

Who's eyes are truly glazing over? It's okay. You can raise your hand. I know there's more than that.

So what I'm going to do, I'm going to go through this. And for those people who are kind of eyes glazed over on RPKI, I'd like you to pay attention to the first couple of slides -- you might learn something about RPKI -- and the last three. Okay, it's kind of like the Cliff Notes. All right.

For the rest of us, we'll just go through it. Much of it, hopefully it's a learning opportunity. And for our transcriptionist out there, I apologize in advance because I'm going to be using lots of acronyms and they're not ARIN acronyms as well.

Okay. The ecosystem and trust anchors, one of the things I want you all to hear is really contains two things. Repositories. Those repositories are actually generated from data that you give us and that we disseminate to the community.

This in turn is given to validators that validate the information and feed it to the routers. Cool? Are we good? All right.

Next one. We're going to focus in on validators, because there's a key part here. And that is that validators need to bootstrap their information. It's much like your web browsers. When you go to a site that starts with https, it has a certificate store in there on the number of CAs that actually come with your web browser.

And it has to be one of those CAs or, unless you've actually configured some other ones as well, that is how it validates that site to make sure that you're going to the right location.

Similar sort of things go with RPKI. But it actually goes through a little bit more advanced topics that we'll talk about soon.

But the big thing here is that the RPKI system is bootstrapped off a thing called a trust anchor. And this trust anchor is configured on each validator. So it's very important to know that.

So what are we going to talk about? We'll have a brief tutorial on RPKI certificates; ARIN's structure and how we sell it, how we put this together; I'm going to talk about why is this important, why is a trust anchor important; and then designing and actually exercising the signing process because we go through a lot of due diligence to ensure that this information stays secure.

Okay. Brief tutorial. So unlike the certificates that you get through your web browser, they're basically at a single level. Resource certificates, however, that are used in RPKI, actually follows a tree. You have certificates at each level where you go -- that these certificates match the allocations. And that's how it's designed.

For example, you have an issuer from ARIN that says this ISP has this resource. That resource is then given to another ISP or an end user site somehow. It's reassigned to someone else.

And that information is actually transferred -- is actually used by the validator to figure out where to go, where to get the information, to actually do the validation. And it's all done via certificates.

And you can actually go one level down where it actually finds the ROA, basically the big component here that's used to actually do the route validation. Okay? So all you can see that you have all this stuff -- whoops -- you can see that this path-finding is very important in RPKI-land.

So our structure. And I apologize in advance for this, and this is different nomenclature that what we use within ARIN, but we're trying to use the same nomenclature between the regional registries, and this is the documentation that's publicly available that you can see.

So you have an offline trust anchor, I'll talk more about that soon, that signs basically an online operational certificate, which in turn is used for organizational certificates, which basically are resource certificates that you use to sign over your ROAs.

The offline certificate is used basically to sign the online certificate. The servers are not on the network -- never have been, never will be. The operational, online operational certificate is, of course, online. And it's the workhorse that's used to sign certificates or resources for each of you who participate in RPKI.

And the organizational certificate signs over the ROAs and ASPA objects or whatever else as we go forward. All these things are signed by either online or offline high security modules.

Offline trust anchor details. So the offline box, boxes, actually, are not on the network. Their keys are stored on an HSM. And actually when we do a key-signing ceremony, we actually physically transfer the signing material from our offline to our online box. When we set these things up, we actually reboot the OS. We reimage the offline box to start this whole process going forward as we bootstrap it.

The keys are stored on HSMs, which is why we have them. And that's how we go ahead and do that.

Offline trust anchor, their keys are protected. Offline operational certificate servers and their keys are protected by not being -- it's not on the network, as I said. It also requires third-party access, has a multi-factor safe. Basically these safes have to be opened by, what we call keyholders. I'll talk about that a little bit more in the future. But each key holder has one part of opening the safe.

The monitorings at each site are -- actually, there's TV cameras watching over them. We log the access entry both at our primary and backup sites. And these safeties are huge. They have a little bit of material in them, but they're really big. I certainly can't lift it.

In fact at our facility in Chantilly, we were worried that the elevators were not going to be able to have enough lift capacity to bring these things up to our offices.

And we were worried a little bit about whether or not the floor could actually support the load. We found out it could. So it's good. They're bolted to the floor. They're in our office space in Chantilly, and also our data center that is in Ashburn.

And when we go to our new data center, that safe will be transported, hopefully with something like my dually pickup truck, to its new location.

Operational online certificate. The servers are on the network. The keys are safeguarded by the HSMs. And there are certificate servers at two sites. There are actually redundant servers at both sites.

The organizational certificate. It is also called a resource cert. In fact, that's what we use internally. It signs all the ROAs, all the ASPAs. And also there's these other things that are used internally or actually by the validators called Certification Revocation Lists and manifests to make sure that all the information that's in the if

repository is all there. None of it is actually missing. That's what the manifest does. And signs over delegated certificates. And there's, of course, two modes that Brad talked about, hosted and delegating.

So why is all this important? RPKI is a system built on trust. You trust us to safeguard this information. It's also hierarchical. I demonstrated that by showing a path validation that's used within RPKI.

ARIN is one of five regional registries that has a trust anchor at the very top of the tree. So all five of us have the same sort of responsibility making sure that these things are secure.

If there was a compromise, hijacks of existing space could be done. Hijacks outside of ARIN's region actually could be put in our trust anchor. And if this compromise does happen, you can see it would create all kinds of havoc and it would cause people to go back to their validators, remember that thing on the second slide, I said is manually configured on these validators, people would have to make changes to try to deal with this. This is something we don't want to do.

We want to make sure that this information remains secure. So what do we do? We didn't want to reinvent the wheel. The DNS root is very similar to the RPKI trust anchor. ICANN has a very well-documented process in how they do this with root signing key and DNS, which is very analogous to what we do in RPKI-land.

In fact, I know there's a couple of key signers here that deal with this information with ICANN.

We witnessed this. I have to tell you, it's very boring. It's a very long, dry process. It follows a script, and we actually use the basis of that script for our own system.

And much like ICANN, we store things on our HSM. We use a different kind of HSM than ICANN. They actually take their HSM, which is a physical box, and put it in a safe on site, has a battery that most of the time works. I know that there were problems with one a long time ago. Our HSMs are actually physically in boxes.

Signing Ceremony Overview. The offline operational certificate has a six-month operational lifespan. It's actually eight months. The online operational certificate also has a six-month lifespan that we go ahead and make sure it's good. Both certificates are signed by the offline operational key and transferred, as I said before, from the offline to the online by hand.

So what do we have to do to access this keying material? You have two key holders. The key holders are not from engineering. They are not people -- they're people, well-known trusted people within the organization but they're not engineering people. It has an operations person who gains access to the secure room. That operations person also has root on both the HSMs. And we also have a witness and a master of ceremony. So one who actually reads the script and makes sure and watches over the operational person making sure that he's actually following the commands that are in the script and there's a deviance on that. We actually write that down so we actually make -- we actually record that, actually put that in a separate safe.

As I said, each step is explicitly laid out. Every command is done to a T. There's no variance. As I said before, if there is, we go ahead and document that.

Each step of the process is initialled by the MC, and if there's a deviation, as I mentioned, it actually requires documentation and it's stored in a safe that's accessed by the witness and master of ceremony.

Accessing the safe: We actually have keyholders designated within ARIN from various other departments, and they have access to unlock the keyed material that's held in the safe. It's a multi-factor safe, as I mentioned before. It has two separate locks, two different combos, and each of them have to unlock their portion of the combo to access the keying material.

And the witness who has a very important role ensures that each keyholder, when they get that keying material from the safe, they actually keep it in their hand. It doesn't leave them, except when it goes into the machine.

I missed something. I think that was it. I actually made it in three minutes and 17 seconds. So any questions about any of this?

Hollis Kara: Happy to take a couple of quick questions. Also going to note that folks are absolutely able to chat with Mark on the break if you have questions from the room or if there's some online we don't have time to get to, go ahead and submit those we'll get those offline.

Matthew, go ahead.

Matthew Wilder: Could you go back a few slides to the trust anchor slide?

Mark Kosters: Which one?

Matthew Wilder: The one where you're talking about how heavy it is.

Mark Kosters: Just tell me when.

Matthew Wilder: Go forward. I think it was forward. It's not really important which slide. The important thing is, this sounds like a very heavy anchor.

Mark Kosters: It's a heavy anchor. It requires a lot of security.

Hollis Kara: I gotcha, Matthew. That was a golf clap joke, I'm sorry, but I appreciate the effort.

Mark Kosters: Thank you all very much for your attention and hopefully it made sense to some of you. I'm hoping it makes sense to most of you. If not, I'm sorry.

Hollis Kara: Mark, it sounds like a blog. Thank you.

(Applause.)

I appreciate everyone's forbearance with our little delay in the schedule. I am going to dismiss folks to break. I will note that we do need to come back promptly at 11. We do have a virtual presenter who is going to be joining us online and I want to be respectful of that.

So I do invite everybody to go ahead and head out to the break. Please rejoin us at 11. Folks online, we will be back at 11. Go get some caffeine, grab a snack, and we'll be back in just a bit to start off with our grant presentations.

(Break taken.)

Hollis Kara: Thanks, everyone, for coming back from the break. I'd like to welcome Amanda Gauldin, Project Manager, to give an overview what we've been doing in the outreach space, our Fellowship Program and introduce our grant reports.

OUTREACH OVERVIEW, FELLOWSHIP UPDATE, AND GRANT REPORTS

Amanda Gauldin: Hi, everyone. My name is Amanda Gauldin. As a project manager at ARIN, I'm happy to give you an update related to outreach, the Fellowship Program and the Community Grant Program.

So you'll hear a more extensive update on our outreach strategy and priorities for ARIN as an organization later this afternoon. So this slide just highlights our direct customer outreach for our January through July calendar.

These are various technical conferences where we have or will attend, operate an ARIN customer service desk, answer attendee questions and/or present on popular topics such as network autonomy, planning your IPv6 network, or protecting your routes with RPKI.

We love to be out in the community interacting directly problem solving and supporting ARIN.

The rest of the year promises to be just as busy, but we do love to hear of new opportunities and so if you have a question or comment related to an event you're involved in, let's chat and hear more about it.

And moving on, you've heard, seen or met a number of Fellows already, and if you weren't aware, ARIN's Fellowship Program launched in 2009 and more than 250 individuals have participated since then, with quite a bit of program evolution through the years.

One of my favorite things is to see where and what the Fellows have been up to since they participated. So here's a fun at-a-glance look at that. It ranges from they're presenting at an ARIN meeting helping to support us with outreach events, to writing content for the ARIN blog, volunteering for committees, and even running for the ARIN Advisory Council, NRO NC or Board of Trustees.

Either way you look at it, we're so pleased to see continued participation in the ARIN community from our Fellows.

So we have a group of 16 Fellows joining ARIN 55 virtually or in person. They've come from all areas of the ARIN region, are at various levels of their career or currently attending universities, but all expressed interest in ARIN, applied to be here and then were selected for the opportunity.

We also have five mentors from the ARIN Advisory Council and the Board of Trustees and they've played an important role in this program as well as the following guest presenters.

So Fellows invest a good bit of time in the program learning about the ARIN Policy Development Process, what to expect at an ARIN meeting, policies on the docket for this meeting, ARIN 55 and more. And then more time with the mentors in small groups for additional Q&A time on the topics that we discussed as that larger group.

And if this sounds of interest to you, our application for the ARIN 56 Fellowship Program will open in July for the meeting that we'll have in October. So when this

meeting concludes, you'll see that information updated on the ARIN website, and we'd love to see your application.

So lastly, I'll mention the ARIN Community Grant Program. The application site is currently open now through the middle of June. And since 2019, ARIN has operated this program funded 23 projects which have supported initiatives that improve the overall Internet industry and user environment.

So we're pleased to bring you two updates from our 2024 grant program recipients next, DNS Research Federation and the Internet Society. They received funding last fall and they're halfway through their projects. At the end of this year we'll have a final report from each of them posted on our blog.

So just a quick encouragement to you all, that if you have or know of a project that aligns with ARIN's mission and strategic goals, to check out the opportunity on our website to read more about the guidelines and the program.

So thank you for your time. Since we are going right into the grant presentations, we have Alex queued up next to speak. I can take questions about outreach, Fellowship Program, grant program, either at Open Mic or find me as you're here at the meeting.

Thank you so much.

(Applause.)

Hollis Kara: Thanks, Amanda, for that quick overview. We want to give our grant reports lots of time.

If we're ready, we can bring Alex Deacon up from the DNS Research Federation to present his report. I see him on screen down here. Waiting for him on screen. There he is. Hello, Alex.

Alex Deacon: I'm here. Can you hear me clear?

Hollis Kara: We can.

Alex Deacon: Should I jump in?

Hollis Kara: We're ready for you, go ahead.

Alex Deacon: Okay. So if you go to the first slide, which I'm not seeing.

Hollis Kara: Give us a moment, Alex, as we get those slides. Where are you coming to us from today?

Alex Deacon: I am in San Francisco. So it's a bit earlier than you.

Hollis Kara: I'm sorry, did you get coffee before this?

Alex Deacon: Of course.

Hollis Kara: Okay. Good.

Beverly Hicks: We have to do a quick pivot. Can we possibly go to the video and ask Alex to hold?

Alex Deacon: That's fine.

Hollis Kara: We're going to switch it around. We're going to cut to video for our other grant presentation and come back to you in just a few minutes.

Alex Deacon: Sounds good.

Hollis Kara: Thank you. Appreciate your patience.

Amreesh Phokeer: Hello, everyone, and welcome to my presentation on exploring potential use cases for the RPKI Signed Checklist, or RSC, under the RFC9323.

This work is supported by the ARIN Community Grant Program. And my name is Amreesh Phokeer, and I specialize in internet measurements and data analysis at the Internet Society. So the Resource Public Key Infrastructure, RPKI, as you know it, is designed to secure routing resources.

One of its most common applications is the Route Origin Authorization, or ROA, which asserts the validity of IP prefixes and the Authorized Orgin Autonomous System Number allowed to do the announcement.

Another application is ASPA, Autonomous System Provider Authorization, which allows AS holders to declare which provider ASN they use, thus reducing the risk for route leaks.

A more recent development in RPKI is the RPKI Signed Checklists, or RSC, which was introduced in 2022 under RFC9323, and this is what we are going to talk about.

RSCs allow resource holders to cryptographically sign a list of arbitrary texts or hash documents using resources they own, providing a new way for third parties to verify resource ownership security.

So in this study, we are currently exploring the potential use cases of RPKI RSCs, as well as the challenges in using and deploying them. Specifically, we aim to

understand where RSCs can provide value, as well as the obstacle preventing their widespread adoption. So let's first have a look at how RSCs work.

So in step number one, RSCs are created and verified for a very simple process. First, the resource holder, for example, an ISP would create a list of files they want to sign.

This file could contain anything. For example, it can contain information about information on IP addresses or ASNs. It can contain information about peering arrangements or agreements, routing security attestations, or any other arbitrary digital object requiring validation.

Then the resource holder computes a cryptographic hash. So for example, they could use SHA-256 for each file. And these hashes along with the file names are packaged into an RSC object. The RSC is then signed using the resource holders RPKI certificate using obviously the private key. Then the RSC object itself needs to be sent to the third party.

Well, the difference with ROAs is that RSCs are not necessarily published in global RPKI repositories. So in step number two, basically, RSCs need to be transferred to the relying parties out of band, basically.

So instead, they can be privately shared with relevant parties, such as cloud providers. So for bring your own IP verification, we will talk about that a little bit more. They can be sent to peering partners for cross-RIR resource validation. They can be sent to customers or vendors for internal verification purposes.

And distribution can happen over multiple channels. For example, there can be APIs in place where the RSC is transferred in an automated process. You can send it over email or over file sharing, secure file sharing, or using physical means such as a USB key.

Then the third party, once it received the RSC and also the original document, can now start the verification process. They would extract the cryptographic hash from the RSC. They would compute the hashes of the actual files that have received. And then they would compare whether the computed hash are those that are appearing in the RSC.

Obviously there must be -- the RSC itself being a cryptographic object must be a valid object by RPKI in RPKI terms. So a validator in place would validate the

authenticity and validity, of course, of the RSC object and make sure, for example, that it is cryptographically valid and also not expired.

Now, let's have a look at the potential use cases of RSCs. There are several potential applications for RSCs, including, number one, verifying resource ownership. So this is critical in the case of bring your own IP address scenarios. And this is usually used by cloud providers. We will talk about that a little bit more.

A second example is to enhance security in transit, Internet transit services. So RSC can replace traditional, what we call, Letter of Authorizations.

So usually downstream would need to provide to their upstream a Letter of Authorization making sure that they are the proper owner of the resources they want to advertise. There is a use case about improving the integrity of routing information database such as PeeringDB, so platforms such as PeeringDB can rely on RSC to make sure the data in there is accurate.

And finally, about geolocation. In some cases, where operators need to report on their geolocation, for example, where are prefixes used and announced, if they attach, for example, an RSC object to that claim, it will allow, for example, a geolocation database to have a more accurate picture.

Now let's dive in the case of Bring Your Own IP. So one of the major use cases for RSC is, as you figured, is Bring your Own IP model where customers bring their own prefixes and ASNs to the cloud providers.

Before onboarding these resources, the customers must prove ownership, and RSC provides a cryptographically secure way to do that. In usual -- now let's have a look at what are the current practices of Bring Your Own IP.

So there are different techniques that are currently being used. For example, email verification, where a verification link is sent to the Whois contact. There are also cases where cloud providers will ask you to place random strings in your Whois records, and then they would compare those random strings.

There are cases where you would use self-sign certificate, and then the public key of those self-sign certificates are placed in the Whois record. And then it is then used by the relying party to verify the signature, for example.

And finally, there is the Letter of Authorization, which requires manual verification. You would agree with me that each of those different techniques used here has flows that can be exploited very easily by ill-intended people organizations. You can

also use ROAS, which provides a little bit more of added security because it is using RPKI for the cryptographic check.

But the issue with ROA, it does not fully verify identity. And finally, you have reverse DNS updates, but this requires also modification of DNS records. And it's more of a trick rather than something which is made for identity verification.

So we did a very quick survey of the different cloud providers and what are the different techniques that they use. For example, Google Cloud is using ROA and rDNS.

Amazon is using a mix of self-signature and ROAs. Oracle is using self-signature only. OVH is using random string. Vultr is using email verification ROA and LOA. So as you can tell, different cloud providers are using different techniques, and this doesn't make things easy for the end user.

If there is a system that could facilitate the due diligence for cloud providers, in the case of Bring your Own IP, this, I guess, would create a lot of facility for many people. So obviously each of those techniques have challenges. So the email verification obviously is subject to email security. So email can be hijacked.

The Whois, where you put a random string in Whois, you're exposing some some level of information which you don't want to to do and it's not necessarily very intuitive. The self-signature as well is not necessarily very intuitive, and in that case you're technically forced to put your public key out there for this purpose.

So ROAs can be useful, but the issue is, as I mentioned, it is not providing any information on the identity.

LOA, so Letter of Authorization, is a manual process and therefore can easily be faked. And finally, rDNS is not easy to use, and you're also introducing new information in your DNS record, which you do not want to do, necessarily. So looking into the RSC -- sorry, into the Bring Your Own IP. So let's see how it works. So what can happen is that the network operator will sign the Letter of Authorization with an RSC of the object that they would create. So this would ensure authenticity of the authorization document.

It can also put a random string with the RSC and this provides cryptographic proof that the resource owner controls the IP address. So another use case is providing Internet transit services. So another area where RSC can be useful is, as I mentioned, when someone is providing Internet transit services.

ISPs require LOAs, so Letter of Authorization, to verify resource ownership before providing transit services.

With RSCs, resource owners can digitally sign their LOA, ensuring a verifiable and tamper-proof authorization.

The next possible use case is routing databases. So platforms like PeeringDB rely on Whois data to verify ownership, but Whois records are not always very accurate. So RSC allow resource owners to sign specific content provided by PeeringDB, providing therefore cryptographic proof of ownership.

Finally, we have the use case which is about geolocation reporting, so geolocation databases such as Google, IPinfo, MaxMind allow resource owners to report their own location, but there are no standard way to verify these claims.

By signing location with RSCs, resource owners can provide verifiable proof of their location information. So the advantage of RSC is that it can provide continuous verification as opposed to the current techniques, Whois-based techniques, or email, or manual techniques that we currently have.

So if there is a system in place that continuously provides access to those RSCs, then it makes it very easy for the third party to verify those RSCs on a continuous basis. Then the resource owner can, for example, create new RSCs or revoke existing RSCs based on their current agreements and the changes in the current agreements.

So to conclude, RSC offers significant advantages of existing ownership verification methods, as we have seen. They improve security by providing cryptographic proof of ownership and hence privacy by eliminating public Whois dependencies and enable continuous verification and revocation.

However, for widespread adoption, service providers must update their workflows to support RSCs, and this is what this research wants to highlight. Basically the challenges that service providers are facing and which could hamper the deployment of this technology.

So quite recently we did a survey at APRICOT 2025 in Malaysia. And we interviewed major industry players, such as Telstra, Telecom Malaysia, and Vocus. So we have received 35 responses from different organizations.

We understand that this sample is still small, but it is indeed providing some valuable industry perspective. And we are still continuing to gather feedback using the survey.

So let's have a look at what we have seen in the responses. So the key barriers to RSC adoption are lack of awareness. So 60 percent of respondents say that there is a lack of awareness. Integration challenges with existing RPKI infrastructure. Of course, right now, it's still a very nascent technology, so integration is inexistent in most of the cases, but there is that integration move that operators need to do to ensure that RSCs are generated in a very small fashion.

And then the benefits of the business benefits are still unclear for 30 percent of the respondents. So maybe there is more awareness to be done in these regards. And finally, a big concern is the regulatory and legal concerns. So, for example, compliance to existing regulations and laws in some country and liability issues.

These are things that are still being discussed at the different levels, whether it is at RIR levels, because they are the one that are going to create those RSCs using their member portal, or also on the relying party side, there are also legal considerations.

So despite these concerns, nearly 50 percent of the respondents are open to testing RSCs in the sandbox environment, indicating growing interest. And this is good news. So several respondents use RSC as complementary to ROAs rather than a replacement. And about 40 percent believe that RSCs should replace LOAs, but 30 percent of the respondents raised concern about operational complexity.

There was also a debate about whether RSCs should be stored in public or private repositories. So the key observation are that RSC can apply to virtually any digital objects. Tools, documentation, and best practices must be clearer. It can simplify or replace legacy LOA processors. And we would need more feedback from operators on the actual use cases and implementation challenges.

So we are, as mentioned, we are still running the survey. So if you scan this QR code, you will have access to our survey, and we would really appreciate if you can send in your responses and tell us what you think about RSC and whether this is a technology that can be useful to your use case.

With this, I would like to thank for your attention. And I would be happy to take any questions. Here is my email, phokeer@isoc.org. Thank you very much.

(Applause.)

Hollis Kara: Thank you. Now we're going to bring Alex back. I'm assured we have slides at the ready. Here we go. Welcome back, Alex.

Alex Deacon: Thanks. So thanks for inviting me here to present the findings of our study on measuring Internet abuse using IP addresses. This is me, if you could go to the next slide.

The DNS Research Federation a not-for-profit organization based in the UK, as you can tell from my amazing UK accent, with the mission to advance the understanding of the domain name system's impact on cybersecurity, policy and technical standards.

Having said that, our remit is a bit broader than DNS, hence this research project on IP addresses. We achieve our mission through education and research, through access to data and engagement in technical standards. Next slide.

So I'll start with a quick intro to the project, describe the methodology we use and then we'll talk about the findings. Next slide.

So this project was funded by ARIN, as you heard earlier, to raise awareness of the issues of IP address space abuse. This is different from abuse that we see using domain names. The focus here is IP addresses only.

Towards that end, we have developed a set of indicators showing how numbering resources are being misused in malware and phishing. Next slide.

So there's three major questions we wanted to answer. The first is, what percentage of reported malware URLs rely on IP addresses for their distribution.

The second is the same, but for phishing.

And then we wanted to understand the geographical distribution of IP addresses used for malicious purpose. So we've sliced and diced the data to show that by RIR and also by country. We wanted to get a sense of how abuse is being distributed around the world. Next slide.

First, the source of the data is from reports of abuse reported to third-party abuse feed providers. I think many of you are familiar with these.

For phishing reports, we used OpenPhish, APWG, Malware Patrol and URL Abuse. And malware, we used URLHaus, Malware Patrol and URL Abuse. Next slide.

The focus here is IP address space attacks. And we typically receive the data from the providers in the form of URLs. These are deduplicated daily so we don't over or double count.

And then once we've deduplicated the data, we enrich the data using other feeds available on our platform, including details of the website, of Whois registration, SSL data, hosting ASN info and the like just to give us as much background and insight as to what may be happening when these IP addresses and the URLs that are associated with them resolve. Next slide.

In terms of determining geographic information, we look at the BGP data to determine AS name, and then we use RIR stats to determine which RIR and country is associated with the address. Next slide.

And once more. So what did we find? So what I'm presenting here is the last 12 months of data, but we'll talk about this later. We're going to be having live dashboards, so you can see the latest and greatest.

So we see that both malware and phishing, they have a fairly seasonal pattern, different trends, different points of the year.

On average, for malware, we get about 58,000 reports per month. For phishing it's about 85,000. And just to note, these aggregate numbers here are our reports, not just IP address ones. Next slide.

When we look at just IP addresses for malware, we see the majority of URLs are only using IP addresses. About 80 percent of the URLs that we see are using IP address only. And I think this makes sense. For the most part, malware is kind of machine-to-machine. Distribution and communications happen without user interaction or the need for human eyeballs. So there's no need for a human-readable name such as domain name. Next slide.

Here you can see the trend for the last 12 months. This is the percentage of reported URLs using IP addresses. And we see a slight upward trend from about 76, 77 percent to about 80 percent today. Next slide.

So looking at phishing, we see something very different in terms of IP address usage. IP addresses are a tiny percentage of the reported phishing URLs, about a .12 percent. It's almost insignificant.

Again, I think this makes sense. If you think phishing as more of a human, consumer-driven exercise, requiring a domain name or a sub-domain to trick or

encourage users to click on a link. It happens here in the brain and not so much machine-to-machine.

So the fact that there's not a high percentage of IP address-only URLs is not really surprising. Next slide.

And then the small percentage we see over time is actually getting smaller. And if you think about this for a little bit, why would an attacker pay and deal with managing a domain name when really it's not necessary, especially when distributing malware. Next slide.

The third indicator is geographic data. This is the visualization by RIR. In this graph, we have data for both phishing and malware, although we know it's mostly malware in this dataset.

We can see how it's split across the world based on the regions defined by the RIRs. What we found is that a vast majority of reports are coming out of the APNIC region. Next slide.

If we look at this by country, we see that India and China are way out in front, followed by the US and the others. Again, this showing how APNIC region is where most of this abuse is happening.

If you go to the next slide, we'll look at region by region. This is ARIN. To be expected, most come from the US, being the largest country in that region, followed by Canada. Next slide.

This is LACNIC. We see Brazil out in front. Again, it makes sense since it's the largest country followed by other countries. Next slide.

This is AFRINIC. As I understand, there's some background and history here. So this may not surprise some of you. But we see the Seychelles out in front for AFRINIC followed by South Africa. Next slide.

In Europe, it's interesting, we see a more equal spread. You see the other category here is the highest. It indicates a more equal spread of abuse spread across the European countries, with Russia in the lead. Next slide.

This is APNIC. Again, we saw this earlier. We have India and China towering above all the others in the region. Next slide.

So our summary is that while we see malware IP abuse, it's significant and it's on the rise. We see the AP region accounts for a majority of the reported IP-based abuse that we see coming through these data feeds.

One thought we've had is that the country results might benefit from a scaled metric based on population size versus the absolute numbers that I showed you. Basically we want to perhaps look into a ratio-driven metric here. It's not clear this is better, but it might provide some insight.

So with that, I will end it and take questions, I guess, now.

Hollis Kara: Absolutely. Since we have the benefit of having Alex online, if there are any questions about his research project, we can take a few before we move ahead.

Gerry George: Gerry George, DigiSolv. Referring to your geographic analysis of malware based on the ES hosting, it showed that a lot of the large percentage are coming from the APNIC countries. Does that suggest that a large portion of the actual players are based there or just compromised machines? Would that information be available?

Alex Deacon: That's a good question. We don't have that information available, especially whether these are compromised machines or machines just being used maliciously and rented by various providers.

We also don't -- haven't done further analysis on the use of reverse proxies and the like. So the data that I showed you today is really just the data that we get from the RIR stats where we map the IP address that we see in the URL to what's in that stat information.

But obviously there's a lot more nuance there happening behind the scene. But we haven't looked into that yet in our research.

Hollis Kara: Great. Thank you. I see one more question.

Sumon Ahmed Sabir: Sumon Ahmed Sabir, from APNIC AC. You showed that India, China and [the US], and then I can see Russia. Is it the population of the country or, more [popular], people there, so they receive more malware? Or is there any specific that those countries actually are abusing or are using malware?

Alex Deacon: Yeah, I think that's the question, I think, we need to understand better. Why is it the case that we see a lot happening in India and China? Is there a call to

action based on this? I can't say for sure why this is the case. Perhaps it's a price issue. Perhaps it's an ease-of-obtaining-infrastructure issue.

Also in terms of the raw numbers, as I mentioned, the fact that the three countries at the top of our list, if you will, are some of the largest. Obviously that influences the raw numbers that we showed and it's why I mentioned perhaps we should take into account population to get maybe a more insightful understanding as to what might be going on here. But we haven't done that yet.

Hollis Kara: Thank you. All right. I see one more over here. Do we have anybody online? No. Okay, Kevin, let's close it out.

Kevin Blumberg: Thank you. Kevin Blumberg, The Wire. No country is immune. And if you are blocking based on countries for the malware, you're obviously not doing a great job.

But the one thing that we saw a couple weeks ago was, an interesting stat was a sub, sub, sub-delegation within Whois. And really the question is, are you looking at the primary owner of the data, the secondary owner of the data, the tertiary owner of the data as the one who is actually creating the problem.

In this particular case, that third delegation down was a company that was there specifically to port scan and look for problems legitimately.

But when you looked at the first one, it was a random Internet provider in Canada. You looked at the second one, it was a leasing company. And then you looked at the third one, it was a US-based company.

So that could really have an impact to how some of these datasets are looking depending on who you're choosing as your delegation choice.

Alex Deacon: Yeah, absolutely. And I said I think there's a nuance and complexity underneath the covers here, which we haven't jumped into yet. But absolutely, I agree. Things get quite complicated.

Those that are attempting to abuse Internet users are good at hiding their tracks behind proxies and proxies and proxies, and primary, secondary, tertiary delegations and the like. So obviously it gets complicated and confusing.

We haven't jumped into those nuances yet in our research.

Kevin Blumberg: Thank you.

Hollis Kara: Thank you so much, Alex. Seeing no more questions, I think we're going to move on. I appreciate your time today and that concludes our grant reports.

(Applause.)

We're moving forward with our RIR updates. First will be a video update from AFRINIC.

Willy Manga: Hello, everyone. My name is Willy Manga, working for AFRINIC as a Deployment Ops Engineer. Today I will present several updates from AFRINIC.

AFRINIC is the fifth Regional Internet Registry, and we cover 56 economies in Africa and Indian Oceans, and at the moment we have 43 staff.

Let's talk about the status of AFRINIC. At the moment, we don't have a quorate board and no CEO, and we had 24 ongoing legal cases.

Appointment of the Official Receiver terminated by the court on 12th February 2025. Since that date, a new receiver has been appointed. The new one, just for information, has announced that the AFRINIC board election will be conducted on 23 June 2025, following an extension granted by the court.

In the meantime, how do we capture and bring value to our members?

It's through the services we offer to our members and also we continue to strengthen our services and to build the Internet community. So let's talk about the growth we had in 2024.

We had a total of more than 2,300 members, but in 2024 it was specifically 132 new resource members as you can see on the graph.

So we continue to allocate and assign resources to our members, be it IPv4, IPv6, and Autonomous System Numbers. So as you can see, the allocation, we still provide resources to our members. And last year, we handled more than 45,000 support tickets.

Regarding the usage of the service, at least last year, in 2024, 720 members were using RPKI. By using RPKI, we mean issue ROA, yeah, issue ROA mostly. So in total last year, it was 11,000 numbers of ROAs that has been issued, and more than 75 percent of members were using IRR Internet Routing Registry. By Internet Routing Registry, of course, I mean the Route6 manage your asset inside the AFRINIC IRR database.

As most of you are aware, we are almost out of IPv4, and by the end of 2024, we had 0.06 percent of the last /8, and we reached the soft landing phase 2 in January 2020. Since that date, the minimum IPv4 allocation or assignment is one /24 and the maximum IPv4 allocation or assignment is one /22. And we had, by the end of 2024, 1 million IPv4 addresses left in our pool.

So let's talk about the capacity building achievement. So we have an online platform whereby we offer e-learning courses in English and French. And last year we delivered this content to people across the world from 85 countries. So it was not just in Africa.

And, yeah, that was -- and it was done and we trained more than 1,900 engineers last year.

We also have a certification platform, cert6.io, and in that platform you'll find certification on IPv6.

We have two tracks, the silver one and the gold one.

So in 2024, 71 people took the test and they were from 41 countries, not just in Africa, but also across the world.

We also have what we call the Deployment Ops program. And in that program, we assist our members on how they can take advantage of IPv6, RPKI. So we assist them on the deployment, advertisement of their prefix, and also advise them on best current practice on how they can use IPv6 in their core network or also for their customer.

So last year, we assisted 14 network operators from 38 countries in Africa.

In terms of the Policy Development Process, we have three policies awaiting ratification by the board, once we have a board reconstructed. And also the RPKI ASO Policy Proposal is currently being implemented. We are at the final stage of the IPv6 Policy Implementation.

The RPD Mailing List continues to have a big number of subscribers. In 2024, it was 969 subscribers.

We delivered several webinars in 2024. It was 10 of them, and we had the participation of more than 1,000 people across the world. You can watch webinars, the past webinars, on our YouTube channels. You have the link, and you can also scan the QR code. We also have a blog.

Last year, we published 12 articles and eight of them were from external authors. Regarding the Engagement Activities, we had several discussion and talks with 18 governments and policy engagement on digital transformation. We have 42 new members of the organization, were inducted on AFRINIC services and governance.

One particular item also we managed last year was to update the contacts from 876 members because you know sometimes the contacts are not up-to-date, and as much as possible we advise our members to update them and also ourselves, we contact them and then work with them to at least update everything they have on their profile.

So regarding the services, the Internet Technical Infrastructure, we continue to maintain the availability of our resources and continue to also modernize the resource we are using. Last year, we managed to have two Internet Exchange Points with an

RDAP servers so that it will increase the connection connectivity and also the critical service availability.

We also continue to automate as much as possible and to monitor our resources. Last year, we also managed to increase the speed.

Now the RDAP server is 10 times faster, as some of you may have noticed.

That's all for me. Thank you.

(Applause.)

Hollis Kara: Next we have a video presentation from APNIC.

Vivek Nigam: Good morning. My name is Vivek. I manage the services team at APNIC. And I'd like to give you an update on some of the activities we have been working on since last year.

So 2024 has been a busy year for the services team. We process more transfers, more support requests. So let's have a look at what has been keeping us busy.

I'll start off with IPv6. So in average we have been making around 1500 delegations every year. Last year we saw slight decline but that only tells half the story.

On this chart you can see the size of IPv6 that we have delegated. Last year we made a large /17 delegation to a member in Singapore and that accounts for the tall

purple bar you see on this chart. Now /17 is the largest delegation we have made till date, so we had to adjust the scale on this graph to make this fit.

Last year APNIC also received a second /12 allocation from IANA, so now similar to ARIN and RIPE we have a /11 pool of IPv6 that we use to make IPv6 delegations.

Our IPv4 delegations are mainly driven by new members. And the reason for that is most of our existing members have already received the maximum IPv4 that is permitted under policy.

In the last few years, we've seen a decline in new member signups. And for that reason, we have been delegating fewer IPv4 addresses.

With ASNs, it's a similar story. Last year, we saw a slight decline, but it's not as obvious as IPv4.

And the reason for that is it's not uncommon for our existing members to apply for additional ASN numbers for the new POPs or for the downstream customers and so on.

And the spike we see here in 2021 is as a result of two large AS blocks we delegated to our members in China and India who operate research and education networks.

So moving on to transfers, the coloured bars here shows the size of addresses that got transferred and the line here shows the number of transfers we have processed.

So as you can see, the size of transfers have not changed much over the last few years, but last year we processed a record number of close to 950 transfers.

So what this basically means is we are processing more transfers, but they involve smaller prefixes getting transferred between members.

Last year, we also noticed an increase in the inter-RIR transfer activity. So when we started processing processing entire transfers 10 years ago, most of the transfers were coming into APNIC and very few transfers going out of APNIC.

Last year we processed 252 transfers which went out from APNIC to other RIRs as compared to only 32 transfers which came into APNIC.

Drilling down further, we can see most of the transfers that went out from APNIC, went to RIPE. That's roughly 14,500 /24s, followed by 9,000 /24s to ARIN.

It's also interesting to note here that our members from South Asia are mostly transferring their resources to RIPE, not to ARIN. And likewise, our members from

Southeast Asia are mainly transferring their IPs to ARIN and not much to RIPE. I'm not too sure what's happening here. Maybe it could be the different brokers who are active in these different subregions.

Moving on to membership, last year we saw a net membership growth of 226 members, which is bit below average, but we did reach a milestone of 10,000 direct members.

So while we're seeing a slowdown in the new membership activity, we noticed an increase in the support services that our members are asking for. Typically, we get questions around my APNIC, our PKI geolocation. So last year, we implemented a new online authenticated chat system so we can provide real-time support to our members, help them with password resets, who is updates and so on.

And as a result, we got over 4,500 online chat sessions with our members. And 96 percent of the members who gave feedback after the interaction gave us positive feedback, which is always great to see.

Another big project we finished last year was the Historical Resource Transition project.

So a couple of years ago, the APNIC EC passed a resolution that required all historic holders in the APNIC region to manage their resources under an APNIC account.

Failing to do so, those resources will be marked as reserved. Subsequently, we also had a policy change which says 12 months after these resources are marked as reserved, they should be recycled and made available for delegation to new members.

So, as part of this project last year, we recycled over 1.5 million historical IP addresses, which is close to 6,000 /24s.

So, as of now, a total available pool is bit over 13,000 /24s, and in average, we are currently delegating a bit over 200 /24s each month.

So, if this delegation trend remains the same, our current available pool will last us for another 61 months or a bit over five years. So if you operate networks in the Asia-Pacific region and you need IPs for those networks, you may qualify to get those IPs from APNIC. So if you're interested, get in touch with a member services team and we'll be happy to help you with that.

Moving on to policies, this year we implemented two new policies. The first one, Prop 154, is around IPv4 assignments for IXPs.

So under this policy, new and existing IXPs can get from /26 all the way to a /22 IPv4 assignment.

But resources delegated under this policy cannot be routed and they are non-transferable.

The other policy we implemented is Prop 156 for temporary IP assignments. So under this policy, members can request for IPs on a temporary basis like six months if they need to use it for exhibitions or conferences like this one.

Earlier this year, we also had two new policy proposals which were discussed at APNIC 59.

The first one is Prop 162 for Whois privacy.

So this proposal says we should redact all contact information from the Whois database. And if anyone wants to see this information, they need to query the Whois database through authenticated MyAPNIC or an API.

The other policy which got proposed was Prop 163 announcing Whois transparency.

So this proposal suggests we implement a referral server for Whois so the Whois queries get redirected to the appropriate Whois service similar to order. Neither of these policies reach consensus so they've been returned to the mailing list and they'll be discussed further in our next conference.

So that brings me to the last slide. Our next conference is APNIC 60 that will be held at Denang in Vietnam.

I look forward to meeting some of you there. I hope you found this presentation useful and thank you for listening. Bye for now.

(Applause.)

Hollis Kara: All right. Next we'll move to an in-person presentation. I moved too fast. Happy to welcome Alfredo Verderosa Chief Services Officer, LACNIC.

(Applause.)

Alfredo Verderosa: Good morning. I am Alfredo from LACNIC. I'm going to present on key updates from our region.

First of all, as many of you may know, we are going through our leadership transition process. Last year Oscar our former CEO for the last 10 years, he announced his decision to step out and the Board, in alignment with our succession plans, appointed Ernesto, who is our deputy CEO as the new CEO.

This decision was very welcomed by the community and also by the staff, and it represents a stability and continuity in our process and projects.

And the communication was also transparent internally and externally. If you want that QR, you can see the leadership session we had in LACNIC 42 in Paraguay where we informed the community about this.

Second, 2FA authentication is mandatory since last March for all the organizations in category medium and above.

This is a process we have started early last year because we noticed some unauthorized access to MyLACNIC portal accounts and several credentials were being sold in the black market so we decided to go mandatory. First we conducted a user survey in order to see or validate that there were changes needed to the software.

Immediately after that, we started with a campaign, an information campaign contacting our members and explaining the importance of this and it was very successful campaign because by March of this year, when it became mandatory, other than more than 90 percent of members activate.

We'll do the same thing with smaller categories starting later this year.

Okay. About our campus, which is technical training platform. Last year we had more than 7,000 students. The campus is one of the most valued benefit for our members. And something interesting is that two years ago we started with specializations that are like training tracks with three levels, basic, intermediate and advanced. And this year we are having graduate students who graduated in the specializations.

Okay. About our members, satisfaction survey. Last year we achieved 96 percent of overall satisfaction. And this survey is very important for us, not only because we are very happy to achieve excellence levels but also it provides a lot of feedback we incorporated in our strategic planning.

And what else? Finally a couple of things about our member base. The member base is growing since IPv4 exhaustion it decreased the pace but it's still growing, around 200 or 300 new members each year.

Something interesting is that so far we have almost 1600 IPv6-only members.

And also it's growing our waiting list. It became more of a distant hope than a waiting list. Members receiving services today waited four years and members entering the list today will have to wait about 10 years. We have been very, very clear in communication and telling them that it's at least 10 years' wait.

And I believe that is all. Invite you to join us in LACNIC 43 in Sao Paulo virtual or in person and later in October we'll be in El Salvador. So you are invited too.

Finally, if you want to know more about LACNIC and Latin America and Caribbean, you can scan the QR Code and there's more in the LACNIC blog. Thank you very much.

Hollis Kara: Thank you, Alfredo.

(Applause.)

Alfredo is here through the rest of the meeting. If you have any questions for him, I suggest you track him down at one of the meals or breaks. And last, I'd like to introduce the video from the RIPE NCC.

Alastair.

Alastair Strachan:

>> Good morning, everyone, or good afternoon. I'm not sure where I am in the agenda. My name is Alastair Strachan. I work at RIPE NCC as one of the community development officers.

Sorry I can't be there in person today, but I will be joining hopefully later this year, so I'll be able to see you all and have a good catch up.

Today I'll be running through the RIPE NCC update. This is just a look at the last year, where we are now and what's coming in the future. So first off, just a quick overview of our five main strategic objectives.

So we are working to support an open, inclusive and engaged RIPE community; operate a trusted, efficient, accurate and resilient registry. We want to enable our

members and community to operate one secure, stable and resilient global internet.

We want to maintain a stable organization with robust governance structure and attract engaged, competent and diverse staff. Looking at our focus points for 2025, we are working hard to ensure the registry and RIPE database have the appropriate levels of accuracy, compliance, resilience and security.

We are pushing to be a center of excellence for our data measurements and tools, things like RIPE Atlas, that provide insight on the Internet and its operations.

It's very important to ensure the organization's stability and financial strength, and that resilience also, we need to ensure we're resilient in the face of political legislative regulatory changes that do have the potential to affect our operations.

And also security and compliance, we need to maintain necessary levels of security and compliance with best practices and applicable regulations. We have recently published our annual report and financial report for 2024.

That's part of our general meeting supporting documentation, and that can be found on the website, if anyone here wants to go through, so just RIPE.net, and you'll be able to find the annual and financial reports for last year. Just a highlight, as you can see, we had a busy 2024.

We certainly hit the ground running with the launch of our redesigned version of RIPE.net. That's our main website.

In February, we had the first of our roundtable meetings with governments and regulators. That was within Europe. We also published one of our first big articles in regards to the role of IXPs in the Middle East.

March, we saw the rollout of two-factor authentication across all NCC access accounts. Following that, we joined Mastodon in Athens, Greece. We held seat 12. That's the Southeast Europe meeting.

Alongside that, we had our round-table meeting again for governments and regulators focused on that Southeast Europe region.

May, we hosted RIPE 88. That was in Krakow. It was a great meeting. I'm sure there were some of you in the audience today who were there. We also had our Internet Measurement Day in Uzbekistan.

Now, I know Americans always joke that Europeans take June and July off. I'm aware that this kind of makes that look the case, but I can assure you we were all busy working as well. August, we saw the RIPE NCC Academy summer school.

We then had the CAPF, so that's the Central Asia Peering Forum, that was held in Bishkek, Kyrgyzstan, and we launched the LIR Fundamentals course in the RIPE Academy.

Well, following that, we saw the Internet Measurement Day in Romania, and another pretty big article was published on RIPE Labs in regards to how to get IP addresses for your network, the best practices, the costs, things along those lines. November, we held the second of the RIPE meetings. That was RIPE 89 in Prague.

We had the Internet Measurement Day in Turkey, and then we had the third of our roundtable meetings, this time focused on the Middle East.

We closed off the year with MENOG, that's the Middle East Network Operator Group, that was in Muscat, and then finally we had the Green Tech Hackathon.

So as you can see, there's been a lot happening. Looking at the membership, and now this is as of 2024, the 31st of December. I will note that one member can hold more than one LIR.

That's why we see this difference in active LIRs versus active members. We did see 957 new LIRs.

We have over 120 -- well, we don't have over -- we have 120 member countries and of our active members we see just over 15,000 with v6 allocations. This is below is just a breakdown of our top 10 countries.

So you can see Germany, UK, Russia, France, Italy. It's kind of similar across members, new members and LIRs. We definitely see similar across that.

Now we did have 1,536 closures last year. 196 of those were initiated by the RIPE NCC, 1340 initiated by the members, and the majority of that was due to non-payment. We also saw 952 new LIR applications cancelled.

So looking at 2025, what we're up to this year, there's quite a few things. First up, when it comes to ensuring accuracy and compliance, we are conducting in-depth registry accuracy investigations.

And we are doing more extensive automated sanction screening in the RIPE database. We have, or we are phasing out MD5 hashed passwords and offer API keys for better security.

Organization-wide, we're implementing international compliance standards like ISO 27001 and carrying out ISAE 3000 audits.

There's also EU sanctions that create a significant workload and we actually now publish a Quarterly Sanctions Transparency Report on the website.

With data measurements and tools, we're really looking to improve things in a whole host of different manners. So obviously the quality of our data sets, we are working hard to improve the quality of that.

The data coverage, we are pushing hard to cover the top 10 ASNs in each country with RIPE Atlas. The peering policy, it's a lot more targeted for RIS, so we're looking for greater diversity in peers and networks, or of peers and networks, I should say. The broader data set, we're looking for more information, but more precision within the data that we have. And using that, we can develop more data-driven storytelling, and that allows us to share a lot of insights into what's happening with global routing, things along those lines.

We also -- obviously with these data and measurement tools, we have a huge amount of historical data, and we have been working hard on making a more cost-effective data storage solution.

Therefore, we're drastically reducing our data center footprint and we're actually going from 46 racks down to 10 by the end of 2025. So there's been a lot of work in reducing that data storage.

I've mentioned RIPE Labs a few times now. RIPE Labs is our kind of online blog, our online forum where we publish a lot of the research and things that's been done both by us as the RIPE NCC and also by the community. So these were two very popular articles. One was a deep dive into the Baltic Sea Cable Cuts by my colleague Emile.

And Qasim did a really nice one looking at the internet landscape within the Middle East itself. These are again some more things that we've published via RIPE Labs. So the how to get your IP addresses for your networks. This was kind of looking at the most cost-effective way, what people should do between hosted and delegate.

A whole host of different things were included in that, and also for the second article that's mentioned here, which was focused on the roles of IXPs in the Middle East.

Again, it just pushes this data-driven storytelling that we really want to emphasize on Labs and things like that. So, obviously we're the RIPE community.

We are the secretariat for RIPE community. So strengthening that is incredibly important to us, as well as the RIR system. So, we offer a whole host of online learning through webinars and the RIPE Academy.

We do in-person courses and certification, the RIP NCC certified professionals exam. We support a lot of community initiatives such as NOGs and hackathons. We do outreach with academics and universities, with programs like RACI. We are working hard with the NRO on the review of the ICP-2 document.

That's to increase the resilience of the RIR system itself. And we also represent the technical communities in important internet governance events, like the IGF and WSIS+20.

This slide really just shows kind of the interdependencies of our areas of strategic areas. So by being a center of excellence for data measurements, that helps us when it comes to creating and fostering -- creating and fostering environments and dialogues throughout the service region to maintain a highly engaged community. It also works towards increasing knowledge.

So this is just a slide to show how these different strategic areas help each other towards the greatest strategic goals. Now, I've mentioned there is a lot of increasing financial and legal resilience that we are dealing with.

Things like, I mean, everyone's heard of GDPR by now, but the compliance with GDPR and the Digital Services Act, we're also reviewing the applicability and potential impact of the upcoming NIS2 directive. There's exploring how we can overcome bank limitations to receiving funds from members in certain countries that we're unable to cover due to OFAC sanctions. We've established a legal entity in Dubai.

This is really to enhance our presence in the region and better serve members in that region. We're also working hard in generating sponsorship for our events and data services.

Side note, this is one of my goals. So if anyone in the room is interested in sponsoring our events or data services, please feel free to reach out to me.

Just a little free plug. We have the RIPE Labs podcast. So I've mentioned RIPE Labs. That's where we publish a lot of our material. We also have a really cool podcast program where we interview and speak to a whole host of different cool people from the Internet. And there's some really interesting topics. So be sure to listen on your preferred audio provider.

I don't know the correct way of saying that. But there's some really cool things on there. So please do take a look at the RIPE Labs podcast.

We have our five main events. We obviously do a whole host of other smaller things, but our main events this year, we had SEE 13 and Sofia. That was in April at the beginning of the month.

That went really well. We have RIPE 90 coming up in Lisbon on the 12th-16th of May. We have the RIPE NCC days in Moldova, 18th and 19th of June.

RIPE 91 in Bucharest in October. And then finally we have the MENOG 25. The location hasn't yet been announced but the date is set, 23rd to the 27th. I mentioned RIPE 90.

Please, anyone in the room, feel free to come.

It would be great to have you there. I think some of you will already be registered, but if not, please visit ripe90.ripe.net to register and it would be great to see you there for that. I always love to include a question and comment slide on a pre-recorded presentation and I'm not in the room at all.

So if you have questions, tough. No, If you do have questions or comments, you can always reach out to me astracha@ripe.net.

I'll be more than happy to help with, well, anything I can within my ability. I've learned a long time ago, never oversell yourself.

So, yes, with that, I'd like to thank you for your time. I've always loved being part of the ARIN meeting.

So I look forward to seeing you all later in the year. And thank you. I'll now hand over to -- I don't know if they're this side or this side. But back to you.

Hollis Kara: I've got to love Alastair.

All right. Next we head into our lunch break. I would like to remind folks that in-person attendees can join us for a table topic on ICP-2. If you don't see a sign on

the table, I think it's pretty sure over there, but look for Nick, Amy and perhaps Kevin, they'll be happy to talk more with you about that.

Virtual attendees, please back at 1:30 for the start of our policy block. You're welcome to leave the Zoom up or log out and come back when you're ready. Thank you, everyone, for your participation this morning and I look forward to seeing you back at 1:30.

[Denise to add darby first part].

(Lunch recess taken at 12:20)

[1:30].

Hollis Kara: Do we have lurkers over in the lunchroom we have to round up? All right. Ashley is going to yell for lurkers.

But in meantime, in respect for time, it is 1:30, which means it is time to talk about policy. Chris Woodfield, would you like to come on down and tell us a little bit about Draft Policy No. 2024-5?

Chris Woodfield: I'm Chris Woodfield, representing the ARIN AC. Myself and Bill Herrin are the shepherds for ARIN 2024-5: Rewrite of NRPM Section 4.4, Micro-Allocation.

There's my actual title. We'll move the problem statement to begin with. The current NRPM Section 4.4 language hasn't aged well. As the ARIN 53 Public Policy experience port demonstrated, 4.4 has also become difficult to implement by ARIN staff. The growth and use of Internet exchanges have also changed.

The overhaul seems to have improved technical soundness, respect the privilege of a dedicated pool and to more closely observe conservation principles using clear minimum and enforceable requirements and underscoring the value of routability and allocated prefixes as desired.

We will move on to the Policy Statement text. This is a fairly long Policy Statement. It is a drop-in replacement for the existing 4.4. And as such I'm not going to read the

entire thing verbatim, but I will highlight the parts that are relevant and notably the parts that change current NRPM policy.

ARIN will reserve a /15 equivalent, which is the same as the current policy, for critical Internet infrastructure within the ARIN RIR service area. Allocations from this pool will be no smaller than a /24, as normal practice. Sparse allocation will be used.

The CII includes -- and this will be, this is the topic of discussion, I'm sure -- Internet exchanges, IANA-authorized root servers, TLD operators that offer domain-level DNS services to outside parties -- yes, that's a mouthful -- ARIN and IANA.

Previous allocations must continue to meet the justification requirements under this policy. Use of the policy for CII is voluntary. An IXP or another CII infrastructure operator is not required to use 4.4 space for this purpose. And ARIN will publish all allocations.

Exchange operators must justify their need by providing a minimum of three initial participants, all not under common control, connected to a shared physical switching fabric, which is a new definition in this Policy Proposal. And they must be used for the exchange of data destined for and between the respective networks, which defines the functionality of an IXP.

ARIN will require participant names, ASNs, contact information, and the IXP itself cannot be one of the three participants.

The addresses allocated under this policy may be publicly reachable under the operator's discretion. The current policy text is silent on that matter. And per the Policy Experience Report last year, this was a topic of uncertainty among ARIN staff. So that is covered in this proposal.

TLD allocations must also provide justification of need and certification of status as currently active zone operators. A recipient may request up to a 24-month supply of equal resources. And request for additional resources follow the same policies as other sections of 4.24.1's usage requirements.

This is the immediate timetable. Here is the version of this. As you can see, this proposal has been floating around for quite a bit. There's been several revisions so far.

There was a Staff and Legal that was requested, but then additional comments came in during the Staff and Legal process. And as such we have not promoted this

to a Recommended Draft Policy despite the completion of that Staff and Legal. Apologies to Staff and Legal who may have to go through this process if there are changes.

Here's the Staff and Legal Review text. The staff understands the purpose of the policy, how 24s and additional 24s are requested. It clarifies that they're exclusively for recreational use and it resolves immediately around the routability of the space.

There's other changes that we've changed the RIRs to ARIN. And there were some recommended staff changes to text that have been adopted in the current version of the proposal, as you can see here, including a couple of typo fixes.

So implementable as written. No impact to registry operations and services. No material legal issues. Implementation requirements are training, documentation and procedures. And this was completed in March.

Quite a bit of feedback on the Mailing List around this, a lot of work shopping over the exact language, which continues to this day. The quote of the use of the policy for CII is voluntary, is that unambiguous? There was a concern is could that be interpreted to mean it is not required that the space being used for CII purposes despite language later in the proposal that sets out those requirements.

The term "TLD operators that offer domain-level DNS services to outside parties," yes, it's a mouthful. To some it is confusing. The intent there, as I read it, is to include top-level operators such as ccTLDs, gTLDs and others that offer DNS services to others while excluding vanity DLDs -- there's another term I'm not thinking of -- but a company that registers a TLD for its own use. Its own company name, its own brand would not qualify for CII space but other uses, other TLD operators would qualify.

There is no mention of how root server operators, ARIN or IANA, need to justify their requests. And there's a question about whether or not 4.4.2 creates a chicken-and-egg problem given that they're only an operator once they enable their infrastructure, and do they need to get space in order to get that status, and do we need language to clarify that you don't have to be an existing operator to request this space.

So to summarize the policy impact, first off, it renames the section header to better communicate its intent. It resolves several ambiguities.

The definition of organizations that qualify for CII space are clearer. It states definitively that CII allocations may be routed. And it explicitly restricts the use of those allocations to resources required to operate the IXP.

My read is that staff intends to interpret this fairly liberally but with clear boundaries, just to make a single example. An IXP that wants to host the IXP's website using the space would likely be an acceptable use, whereas, an IXP operator whose parent company uses that space for their website would most likely not.

It also provides guidance on the qualifications for larger than /24 allocations, which the existing policy is silent on.

So our questions for the community: Does the current language match the community's understanding of what types of operators should qualify for space? There's been quite a bit of workshopping on the PPML trying to nail this down, but still open to feedback on that, obviously.

Should there be language explicitly stating that all recipients qualify for an initial 24 on this? Should we not offer larger initial requests? And also are there potential avenues for abuse of this policy that are currently not accounted for under this policy text.

Thank you. Open to questions.

Hollis Kara: We'll welcome up Bill. Microphones are open. So please queue up. Kevin.

Kevin Blumberg. Kevin Blumberg, Toronto Internet Exchange. I'll give you a bit of firehose here.

In APNIC region, they specifically prohibit announcement of this space this for Internet exchange operators, so there's this disconnection between the two regions. And I think that needs to be fleshed out as to why.

I think part of the reason is because we allow this space to be used for non-Internet exchange point fabric. It's your services, your website as you called it.

So when you're a new Internet exchange operator, you now need a /24 for your fabric, you need a /24 for your services, you need multiple AS numbers. I don't know if the CII space today was really envisioned to be about the ancillary services that are not critical unto themselves.

So it may be worth looking at the fabric being the critical nature and the services not necessarily. Again, that's to be determined but more feedback on that one.

The issue with routing is exactly that. If it is for your fabric, there should be no reason to route it. In fact, you really don't want to route it. So I think more time needs to be spent on that.

I do appreciate in the language that we've gotten rid of the "me, myself and I" loophole where you can basically create an Internet exchange with yourself through multiple AS numbers and Orgs. So that language is wonderful in the addition.

There appears to be a major scope creep with DNS operators. I can't really speak to that, but that is a concern. Just how many Orgs are we giving access to the CII space for in the DNS. There was a lot of concern back in the day that it was not meant to be for the thousand-plus new TLD registrations that came in.

So it was fairly limiting. I know you're trying to improve the wording, but by improving the wording, are you actually just expanding the scope well beyond the intended purpose as a way to potentially bypass the Wait List because this is a self-filling pool.

Last thing, there's absolutely potentials for abuse. Staff should have extreme discretion to review what a critical public-good Internet exchange point is. And I think they've done a very good job of that and they should continue to do that.

Last part, it's not in here at all.

Bill Sandiford: Second to last part?

Kevin Blumberg: This is actually the last part. It's not in here at all. We removed out years ago return and renumber. You can't add another /24 to a fabric. You have to return and renumber if you can't get the sparse allocation to do a mass change.

So you may want to actually codify in here the ability for an Internet exchange, for their peering fabric, to be able to do a targeted return and renumber.

Bill Sandiford: Thanks, Kevin. Any comments online?

Beverly Hicks: Yes, I have one comment from Altie Jackson, ARIN Fellow: He agrees with this policy and supports it as written.

Bill Sandiford: Great. Seeing nobody else in the queues and nothing else online, thank you, everyone. The Advisory Council will take your feedback. Thanks.

(Applause.)

Hollis Kara: Thank you, Chris. Moving on to our next policy, Leif Sawyer is on his way up here to talk about 2025-1.

Leif Sawyer: Thank you, Hollis. This is Draft Policy ARIN 2025-1: Clarify ISP and LIR Definitions and References to Address Ambiguity in NRPM Text.

I'm Leif Sawyer. My co-shepherd is Elizabeth Goodson.

And so this problem statement stems from the fact that we incorporated Section 6 sort of wholesale into the NRPM years ago. And that text originally had LIR and ISP in different places. It was not consistent, which didn't matter back then in the places where it came from because they meant the same thing, mostly.

An LIR was everyone who received addresses. And an ISP was a subset of LIRs that could then give out more addresses to other LIRs or other ISPs.

So what this proposal does is it tries to streamline and address the ambiguity by replacing all instances of either LIR or ISP in the NRPM with a combination. You'll see that here as we go through the Policy Statement.

So first off, we're going to remove one word, "primarily" from here, bolded in red. And then you'll start to see a whole bunch of LIR/ISP in red where we are removing it. So this section here is going to just go away because it no longer makes sense to call out that they're interchangeable.

And here we go. And there's a lot of them.

If you really want me to stop and go through any of these specifically I can go back, but they're all in the Discussion Guide and they're all online.

As you can see, we received this Policy Proposal back in January. It's had a couple of revisions, once into Draft Policy and once recently.

Community feedback has been limited, though positive. It does look pretty good. It does what we want it to, and it's fairly limited in scope. Otherwise we've had no other feedback.

So policy impact. No Staff and Legal has been presented yet. This is the first time you're seeing it. And we don't attempt to align definitions with other regions.

So that may or may not be a concern to you all. But it does equalize the application of LIR and ISP terms throughout Section 6.

So, are you in favor of the policy, and should we continue working on this?

Hollis Kara: With that, microphones are open. Please go ahead and queue up. The same with online.

Bill's on his way to the stage. Got nothing online so far. I'm having déjà vu, honestly.

Okay, Kevin.

Kevin Blumberg: Kevin Blumberg, The Wire. I like that you're doing work to clean this up. That is good. LIR has to go, just as ISP has to go for two reasons.

One, LIR is a term used in other regions and has very specific in-use meanings in those regions. And us using the term "LIR" differently or in a way that is not cohesive is a bad idea. So we haven't used LIR in the region in the way other regions have used it.

It is better to just dump it completely, dump ISP completely, and use a new consistent term wholesale because, again, LIR is not consistent with the other regions and was not really used in our region.

ISP is something we talked about when we were looking at ICP-2. The concept of an Internet service provider is not the same as it was when these documents, et cetera were written. And I think there are more encompassing and appropriate terms.

But the flavor of this proposal is good. I'm just recommending, start with something fresh, do that search and replace through the entire document with a fresh definition that doesn't have any confusion with other regions or ourselves. Thank you.

Bill Sandiford: All right. Anything online?

All right, seeing no one at the mics -- here comes one.

Kat Hunter: Kat Hunter, AC chair. There's been a number of occasions when we've been asked to not create new terms or define things. If there's anyone in the community that is in the room or PPML in your own time, we are open to suggestions as to what to use to replace LIR and ISP because I know that could be potentially contentious with whatever we come up with.

Douglas Camin: Doug Camin, CCSI. Originally this policy -- I was the author of this policy -- and this policy was submitted originally because the previous policy from ARIN 53, I believe, was abandoned when it attempted to make a change to Section

6.5.1a that addressed the ambiguity in this text. And the community feedback that we received at the time was that -- was a request to do exactly this policy.

There was ambiguity, and if we were going to change it and fix that text, we should do the whole component and change the LIR and ISP components.

I'm not saying that that doesn't mean we shouldn't -- certainly appropriate to say if we want to create a new definition. But the background of this particular policy and its genesis came from community feedback that was received on a prior policy that was abandoned in order to create this policy and the path for it.

Bill Sandiford: Thank you. Did you want to respond?

Leif Sawyer: Kevin, I wanted to respond to what you said. Would you be in favor of this policy moving forward with the text as written, and then a new Policy Proposal being submitted with definition proposals?

Kevin Blumberg: No. If the new Policy Proposal is to keep LIR in the NRPM, then no. However, to what Kat just said, and I will agree that new definitions are never a great thing, I would be far more supportive of keeping ISP in with a more liberal definition of what an Internet service provider is than keeping LIR in.

So even an ISP, which is a sort of known quantity, the more expanded scope would be fine. But the term LIR to me, in our region, especially with the other regional things, is a nonstarter for me on this policy.

Leif Sawyer: Okay. Thank you.

Bill Sandiford: Online.

Beverly Hicks: Altie Jackson, ARIN Fellow: "Agree with this. It is good to have one standard definition across the region."

Bill Sandiford: All right. Seeing nobody else at the microphones or online, thank you everyone for the feedback. The AC will take it under advisement.

Hollis Kara: Thank you, Leif and Bill.

(Applause.)

All right. Here we go. And we're on to our third policy. Gus, if you want to come on down. Gus Reese, from the Advisory Council to present on Draft Policy 2025-2.

(Applause.)

Gus Reese: Welcome, everybody. I'm Gus Reese. I'm the primary shepherd on ARIN 2025-2: Clarify 8.5.1 Registration Services Agreement. And Kendrick Knowles is my co-shepherd on this policy.

So this was one of two policies that came out of one of the working groups of the Advisory Council. This one came out of the Performance Experience Report Working Group.

This is the problem statement. The current policy mandates entities receiving transferred resources sign a new RSA unless they have an RSA on file no older than the last two versions. However, defining RSA versioning requirements within the policy manual does not align with the Policy Development Process guidelines, as determining which RSA version is considered current is a business decision rather than a policy matter.

All right. The changes to the policy text here. So it goes from -- I put in red the words that would be removed. So the receiving entity must sign an RSA covering all resources to be transferred unless that entity has a current RSA on file per ARIN business practices.

The timetable for implementation is immediate. And this came to the AC as a proposal in February. And after our meeting in February, it was accepted as a Draft Policy.

And this has been submitted a couple times to PPML for feedback and the responses that I received as calling this policy as reasonable.

I wanted to throw in a little brief history of how the two-version RSA was introduced into the 8.5.1 to begin with.

So it was introduced in 2016 and implemented in February of 2017. The initial text of 8.5.1, Registration Services Agreement, stated that transfer recipients must sign an RSA for the resources being received.

When this language originally went through the Staff and Legal Review, they identified a few issues with the original language and proposed modified version, which is what the 8.5.1 says today about having the registration agreement within the past two versions.

What is the impact of this policy? The changes in this policy removes the version requirement from the Registration Services Agreement from policy, returning that

decision back to ARIN staff as to which version of the RSA they consider current for 8.5.1 transfers there.

And that's it for my quick presentation. And the questions to the community are, are you in favor of this policy. I would love your feedback.

Bill Sandiford: We'll start on this side here.

Atefah Mohseni: Atefah Mohseni, ARIN Fellow. I support the policy as written.

Bill Sandiford: Thank you.

Online.

Beverly Hicks: Altie Jackson, ARIN Fellow. In favor of the policy as written.

Bill Sandiford: All right. We'll give it another 30 seconds or so. Remind those in the room, microphones are open. Give the online folks a second because I believe the webcast is a few seconds delayed, correct?

Hollis Kara: There shouldn't be much of a delay.

Bill Sandiford: All right.

All right. Hearing and seeing none, thank you, everyone. The AC will take the feedback under advisement.

Gus Reese: Thanks, everyone.

Hollis Kara: Thank you, Gus.

(Applause.)

All right on to our final policy for today. Doug Camin, come on down. We'll talk about Draft Policy 2025-3. Let's hear it for our next contestant.

(Applause.)

Douglas Camin: Good afternoon, everyone. I am Doug Camin. And along with Gerry George, we are the shepherds for Draft Policy 2025-3: Change Section 9 Out-of-Region Use Minimum Criteria.

So this policy is, this is the first time it's being presented at an ARIN meeting. The Section 9 -- the problem statement, I'm sorry -- the current text has, in Section 9 of the NRPM, the out-of-region use requirements are for an organization to have at least a /22 before they can justify their out-of-region use.

In the problem statement, this makes a statement that this harms smaller organizations that might have less than a /22, but do not require -- this harms smaller organizations that have less than a /22 in region but do require some for out-of-region use.

So this is a really simple update. Change the following text in Section 9 from at least a /22 to at least a /24.

So the result of this would put it in line here. So you can see the whole section here. But under IPv4, change it to a /24. And that's the only change in this area.

This policy was new and was just accepted as a Draft Policy in March. So this is the first time it's been presented at a meeting. It has received a little bit of feedback on PPML. The community feedback that was received, while limited, has been positive.

And the only notable thing that was brought up was a question of whether or not we should go further and eliminate all of the requirements for holding, basically eliminate no /24 and no IPv6 holdings at all.

And the policy impact here. This does not have a Staff and Legal, but if it was changed, smaller organizations would qualify for out-of-region use, and more organizations would qualify if it was a /24.

So our questions for the community are, does the benefit outweigh the risk of potential fraud or security risks by using the smaller block size? And do you have suggestions for change or are you for or against this policy?

Bill Sandiford: Microphones are open, both in the room and online. Start on this slide here.

Eddie Stauble: Eddie Stauble with IPTrading. I originated this policy. We have run across a handful of registrants in ARIN who could use this, but because they don't have a /22 in region, we usually send them to RIPE where they get a legacy block, sometimes from ARIN. It's the cheapest route for them. We would like to see this implemented.

Bill Sandiford: All right. Thank you.

Online comments.

Beverly Hicks: Ray Krivanek from Radio Toolbox: "I am in favor of this policy change as written."

I have a second one if you'd like it.

Bill Sandiford: Yup.

Beverly Hicks: Altie Jackson, ARIN Fellow: "This policy is straightforward and is a plus to small organizations. I'm in favor."

And the last one I have is from Brad Fecker, state of Oregon, ARIN 53 Fellow: "Reasonable policy. In favor as written."

Bill Sandiford: Over to this side here.

Andrew Dul: Andrew Dul, 8 Continents Networks. Question for staff. Are they interpreting the /22 as having to be contiguous or could it be a collection of blocks?

John Sweeting: John Sweeting, ARIN CXO. It could be equivalent.

Andrew Dul: I do not support the policy as written.

Bill Sandiford: Online.

Beverly Hicks: Jason Cook, Dennis Group: "I agree that the current language does disadvantage holders of minimal IP space. However this policy would allow an organization holding a /8 to use only a /22 in the region. Would a percentage or sliding scale be considered instead?

Douglas Camin: Staff question.

Beverly Hicks: I have one more if you want. Max Krivanek from CodingDirect: "I largely support this policy, but also feel we should update IPv6 as well."

Bill Sandiford: Could you repeat the previous comment, please.

Beverly Hicks: Sure. Jason Cook, Dennis Group: "I agree that the current language does disadvantage holders of minimal IP space. However, this policy would allow an organization holding a /8 to only use a /22 in the region. Would a percentage or sliding scale be considered?

Douglas Camin: So, if I'm interpreting the question, if they have a /8 out of region, can they move a portion of it in region to qualify?

Mike Burns: Mike Burns, IPTrading. This is for transfers and justifying transfers, where it's really saying that -- I think the question is saying, if someone in ARIN region wants to buy a /8 and register it in ARIN, they would only have to use a /24

here. But to me that's really not much of a problem bringing a /8 registration into ARIN, which is the only way that question makes sense, to me anyway.

Bill Sandiford: Thank you.

Tina Morris: Tina Morris, AWS. I had a different interpretation. I think the question was, can a percentage of the 8 be required to be used in region and not just a specific size block.

That said, I do not support this. I think if they want to use it out of region, there's a registry out of region, too, to work with. And I do not think that this is a very high bar for that.

Bill Sandiford: Thank you.

Eddie Stauble: Eddie Stauble, IPTrading. I did find it strange when looking at this policy, I'm not sure -- there is no upper limit. If you have a /22 in region, you can theoretically use Section 9 to justify a /8 just by your out-of-region usage, which seems strange that you'd have the lower limit but not an upper limit.

Thank you. Any more comments online?

All right, seeing nobody else at the mics, thank you, everyone, for your feedback. The AC will take it under advisement. Thank you.

Hollis Kara: Thank you, Doug and Bill.

(Applause.)

That concludes our second policy block of the meeting and our final policy block of the meeting so congratulations to the community on that accomplishment.

Moving forward, I'd like to invite John Sweeting, our chief experience officer, to give an update on chief experience officer stuff.

John Sweeting: John Sweeting, chief experience officer. I'm going to give you an update on stuff, as Hollis said. And I won't say NRPM.

Hollis Kara: Thank you.

John Sweeting: I got it in.

(Laughter.)

All right. There's been a lot of stuff going on at ARIN over the last six years, a lot of changes, a lot of reorganizations, a lot of trying to align things and become more efficient.

And one of the big things that our president and CEO asked for was, how do we provide value to our customers? How do we show our customers the value that we provide to the community?

So I was promoted to chief customer officer in 2019. And we started doing some things, some stuff. We brought together the Communications Department and the Registration Services Department. They reported to me. And we started coordinating on our messaging and focusing on improving the customer experience and operational consistency.

Then, right as we were doing this, this was at the very end of 2019, like December is when I got promoted to chief customer officer. And two months later, as we were starting to move these pieces around, we got sent home. And said, work from home for a couple of weeks. We'll let you know when you can come back to the office.

Anyway, everybody remembers what happened then. I don't like to talk about it so I won't say it, but it was very challenging then.

I just hired Joe Westover to come on. He was going to be the product manager for looking at all the stuff for customers, how do we make things more efficient, how do we take our processes and make them more efficient. But he was on there for about, I don't know, he was in the office for about a week before he got sent home.

It's very hard to pull people into an organization, get across what you're expecting from them to help you do when you're doing all this on Zoom. And nobody at that time was that good on Zoom and understanding all the things we could do. But we somehow got through it.

Also during that time we brought on Brad Gorman. RPKI was getting very intense. And our president and CEO said, hey, we need to have somebody focused on being a product owner for RPKI specifically. We brought Brad on to do that.

We added these little pieces. And, finally, in 2023 we were like, you know, being just a chief customer officer is a little piece of the puzzle to be able to provide really good experience and show the value to the community. And basically we were doing a lot more than just a customer-service thing.

So my title was changed to chief experience officer, and we expanded the team. We just recently, in the last, I think, in the first part of this year -- oh, was I talking to a slide that wasn't there yet?

(Laughter.)

Where is Christian. I told you that happens to me, Christian.

Anyway, these are the pieces we brought in. We now have a customer technical service team headed up by Brad Gorman. I think that's the next slide. There you go.

So the department goals, (indiscernible) pursuit of customer excellence. We want to be the best we can be at providing the services. And the one thing that always resonates with me that Mr. Curran always says is, "What's the value? Why are you doing this? Does this provide value to the community? What value does it provide? Would they be willing to spend money on the value they get out of this?"

That's what we always look at. We look at what is the value of what we're doing to the customers.

So all these things, if you wrap them all up, it's value. What's the value? Raising the standards of the services provided to our members, cutting down the time it takes to process tickets.

I'm going to have the slide in the transfer presentation that's going to give some good statistics on some of the good things we've done there.

Eliminating duplicitous processes where we're going from one department to another department internally, and it's a few days, and then back to this department for a few days, then out to the customer. We're trying to eliminate a lot of that. We've actually been able to do that.

And in the process, the very last statement there, develop the next generation of ARIN leaders, where we're really focused at ARIN, not just on my team but on all the teams, of really developing the talent that we have within ARIN so that the rest of us can go fishing some day, or golfing. I'll probably go golfing.

Okay, so the current CXO, the chief experience officer organization as it exists today, I am the CXO. Joe Westover is director of customer experience and strategy. Hollis is our director of communications. The newest team is the registry integrity and oversight, which is managed by Reese Radcliffe, who was sitting outside most of this -- he's in here now because I was going to talk about him.

Brad Gorman, director of customer technical services and our routing security senior product owner. And Lisa Liedel that everyone should know because she's the face of the Registration Services Department.

Going through it really quick, Registration Services Department, which Lisa runs, their main focus is taking care of our customers' requests and ensuring that our customers are getting the resources that they need to run their businesses.

A big part of that today, of course, is the transfers. Probably, geez, I don't know, 70, 80 percent of our ticket-transfer time is spent transferring resources.

I won't say NRPM again, though. The Number Resource Policy Manual 8.2, 8.3, 8.4 transfers. There's a lot of work behind all of that. It's getting better, though, and I'm going to show you that -- like I said, I promised to show you the stats in the next deck that I present, or maybe the next one after that.

Anyway, and to maintain data accuracy and provision of the ARIN registry by helping customers keep their accounts up to date, helping them to update their addresses and anything the customer needs to know.

They run a help desk that's 7 to 7 Monday through Friday Eastern time, 7 AM to 7:00 PM, so 12 hours every day of the week except the weekend.

They run a chat, the chat only runs from 10 AM to 4:00 p.m., so six hours a day. But they get a lot of people using the chat.

I know I prefer to chat if I have to talk to somebody that's providing me service. So it was a good feature. We rolled that out and then got a little bit impacted by the same reason we had to leave the office. But we continued doing all that and providing all those services.

And Lisa does an awesome job of running that department. I have to give her kudos where they're deserved. It's a tough job. I know because I had it at one time. And she does an excellent job at it.

Communications Department is run by the one and only Hollis Kara. She joined this group back in 2020. The Communications Department used to report to the COO, I believe, Richard.

But they did so much in conjunction with the customer-facing pieces of the organization that we felt it was a good idea to put them into the customer service organization.

They coordinate the biannual, the reason we're here. Hollis and her team do an excellent job of coordinating these Public Policy and member meetings.

Yeah, you'll see a hiccup now and then, but what you don't see is how smooth it runs 99 percent of the time. But that one hiccup will stand out. If you see a hiccup, let them know, but give them a break. Hollis is going to shoot me.

(Laughter.)

And a recent thing they've started doing is the training -- it's not recent. They've always done training but they've recently started using our own LMS system -- what's the name of it?

Hollis Kara: The vendor or the -- the vendor is [Tivuity]. The product will be ARIN Academy. I'll talk about that tomorrow.

John Sweeting: She's going to talk about our LMS system tomorrow, but they're doing that today.

Customer experience and strategy team is Joe Westover. Joe's not here -- he's here, but he's not here because he's watching probably from his room because he's been having some really bad back spasms since he got here, and he really can't get out of bed. We don't know how we're going to get him home.

But if you happen to see him, which I don't think you will, let him know you appreciate him.

He's done a lot on this team. His team has been put together since 2020. He has, I think, he has, like, five people in there. He does a lot of stuff. He's done all the work for the gathering all the statistics and everything so we could see how the services are used, how we could better serve the customers, what was the best way to do our fee harmonization, and then our resource harmonization and our membership harmonization. And all the things we've done over the last four or five years to coordinate the services and fees and everything so that all of our customers get the same value and understand how to interface and interact with ARIN.

Brad, as I said, is the customer technical services director. He takes care of all the routing security. And he's taken on more of the technical services, but his main focus has to remain on RPKI. They'll resolve all the security routing issues that anybody might have.

He's available, him and his team are available all the time. You can call the help desk. If you need Brad's team, they will transfer you over to Brad or Nathan or Jason to help you take care of whatever the issue is that you're facing.

He does lead the end-to-end planning and implementation for our routing security services. He sits and coordinates with the engineering team and with the community. He spend a lot of time with the community. He goes to NANOGs and he sits down with the community and listens to the services, the features that they feel are most important, and then he puts the priority on them. Then, as long as we get the okay from our president and CEO and the engineering team will do the development of those features and we'll roll them out.

I believe Brad's already showed you what's coming, so I won't spend any more time on that.

And the newest team, which is I think maybe two months old, is the registry, integrity and oversight team, which we fondly refer to as the RIOT team. Reese Radcliffe is the manager of that.

It's new and a lot if it -- it came down to, I didn't have enough time to follow and research and dig and find all the different ways that people were coming into ARIN and committing fraud. Registering companies in Wyoming with registered agents and using false names and registering 10 companies and getting their IPv6 and their 4.10 space, IPv4 transition space and going on the Wait List.

Then once they get everything, then kind of combining it all back in through 8.2s into one organization. And they never really were real people or real organizations. And it's a lot. It's very difficult. And Reese now has that task with the rest of his team, which consists of Jon Worley and Henry Romero.

Another thing they do is -- people alluded to the fact that 4.10, it's easy space to get one. If you have v6 you can get a /24 of IPv4 space and say, I'm going to use this for IPv6 transition. And we don't ask many questions on that first /24.

Policy says if you want another /24 for it, you have to show that you've been -- it has to be at least six months and you have to use at least 80 percent of that /24 for translation services.

We get a lot of people that -- a lot of requests for additional /24s of 4.10 space for a lot of different reasons. The biggest one is probably for MDN, multiple discrete networks. The claim there is I've got a server in LA. I've got a server in New York. I've

got a server in Miami. I need a /24 for each one of them to be able to do v6 there and have a translation service.

Of course, the community has told us for a while now that's not a valid multiple discrete network reason to have multiple /24s. So we don't approve those. But it takes a lot to convince people that they don't qualify under MDN for that 4.10 space.

And the other thing is that, like I said before, they will register several companies and get v6 and get a 4.10 /24 for each one of those.

We did have -- one of the ways we found this is we found the space being routed on a leasing platform that I won't mention, but we had very good cooperation from that operator. And as soon as we told them the problem, they blocked that whole /10 that we pull the space out for the 4.10 IPv6 transition.

We've had some really good wins in this team. Some of the external impact that you'll see, the whole expanding the general membership to include all of our members. So right now anybody that has an Internet Number Resource from ARIN -- be it ASN, IPv4, IPv6 -- and it's under an agreement, you're automatically a servicemember.

If you wish to be a general member and vote in the elections and participate in ARIN governance, all you have to do is click a box that says you want to be a general member, and you will become a general member, and you will have the right to vote in our elections.

You have to, of course, appoint a voting contact for your Org ID. But other than that, you are then qualified to vote. So that opened the door for anybody that wishes to participate in our elections and vote to do that.

Prior to making that change, it was only ISPs that got to vote. End users had no ability to participate in our elections.

We completed the fee harmonization across all resources and services. The last piece of that was the ASN, the Autonomous System Numbers part, which we now, if you look at our fee schedule, based on your resources held, you will pay either for your v4, your v6 or your AS numbers depending on which would be the highest fee.

For AS numbers, we follow the same pattern as the IPv4 and IPv6 -- four times the space or AS number, then double your fee. There's 3X small, 2X small, 3X smalls, 1, 2, 3 ASNs, 2X small is four to 15 and so on. And that's the way that goes. So it's

really fair to everybody. Everybody gets to pay the same fees for the resources they hold.

There was a really major effort when the Board announced that they were stopping the fee cap on IPv4 legacy for people that wanted to sign an LRSA. And the effort to get out to everyone that did not have space under an LRSA was a very huge effort. And they did it and they got it done and we ended up -- I believe we doubled the amount of LRSA holders from the date that that announcement was made to the date that the fee cap was finished.

So I think it was something -- it went from, like, 850 prior to, like, 1700 after.

We launched a few programs. The Premier Support Program, which I don't see on there, but the Qualified Facilitators Program. And we also cut processing time for transfer tickets by 60 percent, improving the customer experience.

Okay, internal efficiency and service improvements. Implemented the LMS system. Released the IRR auto manager. That was out of Brad and his team. Established a process and product development team under Joe's CXS team.

Basically that's, Marty and Reggie are part of that team, and they gather all the requirements for fixing ARIN Online and ticket flow and what you see there. And they gather those requirements and they write them up and they prioritize them and then they hand them off to our engineering team. Deb Martin takes them on from there and then they write stories for them by the way they're prioritized, and it gets done.

I feel it's really improved getting things done that need to get done for you, the customer.

Improved internal workflows. We did some work with RSD. Mainly our focus was on RSD, which is the Registration Services Department. We're currently focused on Financial Services Department, on their processes. What we did with RSD was Marty and Reggie sat with Lisa and Misuk and Eddie and the rest of the analysts and watched what they were doing and went and wrote playbooks for, okay, IPv4 requests, here's the playbook, to where it was consistent. These are the steps you take. And it was all documented and the teams now refer to that.

There was other things. We had a lot of cutting and pasting here and there. There were other systems that we had to use that we have replaced with systems that are

reachable through the ARIN Online management system that the team uses. And we're now looking at doing that with the Financial Services team.

And just better on-boarding. For membership and stuff, we have a better on-boarding process for the members and what they can expect from us.

All right. That's it. That's where we are today with the customer experience teams and how we support you.

Hollis Kara: Anybody got any questions for John, feel free to approach the mics or start typing. Look, it's Kevin.

Kevin Blumberg: Kevin Blumberg, The Wire. Is the little X a star, by the way? So it could be C-"anything"-O for you?

John Sweeting: Yes, it's everything. But I can't be the CEO, because we have a very good one.

Kevin Blumberg: That's reserved. Understood.

Thanks to many of the teams for really making things easier over the last two, three years, especially post-COVID. I cannot emphasize the automation steps that you've done with IRR, with RPKI, with a number of the systems that you put in place are invaluable.

The moment you remove out the need to have external consultants explain something to you because it's so easy to do, that's a step in the right direction. Please continue down where my job to provide consulting services to help people understand how ARIN works is a thing of the past. That would be a wonderful step, and you've definitely improved getting there. Thank you.

John Sweeting: Thank you, Kevin. And we attempt to do that, by the way. That's the one thing I really want to do is make sure that people can come to ARIN and do their thing. They can go to our webpage and they can say, oh, here's how I request IPv6, and, they can go on and step by step, boom, done.

And that's why we do over 40 outreach events every year, going out to different communities, the WISPAs, the FISPAs, the Internet2s, the CanWISP, the CANTO, CaribNOG, you name it, ChicagoNOG, NewYorkNOG AlbuquerqueNOG -- we go to a lot of places every year to make sure people know how to interact with us and take care of them.

Anything online?

Hollis Kara: Nothing online. Thank you, John. You're free for now.

(Applause.)

All right. Here we go. Next up, there he is, I'd like to invite up Reese Radcliffe, our manager of Registry Integrity and Oversight. I know John gave a brief overview of kind of the remit of his department, but he'll give you a little more insight, I think. Insight on oversight, or something.

Reese Radcliffe: Hi, I'm Reese Radcliffe. As John said, I manage the Registry Integrity and Oversight team. Love that acronym.

This is the agenda of what I'm going to talk to. But I'm not going to read the list for you. In essence, it's essentially what John brought up. We're basically going to address fraud, policy violations, and tell you what we're going to do about it, and just as important how you can help us do that.

So with the obvious lack of v4 resources out there, there's nonetheless still a demand for it, a big demand for it. And there are very creative and clever individuals out there who have identified various mechanisms and paths to circumvent policy or just outright do things that are wrong.

A lot of them John already brought up. People that don't even exist creating accounts, having an Org that's not eligible for more resources. So just create Org after Org after Org.

These are all things that we put in that category of not in the spirit of what we're here for and what we're good, and it's not good for the community. These are fraudulent activities and include hijacking and lots of other things.

So the question is, what are we going to do about it? This is important not just for us and trying to maintain the integrity of the database and the records we keep but to the community as well. Fraud and abuse affects everybody. It affects all of us.

These are resources that could be used by community members for genuine legitimate reasons, for building new business. These are resources that often end up getting dirty. And we have to clean them before they can be used again. I think it's in everybody's best interests to try to address this and do something about it.

That's the question. What are we doing about it? Well, fraud is something that ARIN has been dealing with for a long time. It's not like this is new. I will share that, from a fraud perspective, we do have fraud ticket-reporting process.

99 percent of those are not really fraud that's anything we can do about. We still go through every one of them every day. But "my boyfriend is hacking my phone" isn't really something we can do. Or "I looked it up and it looks like ARIN's in charge of 192.168.1.50, and somebody's hacking in my network." We can't do much about those, but we still hit them. We're talking about different kind of fraud, a lot of the ones that John brought up earlier.

What we have now is a dedicated team. It isn't something that everybody's doing in addition to their day job, like we have in the past. We have a focused team working on addressing this all day, every day. That would be my team.

One of the first things we did, there was a blog released back in February to address the Org Create front. So we eliminate things like RSAs being signed by people that don't actually exist. They're just really good at making up fake LinkedIn accounts and fake websites. And AI is certainly making all of this much more difficult.

So in the event we have an Org Create request come in, because that's the first domino to fall, and looking at that Org Create, it's flagged for one reason or another. Just as soon not share where that's coming from, but in the event it is flagged, we're going to require a Zoom call with whoever the ticket submitter is, and whoever is going to be signing the RSA.

I would say the overwhelming majority of customers we've talked to that we've had go through this have actually been very, very appreciative. The ones that don't never show up for the Zoom call.

So I would say we're already experiencing some degree of success because the bad guys aren't showing up. We don't have any numbers for that. Perhaps at the next ARIN meeting, we'll see.

So we've got the updated Org Create procedures. And that applies to more than that. That would be any organization because we still have legacy Orgs out there that aren't under an RSA. They're coming in to do a transfer, what have you. They're looking for more resources. We're doing them in those cases as well.

So this is specific to that agreement with ARIN to make sure that's with a real business and with a real person.

I think I hit some of these, but I can do it again. So we are -- actually the big part on this slide is that historically I'd say ARIN, from a fraud perspective, has largely taken a reactive approach. When things were brought to our attention, we jumped on it,

we took care of it. And when things were made aware to us, we acted. But there was minimal proactive fraud-detection policy violation actions being taken.

That's changed. That's changed as of the development of this department. We're now proactively going after, looking for policy violations, looking for fraud without it being reported to us. We're trying to find it ourselves. I would say that's the biggest one. This also applies to transfers that are taking place.

We work closely, our team, with Legal, with the CXO team, of course with Registration Services. I worked as a manager in RSD for Lisa for a number of years. And reading every single ticket, every single day gives you a unique perspective and visibility into the development of trends.

And I was able to see some trends on things that were happening, and we could easily collate some of this information, which we'd bring to John, who would say, "I don't have time for this." But he did and he worked on them to the point where it's so overwhelming. Again, now we've got a team doing that, trying to take some of that weight off of John's shoulders.

As I said, we are not just reactive but proactively looking for these things. The big message there at the top is the message we want to get across.

We're watching. We're out there looking now. We're not just reacting. We're seeking the bad actors that are out there, trying to do bad things for our community and the resources that we're so protective of.

Again, to reinforce, this is our effort and our commitment to the community to strengthen our trust and stability in the resources that we have, keep them clean to the extent possible. Make sure they're being used for what they're for, as businesses in the ARIN region try to expand in the ARIN region and do business in the ARIN region, not resources as a commodity.

Oh, one I needed to hit there. Yes, it will be on the next slide, too, but this is important. We're not doing this in a vacuum. We need your help. We need you to help us.

I know it's trite and cliché these days, but if you see something, say something. Let us know if you see something that looks like the resources that are not being used properly.

It's probably unusual to hear this, but believe it or not, some of the best tips that we get are from people that we have caught who narc on their friends.

(Laughter.)

It's like, damn, if I can't do it, I don't see why they should be allowed to do it. So we get some pretty good intel from the people that we're catching.

So as I said, here's some ways, other things you can do, other ways you can help us. If you see suspicious activity, please let us know. And we'll jump on it and look into it. If it's something we can do anything about, we will.

It would be best, of course, the rest of these are kind of SOP for everything with ARIN, but staying informed on the evolving process and procedures, like the blog on here; it's how we're doing Org Creates now, so it's not a surprise in the event you were come in and say, we need to have a Zoom call with you. You'll need to show us your government-issued photo ID and it better match what's in your profile because those are the new rules that we're playing by.

Keeping your contact information up to date, your Org ID information is up to date, not only is it something we will need in the very beginning when you're creating that Org ID and you might be on a Zoom call and you might have to show your ID.

That Org ID, I'm sorry, photo ID you're presenting, that government ID better match what's in your profile. That's not just to get your Org Create. It's important to keep that up to date because in the event you lose your phone, you've got to come in and get your MFA set up again. We're going to get you on a Zoom call for that, too, to make sure you're you. Nobody's trying to take over your account.

If you show an Org ID that says you live in Massachusetts and your profile says you live in California, it's going to be a little bit of an issue for us to verify that you are you. So keep your records up to date so that we can avoid things like Org recoveries.

I don't need to hit the last one, well, everybody here is engaging in consultations and community discussions.

So how do I get a hold of us? The same way you get a hold of pretty much anybody doing anything associated. You can call our help desk 7:00 to 7:00 Eastern, Monday through Friday. Just ask to speak to anybody on the RIOT team. Although that's kind of like an ASN number; that N is redundant -- RIOT team.

Anyway, you can call us, ask to speak to us. You can do that on chat as well. Although we won't discuss fraud things on chat, you can get in touch with us by pinging on chat, and somebody will get a hold of us.

Or the easiest thing, just open up an Ask ARIN ticket. It will get routed to us, and we'll jump on it right away.

That's all I've got.

Hollis Kara: Any questions for Reese, please feel free to approach the microphone or start typing.

John Sweeting: John Sweeting, chief experience officer with ARIN. I just want to emphasize the fact that this all came about from John and our Board saying, hey, we really need to get tough on data accuracy. That's our main purpose of existing is that we provide this accurate data to the world for them to make decisions on whether it's law enforcement, other networks or what have you.

Part of looking into data accuracy, we're, like, we can't really have accurate data if we don't know who the people are that are actually coming in and getting services from us.

So this is an offspring of that. It's been developing over time. This team, it's a small team right now.

The one thing I do like that they can do that was hard for us to do in the past because we didn't have dedicated people is Section 12s, which is, like, the best tool that ARIN has for detecting fraud and policy abuse.

So Reese and his team, they probably do a Section 12 Zoom call once a week.

Reese Radcliffe:At least.

John Sweeting: At least. I just wanted to emphasize everything that's being done to protect your data, your numbers.

People come into the registry, and they fake being T-Mobile, AT&T Comcast, all the big guys. It's hard to detect. We're doing everything we can and we're building some monitoring and detection into it. And Reese is probably manually doing it now, but he is watching for all these reassignments that happen to these companies that shouldn't be happening.

I just wanted to point that out and thank Reese for taking that job on.

Reese Radcliffe: Thank you, John. You brought up one other thing I wanted to hit real quick. When I was asking for your help to help us find some of these things -- we actually have a recent event where that occurred, where one of our

relatively large customers -- who I work with on a regular basis because they get things done to them like all the time and they work with us to get it fixed -- identified to us, without me going to them, they came to me and said, hey, listen, just want you to know we just had this issue with this address space. It's all cool. We took care of it.

But we noticed while we were in there all this other space they were doing to it as well. That belongs to this customer. You might want to jump on that. And we did. So that kind of information is really, really useful and will help us help you.

Hollis Kara: One question from the floor, one online. Let's take the question in the room first.

Atefah Mohseni: Atefah Mohseni, ARIN Fellow. Thanks for all the effort. I really appreciate it. The examples you shared seem mostly initiated by some actions that customers take, like creating a new organization or initiate a transfer. I'm curious if you also monitor some continuous fraudulent behavior like fake usage report.

Hollis Kara: Did you say fake usage report? Fake usage reports. Is there any falsification of that information, monitoring.

There is a data accuracy report coming, so we may cover it then. If we don't fully answer your question after that presentation, then we can definitely circle back.

All right. Online.

Beverly Hicks: Jason Cook, Dennis Group: "How will ARIN handle individuals whose preferred name may not match their legal names, particularly trans individuals?"

Reese Radcliffe: John?

John Sweeting: John Sweeting. We would deal with that when we had to deal with it. You can't say we would do it this way or that way because circumstances are always changing. We would never turn anybody away for anything like that.

Reese Radcliffe: The only thing I would add to that is, from the "your name needs to match your ID in the event you call in and we have to do the Zoom to make sure you're you," but that doesn't mean that in the event perhaps you're out of region and you have an English name in addition to your real name, it's not really that uncommon, we make notes about that.

You'll still need to show the ID that shows your real name and you're you. But we will have notes in there -- English name is John Smith or whatever. So to the extent possible, we accommodate those challenges.

Hollis Kara: I don't see any other questions. Thanks, Reese.

(Applause.)

We've got one more presentation before the break. John Sweeting, it's not 3:00 yet. I think you can do this. Or would you rather go to break and do it afterwards?

IPV4 TRANSFER SERVICE UPDATE

John Sweeting: I'm going to give another interesting topic that we don't get to share enough of because we really like, ARIN, we really like these spring meetings because we get to share a lot of what we're doing at ARIN.

And in the fall when we're having our elections, we have just barely enough time to fit in election information and policy information. So we don't get to do our department reports and tell you all the good stuff that's going on.

Here we go. IPv4 transfer services. Go.

All right. The agenda. I'm going to talk about overview trends, challenges improvements and community resources.

And everybody is thinking, what are those community resources. You'll find out.

So for the overview and the importance. So we have three types of transfers in the policy manual. And that is Section 8.2, which are mergers, acquisitions and reorganizations. And those are probably the most difficult ones, and you'll see why in a while.

8.3 and 8.4, they're really both the same, except for with 8.3, the source and the recipient are both in the ARIN region. With 8.4, it's one or the other. It's either the source or the recipient in the ARIN region. But pretty much the rules are all the same, or the policies, I should say.

Why do they matter? Well, they matter due to the exhaustion of IPv4. There's a lot of space, IPv4 space out there that's not being used that other people would love to use. And so the transfer market allows that to happen. We can take space from somewhere where it's not being used and get it to someone that does need it.

It supports continued growth and innovation. It's probably the only way you can grow an IPv4 network today is with addresses from the transfer market because we don't have a whole heck of a lot of them. So if you need a lot of IPs, you need to go to the transfer market to find them.

It promotes data accuracy because with legacy blocks especially, if somebody that is holding a legacy block and now they want to transfer them, first they've got to come in and update all their records so we know it's them and they're able to transfer them.

Then when they transfer them, whoever they transfer them to, it comes under a Registration Services Agreement and all the data is updated and accurate. And, of course, it facilitates the efficient utilization across the entire Internet community. The fact that we have inter-RIR transfers helps with that as well.

So the 8.4 transfer counts to and from ARIN, that is the inter-RIR transfers. This is the number of transfers -- not the number of IPs, but the number of transfers.

As you can see, 2024, there was an increase in transfers into into the ARIN region. Doesn't mean there was an increase of numbers, though, as you see here, the average /24s per 8.4 transfer.

When I first saw this, I'm asking my team, something's wrong here. It says 140. We had 129 transfers. You mean there was only one /24 per transfer? No the average for each one of those 129 transfers was 140 /24s. So big number of IPs are being transferred in inter-regional.

Okay. So transfer challenges. Common challenges faced by customers during 8.4 transfers, this is the inter-RIR transfers, is really the understanding of the policies and the delays between the different RIRs.

It takes some RIRs longer to process transfers, whether it's recipient or source, based on their policies and processes and everything.

And then we go into this email exchange between the registries. There's no automated platform or anything. Everything is done via email between the two participating registries.

So ARIN will send an email to RIPE, hey, we've got this source that says they're transferring this amount of space to this customer in your region. And then if that person hasn't already put it in, RIPE has to reach out to that customer, get them to put in a recipient.

And then the names don't match, so there's more emails going back and forth. It's a long tedious process. Lisa's shaking her head, yeah, it is.

So then the verification rights and authority. So all RIRs have a sanctions list. For us it's OFAC that we have to check. But then RIPE also has to do their check on sanctions lists so that they don't transfer something from a customer in the ARIN region that they shouldn't be doing business with. So a lot of that takes a lot of time. And the email process, of course.

So the challenges -- and then now for all transfers, not just the inter-RIR transfers, but a lot of times we get somebody who says, hey, I want to transfer these IPs to so and so. And there's nothing there. There's no documentation that we need.

So there's a lot of back and forth with the customer. The document delays, of course. They don't realize, oh, I have to have an asset purchase agreement to transfer these. So then they have to go to their legal department and try to find those documents.

It is very resource intensive processing transfers. Eligibility tracking is time-consuming. Yeah, verifying the block status. So we have policy that says, if you get a block off the IPv4 Waiting List, you cannot transfer it for five years.

So every transfer that comes in, a source transfer, we have to go in and look at the blocks and see where they were gotten from. Maybe they got them from a transfer. If they got them from a transfer, then there's a 12-month hold on them. And there's a bunch of different hold times depending on the circumstances which staff has to go through and verify.

And all of this, of course, a lot of it is manual processing. The tickets are in the ticketing system. But all the verification going to Secretary of State sites and all of that, that's all manual, outside of the management system.

So the improvements and enhancements that has taken place is ARIN has implemented improvements focusing, of course, on reducing the delays, helping people to understand what the requirements are.

I think one of my pet peeves and I think a lot of customers' pet peeves are, you put in a transfer and we have an analyst respond to you and say, hey, you didn't include this. So you find that and you attach it and you send it in. And then it's, like, okay, now we need this.

That is annoying. We have attempted to wipe that completely out. It will happen once in a while, but not too much anymore because we have that checklist that they go down to actually say, oh, I've got to do this and this. And they know what they have to put into the email and the documentation that they need depending on what kind of a transfer it is.

Another improvement is our qualify facilitator program. We find that transfers that are -- they're not submitted by, but submitted by customers that have a qualified facilitator working with them, wow, they open up the transfer request and everything is there that we need -- everything. And it's in really he nice order, and it's all documented. And it's, like, we even know which facilitator they're using based on the way they send in those first tickets. But it makes it go so much faster.

Of course, we talked about the outreach that we do and making people aware of the requirements and why they're the requirements.

We will have people that are so angry -- what's taken so long with my transfer? And they'll escalate. And I'll get on the phone and explain to them. And they'll go, oh, that all makes sense. Now we can go move forward. So we've been doing all that.

John wanted to make sure that we got this chart up here in front of you guys. 8.2 transfers have gone from 79 days meantime to resolve to 22 days.

So that's a 72 percent reduction in transfer times for 8.2s. 8.4s has been cut in half. That's your inter-RIRs, which is pretty good for the process that we have to follow to get through that.

And the 8.3s, 8.4s, they went down 35 percent. But notice that they were the fastest transfers that we processed. So there wasn't as much room for improvement as there was with the 8.2 transfers.

So we had so many 8.2 transfers. I asked for a report to be sent to me, a meta report to be pushed to me every week that would give me the list of all 8.2 transfers that had been 180 days or longer in existence and were still open.

As you can see, over 2021, there was average of 83 on every weekly report. Not always the same ones but you get the gist there. There was always a lot of tickets that were pending after 180 days.

Well, 2024, we knocked that down to an average of 18 tickets that were over 180 days at any one given time, a snapshot in time. The report I got this week, there was eight.

A lot of that is to the Registration Services team and the great job they're doing. And I have to give a shout out to Misuk Kwon. Since she has started reporting directly to me, her task was to make 8.2 transfers very efficient. And she's done a heck of a job on doing it.

But Lisa's team also, we've got some great team members on there that are getting the job done. So really that is a great job there.

(Applause.)

And ensuring a smooth transfer. We have this checklist now that we go down through and it helps us, of course, to make sure the customer has everything. We don't have to do the back and forth.

Somebody was asking, we do validate domains or email control because we do have, people know we have had a problem in the past with people finding domains that have expired. And they register them, and then they set up an email box that matches a POC that has gone away. And a year later they come in, they do a POC recovery.

Reese's team now does a lot of that. If it's suspicious-looking, we do that. We request the additional documentation and we do the Zoom calls. You know, if we're left with, we don't know who we're talking to, we have doubt about that, we'll ask them to get on a Zoom with us and provide that government photo ID.

Community resources, what are community resources? I told you nobody would guess that we would say that our qualified facilitators is a community resource that really helps get the transfer process done and done quickly and nicely.

They know what is expected. They know the documentation that's needed to prove who you are, how you came about getting the authorization to manage those IPs. And the ones we have are really good. We do a very good job of vetting them.

We do background checks. They sign nondisclosures. They sign, we get their first born children if they happen to have any coming. They do a great job.

We do a great job vetting them; they do a great job serving the community. It is a program that's paid a lot of dividends. And it's minimal to maintain once we got it set up. It was a little bit rocky getting it off the road, but once we got it going, it's worked very well.

So, again, you see this all the time. Support, you call the help desk 12 hours a day, Monday through Friday, 7:00 AM, 7:00 PM. Whoever you want to talk to in ARIN, you'll get transferred to them if they're available.

If not, they will always ask you for a phone number that they can give to the person you want to talk to and that person will call you back.

Of course, everybody knows, like most of us -- John, me, Richard, we're available all the time. We have people reaching out to us at all crazy hours of the day, weekend. It is part of the job and we just do it.

That's it.

Hollis Kara: Does anybody have any questions or comments for John?

John Sweeting: Mike.

Mike Burns: Mike Burns, IPTrading. You mentioned that checklist a couple of times. And Marty, our qualified facilitator and program leader, has mentioned it as well. Any idea when you might be able to give that checklist to the qualified facilitators?

John Sweeting: Sure, you'll have it tomorrow.

Mike Burns: All right, good. Makes our submissions even better.

Kevin Blumberg: Kevin Blumberg, The Wire. Last week -- this is tax time, by the way, in Canada, so why you see all the Canadians a little unhappy.

Last week my kids needed to sign into the government website. They took their ID, and there's a special verification service, third-party. It wasn't the government. It was a third-party service that took that information, verified it right then and there. Took a picture of them to make sure they were the person, all of that.

I don't trust deep fake on Zoom and any of these technologies anymore, John. I'm sorry. You can't tell if somebody is giving you the card that they used in their bar days or whatever.

Use a verification service. If a verification service doesn't exist in the country you're doing, yes, go to some manual other process. But --

John Sweeting: That is the next step where we're going. Right now, the Zoom is the easiest we could -- and it is good. And, as I think Reese pointed out, the best thing with Zoom is most of them, if they're fakes they won't even show up and they just go away and close their tickets.

But, yeah, that's part of Reese's mandate.

Kevin Blumberg: As long as what you're saying works until somebody with charisma comes along --

John Sweeting: Part of Reese's mandate is to find these verification tools like you're talking about and other things. We're looking at integrating an API with post office to check that postal addresses are correct and all that. So there's a lot going on.

We now have a team that's dedicated to doing that. I love the suggestion. And thank you for it.

Tina Morris: Tina Morris, AWS. Wanted to say thank you for the facilitator program. Although I don't necessarily need it, I'm glad it exists for others that are not as well versed as I am for the market. It's been a really positive improvement.

However, I do want to bring to light that there is a link on that page that you can report bad behavior by any broker, not just the ones on that list.

I would encourage people to do as there are some entities that are not acting properly. And I would also encourage you to expand your code of conduct to include contact to nonclients prior.

John Sweeting: Thank you, Tina. Good suggestion.

Paulius Judickas: Paulius Judickas, IPXO. Are there any plans in ARIN to work on and introduce them per transfers?

John Sweeting: That policy has not been submitted here. It's been submitted everywhere else. I'm pretty sure it has not been submitted here. There is nothing planned by ARIN.

ARIN community is the ones that put in policy proposals. I do know it did get discussed on the PPML as an idea, and it was pretty thoroughly shot down, like, why do you need temporary transfers when you have reallocations and reassignments?

Of course, one of those is, if you reallocate something to someone, they can't do their own RPKI.

We're working on that. Brad's got a task from John to make it where those people that get reallocations can do their own RPKI. And that would solve that problem, but there has not been a policy submitted, no.

Paulius Judickas: Understood, thanks.

Mustapha Nasomah: Mustapha Nasomah, an ARIN Fellow and a student of the University of Cincinnati. Incredible job with the reduction in transfer duration. But my question --

John Sweeting: It wasn't me. It was the ARIN team. It was RSD and everybody else, but thank you for that.

Mustapha Nasomah: He's right for asking you to add.

John Sweeting: And that guy over there deserves a lot of credit. He's the one we all want to make happy. If he's happy, the community's happy because --

Mustapha Nasomah: So the question is are there any limits on the measure or the transfer, any limits on the IP transfer or measure? Is there any limits on the number of blocks you can sell for transfer or measure?

John Sweeting: How many you can source? How many you can sell off? It's whatever you have authority over.

To receive, you have to have an approval. You can get a preapproval so that it makes it easier, which is one of the tips I'm sure the facilitators tell -- oh, you want to buy space, you need to get preapproved.

If you got preapproved for a 16, you could transfer a /20, and we would take that away from the 16 and you'd still -- you could transfer all the way up until you got that full 16. It doesn't have to be the 16 at one time.

Or you can just put it in and then provide your justification, your needs during the process. But that slows it down a little bit.

Mustapha Nasomah: That answers my question.

Jake Brander: Hello, John. Jake with Brander Group. Tina mentioned an interesting point, improper conduct by brokers. Is there a definition of that, something we can actually reference so we can ensure not to do those things?

John Sweeting: You should have it in your letter that tells you what is not acceptable.

Jake Brander: Outside of that.

John Sweeting: John wants to address this.

John Curran: One of the reasons we did the Qualified Facilitator Program is because that has a code of conduct. That has specific requirements when you're a qualified facilitator. You have to adhere to those requirements once you're accepted and maintain that.

So it's in the program. You can go to the website and find it.

If you're not a qualified facilitator, while you haven't agreed to that, but if someone complains to us, we're certainly going to pay attention to someone out there doing a bad job as a broker.

But the code of conduct of the Qualified Facilitator Program is what primarily we're expecting people to report violations of.

Jake Brander: Is that code of conduct made public to everybody else or just the brokers?

John Curran: It's public on the website by the application.

John Sweeting: Yes, it is public. It is posted on the website, as John had already confirmed. I wasn't sure. I was pretty sure but I don't want to be saying something -- Bev.

Beverly Hicks: Actually not me. Mohibul Mahmud: "Thank you for detailed overview on the IPv4 transfer services and the improvements that have been made. You mentioned a lot of current transfer verification work, like checking the Secretary of State documents, et cetera, is very largely manual. Given the significant reduction in transfer processes already achieved, are there any future plans to further automate parts of that manual process?"

John Sweeting: Absolutely. That is, the customer experience overall team, that is their job to look for improvements and efficiencies to be gained every day that they go to work and look at things. There's so much going on on that team, I can't even tell you.

Hollis Kara: Awesome.

John Sweeting: There's not enough time. And it's almost break time.

Hollis Kara: It is break time. Are you done?

John Sweeting: I'm done. Are we done? We're done.

Hollis Kara: We're done.

(Applause.)

Or rather, I should say done-ish. We have a few more presentations after the break and before Open Microphone. If I could please have folks back in the room at 3:30, that would be great.

There are Moon Pies and pimento cheese outside. I don't suggest you eating them together, but you do you.

(Laughter.)

[[Break taken]]

.....

Hollis Kara: John, come on up. Next up, we've got an update on ARIN agreements from John Sweeting.

John Sweeting: This used to say "Joe Westover," but as I informed you earlier Joe is not down here. But he is here.

So we wanted to give you an update on ARIN agreements because there's been a lot of changes over the last several years and more in the last four years. There's been a lot.

The LRSA was updated. The RSA was updated. The LRSA fee cap was stopped, and the LRSA has now gone away. You can't get an LRSA.

However your legacy, if you have legacy resources they are protected in language that's in the RSA. That's actually been a while. People just never really understood that, but I could get Michael up here to explain it, but I don't see him in the room.

Okay. History of resources. So everybody knows, Internet protocol address space, Jon Postel was the administrator out of IANA, and early on the Internet Number Resources or any organization that filled out the simple request that he had and they had a good reason -- and remember it was, when he first started doing this it was classful, so if you said you had 257 host addresses that you needed, you got a Class B, which was a /16. If you had over I think 66,000 IPs, then you got a Class A, which is a /8.

A lot of that space was given out during that period and tracked by Jon and his little black book. And then it eventually got onto a database. And eventually it got turned

over to -- Network Solutions did it for a while. And then ARIN came about out of that in 1997.

As a matter of fact, I think -- ARIN was formed in 1997. And ARIN was tasked with the administration and management of the entire database of IPv4 addresses and autonomous systems that were not administered by either -- that's a little bit misleading because it was only the IPv4 addresses that had been allocated out of IANA.

IANA still had a bunch of IP address space that ARIN wasn't responsible for. But all the space that had been given out from IANA at that time, ARIN took over the administration of it except for those that were specifically being administered by RIPE and APNIC.

We had part of Africa. We had South America, Latin America, the Caribbean and, of course, those resources prior to ARIN are usually referred to as Legacy Number Resources.

We at ARIN, internally we try not to use that term anymore. We talk about Number Resources under agreement or not under agreement. And legacy resources are not under agreement -- the only resources that are not under agreement are what are referred to as legacy resources.

At that time the Board of Trustees, the ARIN Board of Trustees decided ARIN would provide the Registration Services services for those legacy numbers that were available at that time. So basically reverse DNS, updating your information, changing POCs, transfers, M&A transfers and the like -- without paying any fees. So they were grandfathered the rights of using the ARIN -- of ARIN maintaining their entries in the Whois database.

So the timeline of legacy resources, in October 2007, ARIN began offering the LRSA, Legacy Registrations Services Agreement, which was associated with a fee cap.

I believe John was the chair of the Board at that time and had a lot to do with trying -- it was the attempt to try to get legacy resources under an agreement. Of course that helps data accuracy and all the other good things that come about from that. It hadn't been working. Nobody had been really signing up.

That's how the fee cap came into place. Let's incentivise them into signing the agreement. There was a big signing, like I think it was about 300, a little more than 300 that signed it. And then it dwindled off and there was like 10 or 12 a year.

In January 2022, ARIN's fee harmonization -- the fee harmonization was initiated, which transitioned end-user customers and ASNs to the Registration Services Plan fee schedule. Then in 2023 ARIN announced the legacy fee cap would be retired at the end of 2023, which actually dragged out to the end of 2024 because anybody that initiated a ticket in 2023, we allowed them time to get the documentation and everything they needed to be able to sign an agreement and transition into that agreement.

A lot of people took a lot longer than we thought it would take. So midway through 2024, the Board said, you know, like, if it's not done by the end of 2024, then those tickets get closed. We didn't have very many pending at that time, but there were a few. And that's what that last bullet talks about.

Ongoing legacy resource requests. Throughout 2024, we continued to work with organizations that initiated the process. It's kind of what I just said. We worked with them as long as they initiated it before the end of 2023.

And they were still able to -- and we're still able to assist legacy resource holders. The thing is they have to sign a regular RSA which has protections for their legacy resources in it, but the normal fee schedule is applied.

So here's the difference of having an agreement and not having an agreement. That's why we don't refer to legacy anymore. We refer to resources with an ARIN agreement and without an ARIN agreement. And if you have an ARIN agreement you can maintain unique registration -- let's just talk about the things you can't do if you don't have an agreement.

You can't do RPKI. You cannot do Authenticated Internet Routing Registry. Otherwise, you can do anything else with or without an agreement.

Unfortunately the big thing everybody wants to do today is RPKI. So there is still a lot of people that are working to get the documentation they need to fall under an agreement, and they don't really it's not really concerning to them what they pay for the fees they need to do RPKI and they know they need to do it. So they work with us to sign that agreement.

[DAN STOPPED] benefits of the ARIN agreement. Confirms your rights to IP Number Resources enables access to ARIN's full suite of services and support. Michael always likes to say why would you want these resources that are worth so much not to be under an agreement without the agreement. We could really take them away anytime we felt we needed to.

That's not really true, but in the legal world, if you don't have an agreement or a contract, you're really not taking the care to protect those resources that you could take.

It does enable you to become a servicemember and participate in ARIN governance and elections and it provides access, big thing, provides access to the routing security tools, RPKI and IRR. And the voting and being part of the elections is actually a big thing that people really like to sign the agreement for.

So key changes to the legacy resource agreements. LRSA version 3.0 in 2011, that just clarified the ambiguous language that was in the earlier versions.

I believe that was the first one that was the same as the RSA, same language as the RSA but we still called it RSA and LRSA. And then there was updates in 2022. As we got closer to RPKI and people not being able to do that, Michael and his team, our general counsel, Michael Abejuela, and his team and, of course, John Curran and the Board spent a lot of time looking at the language in the agreement.

So there were changes that were made, significant change in 2022 was the got rid of the no property rights because that was a sticking point for a lot of legacy holders that we were telling them they had no property rights. That was changed to acknowledge rights to included Number Resources. It helped with some people. It didn't help with all of them. So March 2023, there was -- we announced the deprecation of the LRSA and the associated fee cap.

Again, we did honor requests that were submitted prior to December 31st, 2023 to complete them as long as we could complete them before December 31st, 2024.

Oh, so here's the one I was talking -- I think I said like 850 to 1700, but it was actually 984 legacy resource services agreements -- Legacy Registration Services Agreement signed before September 2022 and then from 2022 to today, it doubled. Not quite doubled but you get the gist. It was almost doubled, which is a big thing.

We got all of that, the 885 of them in two years and it took like from 27 -- 15 years to get the first 985.

So that's it. Thanks what we have for the agreements status. So today the status of ARIN agreements are there is one. There is only an RSA. However, it does provide you the protection for your legacy resources in there. And that's it. No LRSA available anymore. And Kevin, come on up.

(Laughter.)

Kevin Blumberg: Kevin Blumberg, The Wire. Two questions. First question is, under no agreement are they still paying the yearly legacy rates that were there before, or they have zeroed out now.

John Sweeting: If you have an LRSA and a dash Z account which signifies LRSA with fee cap.

Kevin Blumberg: I'm talking about those that have not signed an LRSA.

John Curran: Your question is the annual maintenance fee for the record it was only paid by people under agreement if you didn't under agreement you're a contractor with no fee and same services you had in 1997 plus whatever development we've done since. So you have the same services that you had before ARIN was formed only you can also use ARIN Online and you can have DNSSEC. But you're still not paying and you're still not under contract.

Kevin Blumberg: Thank you. So the people that are left that have not signed an LRSA or RSA are reaping the benefit from the community with zero dollars to the organization?

John Curran: That's correct. They have a subset of services. We spent a lot more time invested doing authenticated IRR and RPKI, a huge amount of your resources, and so it was felt, look, if you're really going to benefit from those, you should step up and have an agreement just like everyone else, pay the same fees as everyone else.

Kevin Blumberg: Thank you. Are these noncontracted parties allowed to do SWIPing?

John Sweeting: Yes, because everything in the ARIN database is allocated today. They can do reallocations or reassignments.

Kevin Blumberg: Right. They get the benefit of another feature of the database which is assignments new Orgs have to be created to allow those assignments and things like that.

John Sweeting: Yes. But that was something that was available at the time ARIN was created.

John Curran: SWIP is very old.

Kevin Blumberg: Understood. Understood. But there's validation at work that is required on a new Org ID they would need to be going into, just again I think --

John Sweeting: We do have an Org Create fee today.

Kevin Blumberg: That's fine.

John Sweeting: For what that's worth. It's $50, I believe.

Kevin Blumberg: Last part, APNIC did a presentation earlier where they basically said get into contract or your space is now basically going back to the free pool. I'm not suggesting that for the ARIN region but to your slide you don't have any contract and you don't have anything and this is good for everybody, it may be worth to point out that in the other regions they have made the decision after 25 years to finally deal with this issue rather than keeping it under noncontract and not anything. So that's just sort of an opportunity while you're not --

John Sweeting: Believe me we do know that. John will take this one.

John Curran: When ARIN was formed in 1997, 100 percent of the space assigned before our formation, 100 percent of the space in the registry was legacy holders because the day we were formed we had no contracts, no customers.

And so we started assigning, and over time the amount of space in the full registry has gone from 100 percent legacy at the date of our formation to a smaller and smaller and smaller number.

If we went back five and a half years, it was -- we had some 60 percent of the registry was under contract, 40 percent was not.

Today, 26 and a half percent of the registry is not under contract. Uncontracted legacy holders, 26.5 percent. It's dropping. It's a chart that shows up every quarter on my desk in front of the Board. This is a problem that will, over time, get smaller and smaller. I'll never say go to zero, just like v4 won't go to zero even if v6 is really popular. But it will get smaller and smaller.

Your question is whether or not it's worth going and telling these people, okay, now you have to get an agreement and you have to be contracted or we'll take your space back?

Kevin Blumberg: No it is not exactly. I don't believe it is in our region necessarily today a worthwhile endeavor there are complexities I understand in this region I'm

saying I understand other regions have done this maybe at some point in time the community may change its mind good point for people.

John Curran: That's excellent because if you were heading towards time to take it back I was going to have to explain some details. But let me go to one thing. The people who aren't under agreement actually probably a lot of them probably don't have a problem with our fees, even our full fee schedule.

The challenge is that even though we've done a lot to make the agreement more palatable, if you enter an RSA agreement with ARIN, the only way you leave the agreement voluntarily or to return resources or if we fail you there's a judgment or arbitration that says that. So you walk through the door. It closes behind you. You're a member of this great community, just like every other member of this community, but you can't undo that ever.

Now, for a lot of people they look at and go I want to be a part of this community. I want to vote. I I want to do that. I realize this community has been the instantiation of the mutual cooperation of all these people and I want to be part of that cooperation.

It's not like you can voluntary say I don't want to cooperate next week, you are whether you know it or not you're cooperating to make the Internet run.

If you think you have property rights and you have to ability for independent agreement, when you sign the agreement you're incumbered, you don't have the right to use them independently. It's not lost on the staff or ARIN Board. It comes now and again in discussions with people who don't have an agreement with us, obviously.

There's groups that are particularly disadvantaged by this if you look at the education community that have address resources from pre-ARIN, large groups that are impacted. This is not the final chapter, necessarily. We're still looking at what can be done. But there's also a fairness question. Okay. There's people who have signed the agreement because they wanted the benefit and now if you suddenly look at legacy holders and say, well, in order to get you in, we need a two-way door, what do you do for every legacy Org signed before do you have to give it to them in fairness too. There are some questions which need to be grappled address the last segment that hasn't come under agreement. This is, by the way, every year we have Board elections. If you run for the ARIN Board this will occupy some amount of their mind space every year you can weigh in on these issues too. It's an open topic. I

want to say it's not that we've forgotten about them. We're just trying to deal very fairly with them and recognize that the concern they have is a real concern. It's based on a different set of assumptions than being part of a community but that doesn't make it any less real.

Kevin Blumberg: Anything you can do to help bring them into having RPKI and IRR is appreciated. Whatever that may be. I understand there's a lot of complexity to this. The ultimate goal is that they're part of the Internet community of 2025 and are not stuck on the Internet community of 1997. So by all means. Anything you can do to support that without getting into complexities or specifics, I think the community would appreciate as a whole.

John Curran: If you're on the ARIN Board of Trustees and you're in the room, could you raise your hand. If you have views on the particular topic and tradeoffs involved find those people discuss it with them. This is an active topic.

Kevin Blumberg: Last question you have the one slide the one statistic I'm interested in of the 1780 how many of them got the LRSA signed so they could then transfer the space out as in how many of them today of those 1780 actually have active resources anymore because the sole reason they signed it was then to do an 8 point X transfer.

John Sweeting: Those are numbers as of today. It does happen. Not a lot.

Kevin Blumberg: But a good thing I was curious how many actually --

John Curran: When someone does do that they're no longer a member or no longer LRSA if they transferred out entirety. I don't know if that stat removes that count. I'll find out.

Kevin Blumberg: That was the question.

John Sweeting: It's not very many.

Mike Burns: Mike Burns, IPTrading. Two questions, I don't think a legacy RSA have has to transfer out of region.

John Sweeting: That's correct.

Burns:

John Sweeting: As long as they're the official organization that was issued those addresses. So if it's the same company in 1993 today -- the company in 1993 is still the same exact company with no name changes and all that other stuff, they're good. We know who they are. They have the right to transfer them and we don't make them sign an agreement just to transfer them.

Burns: Correct.

John Curran: But, but you may have to sign depending on the transfer and the paperwork involved. You may have to sign a piece of paper that offers similar things to ARIN like an indemnification even if it's not a full Registration Services Agreement.

John Sweeting: They have to sign the officer acknowledgment which has it all in there.

Tim burns: My second question says legacy RSA protects the rights within the single RSA.

John Sweeting: Where is Michael. John could maybe answer it but Michael could answer it.

Tim burns: I haven't asked yet. I have two questions. One, what are those protections? And number two, if a legacy holder signed an RSA with legacy protections, could he transfer the block to RIPE as legacy?

John Sweeting: It's not our decision. It's RIPE's decision -- no, now today, no. Only if they're in a dash Z account. Today they come under a Registration Services Agreement, we would tell RIPE they're not legacy, they're not considered legacy any longer.

Mike Burns: Yes.

John Curran: Recognize ARIN recognizes legacy status as being an address block held by the original registrant or legal successor. It is a status of the block and the party holding it. It's not some magical we don't paint the block orange and it's radioactive as it flows through the registry system. It's only saying you were issued, you or your legal predecessor were issued this block. So we're willing at ARIN here we're the ones who kind of created the legacy status, we're willing to extend the same basing uncontracted services without fees to you. I don't know what the meaning is at other RIRs because if you transfer to another RIR and it's not the legal successor, I don't know what credit they're extending or why. You have to ask that question to them.

We would say you've signed an agreement, you're paying fees, you're just like any other member.

Mike Burns: Correct. My point was going back to your discussion about a one-way trip and the way it works with RIPE is if the addresses are legacy in ARIN, you have the option of registering them as legacy in RIPE.

John Curran: Even if you're not the legal successor entity.

Mike Burns: Right.

John Curran: We're extending to the same party who got the block free services because they existed at the time we formed. RIPE is extending a different benefit under different terms.

>> Mike Burns: They call it legacy I know you don't like to call it legacy. But they basically give you that option if they're legacy in ARIN. So my question was whether the protections afforded in the RSA.

John Sweeting: Today, if somebody with legacy resources wanted to come under an agreement to get all those other services, they would sign an RSA which terminates the legacy status.

Mike Burns: You said there was protection.

John Sweeting: If takes it back not under agreement.

John Curran: Legacy holders by the agreement have different language in the termination, slightly different. That has to do with the status with ARIN.

Mike Burns: The protection is --

John Curran: That's in the standard agreement for everyone.

Mike Burns: But the legacy holders, their protection is different termination options?

John Curran: No it's now --

John Sweeting: Goes back to current status. Current status they got from ARIN the current status would be with ARIN.

John Curran: Again legacy status says you were receiving services when we were formed and we'll continue to give you those basic services that's all it means.

Tim burns: The issue here is that the treatment of legacy resources is different in RIPE and in RIPE, for example, legacy holders can do RPKI, and I'm not sure, but I think Kevin was making a plea to offer something similar in ARIN that would allow legacy holders to do RPKI.

In RIPE, they can sign an agreement which is voidable that allows them to do RPKI I think if something was available like that in ARIN you might see more.

Tina Morris: I was going to say that in RIPE you have to sign an agreement to do --

Hollis Kara: Can I get name and affiliation for the transcript, please?

Mike Burns: In RIPE you can sign --

Tina Morris: This is not RIPE.

Mike Burns: I know it's not RIPE. It's legacy. The point I was just saying if we want to incentivise more legacy holders in ARIN to do RPKI, maybe making it not a one-way street is the way to do that.

John Sweeting: Kevin, could you let sander.

Kevin Blumberg: I was going to directly respond because words were put in my mouth.

Mike Burns: I said I wasn't sure.

Kevin Blumberg: I'll respond directly. Kevin Blumberg I was not saying noncontracted with whatever means possible but that did not imply not having some form of contract or agreement with that holder.

Mike Burns: Neither did I.

Kevin Blumberg: I brought up the issue with the APNIC region where they unilaterally got rid of and to compare any one region to another where they could change their mind at any one time I think is a little disingenuous.

Mike Burns: My only point was that you mentioned one way street aspect of signing an RSA. And that might be something that prevents legacy holders from engaging in it and therefore preventing them from doing RPKI.

I was simply pointing out that other registries have other ways to allow legacy holders to do RPKI. It does involve a contract but it's not a one-way contract.

John Curran: I'm very aware of that. Other registries have different approaches. As Kevin said some will reclaim the space. There's a lot of options. I would say find a trustee, propose what you're talking about. This is an open topic.

Mike Burns: That's fine. I understand. I could propose a contract like that.

Sander RIPE NCC executive Board just a small clarification. Like you said we treat legacy in a bit different way. For those who don't have a contract, we provide the basic services like John said, but also no RPKI.

The difference is we have several ways of getting a contract with RIPE NCC directly or indirectly. But, yeah, there definitely needs to be a contract because you're writing -- at the stage with a certificate and we can't issue a certificate with somebody we don't have a relationship with.

John Sweeting: Right. Thank you. Michael, you never even had to get in there.

Michael Abejuela: I was ready.

John Curran: Michael does all the hard work. I get to talk to it. Great relation.

John Sweeting: That's it, Hollis.

Hollis Kara: That's it. You're done, John.

(Applause.)

And now on to our next topic. Brad Gorman, director of customer technical services come up and talk to us about data accuracy in the ARIN registry.

Brad Gorman: To be light for a minute I'd like to challenge the attendees at the meeting today present and online to tell me by sending me an email this jacket has made three appearances on stage including this one. Two of them have been me. If you name the third person who wore this jacket on stage, send an email to routing.security@ARIN.net and you could have one-on-one free routing security advice from me.

(Laughter.)

So get back to the real reason we're here. So this morning things were about security this afternoon a lot of the discussion has been about accuracy. To the point

ARIN is trying to do our best to look at information at our registry to be the most accurate and useful and worthwhile for the entire community.

To that point, we have established and we're starting a new program that is focused on data accuracy in the ARIN registry. I'll just go ahead and jump in. Three main points. Three main points that I'm making here. The data is important. It's important that it's accurate. I'm going to go over what our plan is, what our current state and where we're going and then how do we make it easy to maintain the registry information moving into the future.

So the accuracy. What does it mean that ARIN -- that we're committed to ensuring that we get the most accurate data in our registry. Fundamentally that's what ARIN's primary purpose is, maintaining an accurate registry for the resources that we maintain.

And providing that accurate information it makes it useful for organizations that rely on that accuracy component to be there, and we know that it is an uphill battle to get this done.

To that point, again, we've created a project and we have a team of individuals across different departments inside of ARIN that are going to be focused on doing this starting now and moving forward into the future.

Why with is it important to have accurate data? It ensures the operability and stability of the Internet, what does that mean? Well, the Whois and RDAP services that we provide are an integral piece of what network operators need to really do business.

The operator community needs it to be up to date so that they can be confident that information is there and it has been entered by the people who are the authorized holders of those resources.

It will help the resource holders to close some of the attack surface and keep your resources more secure. If you make accurate statements about your resources and your contact information and how you want it to be presented to the outside world, this is your part. This is your way of making sure that the accurate information is used appropriately by the community.

And of the broader community, there are multiple users of this data. There are again network operators or organizations that perform anti-abuse or law enforcement,

cybersecurity teams, researchers. They all rely on this active registry, the accuracy in the registry to report clean and correct data.

So what are the tenets of what this team is? We are looking to validate and make sure that there's correct information. We are coming to the community in many different ways starting with this meeting here, making sure that everybody's aware that accuracy is a two-way street. We are going to take our efforts into doing it but resource holders need to take their own effort and do it.

And then we will be actively engaging the community in order to bring the level of understanding and make sure that the registry is as accurate as we can get it. So here are the three main initiatives. We want to validate the data. We want to correct data that may be inaccurate. And we want to make sure that it is quality information that is useful. What is that? Maybe a contact information is more than just a phone number, 800-555-1234. This is again getting us to a point where we want to have the best possible information available to everyone to use it by maintaining, again, a clean and accurate registry.

How do we define it? There's three main criteria. If information is complete, it means all the fields are filled. Information that's correct is information that has been vetted and validated by ARIN or people inside of ARIN.

And current is information that has been validated within the last five years. So that's moving forward that's the definitions that we're going to use on what is complete, correct and current.

The current validation process is in the policy manual in Section 3.6. And it clearly states that points of contact, these are admin, tech, NOC, abuse points of contact, need to verify information, their contact information so that it is, again, freely available for use and it is in the policy, it's a requirement of you, the points of contact for those organizations.

Annually we will send emails to verify your information. If those emails have fallen on deaf ears after 60 days, we will go back, attempt final communication, and then say, hey, we want to make sure these records are valid. Otherwise, you know, it's not useful. So what ends up happening is those points of contact will end up becoming an orphan. An orphan Org ID is an organization that has no Number Resources associated with it. It's out there in existence, maybe transferred out a long time ago, but clearly orphan floating in space.

A Point of Contact is orphaned for one of these three potential reasons. One, it's not associated with any resource numbers. It's not a resource POC. It's not connected to an organization with resources.

Or it's associated with an organization that's been orphaned. So this is how we are identifying the first steps and first stages of incomplete or inaccurate data within this program that we're running.

Our ultimate initiative, ultimate cleanup, is to get rid of orphaned organizations, orphaned users, cleaning up this data so that we're bite by bite getting towards the most accurate registry information we can.

So where are we now and what's the direction that we're taking? Along with the new initiatives, specifically again forming this team and this project, more active communication to the outside world, more reachout. What you're going to see maybe direct communication to an email that's live, hey, that's great, if you have an email that's responding or still, you know you're related to an old resource or an old organization, that's fantastic.

Check those old emails, too. Check those old points of contact. It's very possible that things have been forgotten long into the distant past. We are trying our best to get to everybody.

So reach back into the way-back machine and check these messages. Talking about the charts here, over the last five years, currently what we've seen so far today, the numbers haven't really moved that much.

What our goal is to make these numbers move. This is why we are doing this, this is why we've undertaken this project.

It is the 3Cs. What are the three Cs? So it's here -- now I left the presentation.

Hollis Kara: What did you do?

(Laughter.)

The complete, correct and accurate, those are the three bars that are here -- current. And clearly we now want to bring these numbers down arguably, we want these numbers to go down for ones that are not under agreement, bring the numbers up that are.

How do you help? It's pretty straightforward. Recognize that being that it is your responsibility, go and validate your contact information. Go and validate the

messages that you have received from ARIN to say, please, we're trying to do our part to make sure data is right. Please do your part. And it's in policy that you need to do your part.

So another thing, when we do reach out, respond back quickly. If you have a question, always reach out to the Registration Services Department, open a help ticket, we're all here to help.

So if there's any confusion, anything like that, we all want to get to the same end goal of being as accurate as we possibly can.

What are we trying to do moving forward? We're trying to explore newer avenues and newer ways of helping the validation. If there's a new way, a new protocol to reach out to the information and pull it into more useful format. Are there other potential new tools? This is the future. We're thinking whether it will be a new standard or new method with which we offer access to the information. These are what we're looking for. This is what we're trying to do. And again take your suggestions on what would be helpful.

This is a joint effort here. That's it.

Hollis Kara: If anybody has any questions or comments for Brad, now would be the time to approach the microphones or start typing.

Leif Sawyer: Leif Sawyer, GCI Communications. You had a note on the slide about RWhois and RDAP. Back at the beginning. Right there. It says that they are an integral resource for the operator community. And they are for my company. We publish all of our resources via referral Whois and we have a bunch of automated processes for that.

So, yes, definitely integral. But that statement seems to be in conflict with what Mark Kosters' presentation earlier said, which says we're getting rid of those.

So getting rid of an integral resource seems to be a bad thing.

John Sweeting: John Sweeting, customer service officer we'll not get rid of anything that's integral until we have provided a substitute that is acceptable to the community to replace that integral part that may have to go away just because it's no longer like is not able to be kept up based on technology and other things.

But I assure you, I hear every day, we will never get rid of anything that will hurt our customers without first giving them something to replace it.

Leif Sawyer: Thank you.

Brad Gorman: Couldn't have said it better myself, John. Thank you.

Hollis Kara: Anything else for Brad? Nope, nothing online, nothing else in the room. All right. Thank you, Brad.

(Applause.)

All right. Look this one changed. For this next presentation, I'll be playing the role of Joe Westover he's on line. So if everybody could just say hi, Joe.

>> Hi, Joe.

Hollis Kara: Thanks. We're going to do something a little different here. We're mixing it up I'd like to invite a few of my colleagues from government affairs to come join me up on stage for our first inaugural game of duck duck goose at an ARIN meeting. Not really. Leslie, Bevil, Nate, if you'd come on down.

This is kind of funny, when this presentation was being prepared and I was looking through it with Joe, it was like, dude, we do a lot of that. He's like I know it's cooperative effort. You're right it all is. What I'd like to take a few minutes give an overview of ARIN's overall strategy outreach for the year. I'll kick it over to some of the no objection that have a more specialized audience to talk a little bit more how that fits in with the work that they're doing.

So everybody got it? Got it. Good. Here we go. All right. Look, see I'm playing Joe.

All right. Why does it matter that we do outreach? Why is outreach we talk about so much. It's how we help you as customers understand what we can provide. It's how we educate you about the tools and programs. It's how we build trust. It's about how we build relationships and it's a way can promote and build our services and programs gets you more involved you get to talk to us those folks are cool maybe I'll hang out with them. Nice.

Our priorities for outreach this year are to continue to train more of our customers on the use of our tools and services. It is to show up where it matters and where it matters is where folks gather. So we're getting out on the road. And it is to support underserved communities, places that maybe don't have as strong infrastructure as we may have in other places or as much industry and support to help them get the ball up and moving.

So our focus areas first are education. I'll talk more about this tomorrow but we're getting ready to launch e-learning here at ARIN. It's been a long time coming, but we've been doing that while we've been continuing to maintain the other forms of training that we support and that's running sessions live and in person at events, as well as online and it's building content that works for you as you're trying to do a task, just in time video handouts, how to guides, and it's also the process that we go through to track and review how those things are working and how we can continue to iterate them and make them better.

So there's that. Then again as I said showing up in person. We do this in a couple of different ways. We host several events throughout the year that we call ARIN on the Road. And they're a way for us to make deeper local connections with customer audiences that maybe aren't as likely or haven't traditionally participated in ARIN meetings, going to towns that we don't take a conference to.

So quick plug. If there's someplace that you think we should be, send an email in to training@ARIN and we'll put it on our list of places to look at for future events.

It also then extends into a very, very very busy set of industry outreach, both with partner organizations and at different NOGs across the region. If you have a NOG, we'll come hang out.

And following up and supporting those events.

We do that by hosting help desks. Sorry, customer service desks. We don't call them help desks anymore. And getting speaking slots on the agenda where they're available to talk about the things that we tend to talk about. Right? IPv6 adoption. Network aut, RPKI. And so we'll send folks to those events and be there to both provide education and also practical help on site with issues that you may be having with tickets that you have in with us or other things that you're trying to do.

We're trying -- we're not trying -- we are continuing to improve our one-on-one engagement. So we have been working to revise and improve some of our welcome packets and newcomer information that we're distributing to customers as they come in to help them be prepared to take advantage of all the things that they can do once they are part of the ARIN community and ARIN customers.

We are going to transition that to the next step with more follow through to connect with those folks after we've done that initial welcome to kind of check in and see how they're doing and where else we can help.

This is really about trying to get away from the idea that ARIN is just a transactional entity and that we're really here to build relationships with you and help support your business and to reinforce that trust and to really ultimately drive down support issues that you're having in dealing with your accounts.

Cool. Now I'm not going to go too much into this because Bevil will talk about it in depth but it includes specialized specific outreach in the Caribbean count on his partnership to help us know where we can be most effective in that space.

This enables us to cultivate a pool of better engaged and informed customers. It allows, hopefully, for that to transition into greater participation in our programs and uptake of our services, and hopefully creates and provides a clear path to adoption for folks that are trying to tackle new services like RPKI, if you haven't yet.

This all leads towards the ultimate goal of stronger Internet stability and security. We all love that. So now I'm going to hand off to our key teams. They're not going to be in the right order on this slide. But so first I would like to welcome up Nate. You're first. I lied to you.

I will say that what we're going to do is run through all these kind of quickly. Not quickly. Don't feel rushed. We're going to run through all of these decks. When we get to tend we'll open it up you can ask questions of any of us.

With that I am going to slow down, actually stop talking, and let Nate have the clicker.

Nate Davis: All right. Good afternoon, everybody. It's great. I have 24 minutes to do this apparently. Anyways, I'm going to talk about government outreach. It's an area of ARIN that we don't always get to talk about thoroughly. I'll spend a few minutes talking specifically what I do along with Einar and obviously my colleagues on stage.

With that in mind, let's start first about who we interact with. I'm going to handle this presentation in a who, what, where, why, how scenario so hopefully all the questions are answered in advance.

So with whom do we interact with? ARIN's efforts in the government affairs forum, if you will, we can't do it alone. We engage with governments, businesses, nongovernmental entities, standard development organizations IETF as an example, and, of course, network operators like yourselves.

And on what topics do we engage in well, our remit is very small, but when we look at some of the work that we do at the ITEU, the ITEU is an affiliate of the United

Nations 193 member states there. Of course they're looking at sustainable goals. There's a whole variety of the things that they look at when it comes to ICT, our information and communication technologies. To that end, our remit is very narrow. We try to stay within that.

And specifically global policy considerations and those are both standards as well as development issues. And we serve in that role as experts regarding Internet number registry strategy, operation and tools.

And secondly, we are an advocate for the multistakeholder approach to Internet technical coordination and the Internet registry system.

So the why and the where. Why does ARIN engage? Well, part of what we do is we develop and strengthen government relationships. We spend a lot of time with ARIN reaching governments and conference calls, making sure they are constantly aware of what ARIN is doing, what services that we are providing and what we can do to help them. It leverages some of the things that John Sweeting and his team do makes us fully aware of what we can provide in terms of ARIN services to our government allies. We want to make sure services are well known. Part of this is to increase ARIN activity when we engage we remind them we have Fellowship Program programs, grant programs and that our community really supports the multistakeholder model of engagement for development of policies.

And then lastly, on that why is we try to influence global policy for favorable outcomes. Again, we can't do this alone, and some of these forums. We're one of many, many voices and rely on our partnerships to be successful in that.

But we try to influence as best we can for ARIN and its community. Where do these engagements take place? Well, the organization of American states, the Inter-American Telecommunications Commission CITEL one of the forums we operate and also the International Telecommunications Union ITU. That's an affiliate of the United Nations, and we work there both in the ITU sector, which is the telecommunications standardization sector, as well as ITU-D, which is the development sector. We also have a close relationship with the government, with the Caribbean Telecommunications Union.

And how, how does our work influence outcomes? So here's a few examples of some of the work that we do. This is nowhere near inclusive at all. And I do want to expand sort of our engagement in that we also rely on some of our colleagues within the ARIN organization. It's not uncommon for us to reach out to Brad or Mark

Kosters to get their input on some of the standards that are being considered by the ITU or when we're working stating our positions to some of the rulemaking proposals by the federal government that we also engage John Curran and Michael to review our submissions for that.

But just to highlight some of the items here, Canada, last year, considered a legislation that would change their interpretation and use of privacy. And that would have impacted how ARIN might have handled privacy on our end. We submitted our feedback into that process, legislative process, like many other organizations, and ultimately that legislation was killed.

So that wasn't really necessarily the outcome we wanted, but ultimately it did happen that that was killed and our privacy practices remain in place as they do today.

Department of Homeland Security, the CISSA as we call it they made reporting and ARIN made comments to that proposed legislation mainly from the standpoint of making sure that provisions in that were fully aware of actually -- fully aware of actually how ARIN conducted its policies and procedures because there were some clarifications that were needed.

In addition to ARIN's submission on that, there were 300 other organizations that had also submitted input to that process. So part of our role is just not submitting our own process, we had to go through the 300 submissions make sure any mentions to ARIN were if needed addressed and fortunately they were not. So ultimately that legislation right now is still in process and we have yet to see an outcome of that.

The next one is the FCC and its proposed rulemaking on reporting on protocol. And that is really about routing security. So this came up earlier, I think, when Brad was presenting. We really didn't necessarily have a strong position on this. Again, we were providing input into the process from ARIN's position.

We did have some organizations that also submitted contributions to that rulemaking, and we had to further go back in August of 2024 and make some corrections, some clarifications on some of the other organizations insights into ARIN's policies.

So we did that. The next one, the ITU Study Group 13. This particular item has to do with using digital ledger technology to issue and manage Internet Number Resources as well as domain names.

Now, using digital ledger technology to do that is not necessarily a bad thing, however, this standard that was submitted to the ITU is incredibly vague and is really difficult to ascertain any usefulness as a standard.

So since the time it's been presented is actually now in a final call stage since 2021 and due to objections it's been in a delayed final call stage, we're continuing trying to get this item killed because it really serves no purpose as it's stated today and effectively doing what it's proposed to do, which is manage resources under digital ledger technology.

The last item I want to mention is we made a contribution in the last half of 2023 sort of sharing with the development community of the ITU, sort of the services and offerings and services and offerings otherwise that ARIN provides such as Fellowship Program grants, how to get and use RPKI, as well as general ARIN services, and we'd have to do this in our role as a constant reminder on those things that ARIN does because these delegations at the ITU change from time to time. As those people turn over, these items have become new to those participants.

So our role is always ongoing, always interesting, and certainly always engaging.

I'll turn it over to Leslie who heads up trust and public safety portion of the government affairs team. Thank you.

Leslie Nobile: Hi everyone, Leslie Nobile senior director of trust and public safety. From a high level, my role is engagement, global engagement with law enforcement and public safety and related governmental and nongovernmental organizations.

So before I actually start the slides, I kind of want to preface how our engagement with law enforcement began. From the beginning I've been there since 2000 and we didn't know much about law enforcement. One day they showed up on our door around 2001 or 2002, flashing their badges scaring everyone, asking everybody for people to ask for information I know some of you are nodding heads have experienced this. And we had to sit down with them and explain, this is not how it works.

We'll explain to you exactly how it works. That was the first interaction. Then the second was they showed up again at the door and said we want IP addresses for a project. We said that's not how it works. We thought we tried to tell you this before.

Anyway, that was the beginning of our engagement. They realized they needed us, and we realized that we wanted to reach out to them and explain how things actually worked and how our services could help them do their jobs better.

So that was sort of the beginning. In fact, they had one of the first things we did with them they invited me and some colleagues to teach at the FBI academy. We went down there. We talked about the Internet ecosystem. We talked about Internet governance. We talked about the RIR system, routing, really just teaching them the basics. It was a great experience.

And from there we've really built our relationship and made it much stronger over the years. So it is an important thing and these are some of the reasons. So collaboration information sharing between these communities and ARIN is so important. And you heard Leslie Daigle yesterday. Those were the words she used, collaboration, information sharing in cybersecurity realm is integral.

So it's something we all have to continue doing.

From an ARIN perspective, it supports ARIN's mission of helping the Internet function in an open stable and secure manner. You've heard some of my colleagues say some of the same things.

It provides them, law enforcement, with relevant information and tools that they can use in their investigation. It helps to resolve fraud and abuse cases and cybersecurity-related incidents.

And finally, the last one, it's a direct strategic objective from our Board. It promotes the multistakeholder approach to Internet governance. It does strengthen our relationships with governments and other related entities. Again you heard several of my colleagues say the same thing.

So stakeholder communities that I'm directly engaging with and some of my colleagues are also engaging with -- we've got law enforcement and public safety, obviously. That's my number one role. So there's some in the organizations I deal with on a fairly regular basis, the FBI being at the top.

But we deal with law enforcement from within our entire community. We deal with Canada, the RCMP the US and the Caribbean. The last one I'll highlight couple of examples from these. The Jamaica constabulary. This was an event we did with Bevil. I think it was the second or third direct outreach to law enforcement within the Caribbean happened in the fall.

It was an amazing event. It was a way to get law enforcement and the judiciary and the lawyers all in the same room sharing information and talking to each other because that doesn't happen very often. They're often on opposite sides. They have to work together but they're often on opposite sides and they don't understand each other.

So we found this to be just such an effective two and a half or three-day event. We had high-level officials from within law enforcement community, governments, and not only within Jamaica but external to Jamaica. We had other Caribbean folks show up.

One of my most impressive people that came was the chief justice of the Supreme Court of Jamaica showed up in a limo with flags. I was standing out in front. I was impressed. Got out, very Hollywood, very impressive bright blue sunglasses on bright blue socks to match and he was very tall, a very cool guy. I knew I would like him right away. I did.

He contributed a great deal. We had a great event and we're going to continue with that type of outreach in the Caribbean, Bevil and I have another one planned in Antigua in July.

That's on our strategic plan within our team you. Intergovernmental, Nate mentioned the UN. We monitor and follow what's going on in the UN. I particularly pay attention to cybersecurity, CTU you've heard and IGF. Cybersecurity, global forum -- I'll give you couple of examples, Global Forum on Cyber Expertise reached out to me the new director of Americas Caribbean hub and asked me to join their what is it capacity building coordination committee, and it's a group that they're getting together of global experts to talk about capacity building around cybersecurity and what is needed and what can the GFCE do. That's just starting off right now. Just kicking off.

Trust communities. You've heard from the DNS Research Federation. That was their second ARIN grant. I've been working with them since their inception I think two years ago and M3AAWG, that's what we call it, I'm the co-chairs of names and number committee. I was asked by their Board to participate in order to bring information from the numbers community into this anti abuse working group because there were a lot of misconceptions. They didn't know a lot about us. It's been awesome because I've been able to bring talks on RPKI. We had Brad come to one of our meetings.

IPv6. Let's see what else have we brought. IPv6. Oh, IPv4 leasing, the IPv4 transfer market. Mostly looking at abuse around these types of activities. So that's been a very successful collaboration.

And then industry partners. You know who they are.

So some of the key areas that I'm focusing on and some of my colleagues are is providing guidance information and tools to law enforcement. Law enforcement calls us often. They send us emails often. They call me. They call Michael. They call RSD. They have a lot of questions. The tool that they use, the number one tool, is Whois. I'm going to call it Whois and nothing else. Sorry, I know that's not even the correct term anymore. But anyway, that's what they use. That's what they want to know about. That's where they're looking to find who is using IP addresses.

So capacity building, knowledge sharing among the relevant communities. I tend to get involved with a lot of sort of law enforcement industry partners, trust communities, all sharing information at small events and we're doing a lot of sort of knowledge sharing and it's been very successful.

We all in GAD are gigt information activity and things that are helping the community I'm focusing more on cybersecurity legislative committee. Outreach education training to law enforcement and trading and related governmental entities that's the largest part of my job. Something I've been doing since I was RSD director way back when. I do a lot of direct engagement, a lot of training.

And in law enforcement, we find that there's a lot of turnover. Every couple of years you've got new people. You've got to continue to reach out to them. Continue to talk to them. And finally, facilitating discussions and information sharing amongst parties, between parties. That seems to be one of my real major roles these days. I'm sort of acting as liaison, getting a lot of phone calls from law enforcement asking for information who can I talk at this RIR, how do ITERP this, oh can you help me figure this out. Doing a lot of lay asking and making sure people are able to connect with the people in the RIR system. I think that's all I have. Thanks.

(Applause.)

Bevil Wooding: Bevil Wooding, director of Caribbean affairs. I'll be carrying you through the Caribbean initiatives. Before I do I want to make some points about

ARIN in the Caribbean. I know most of you think Caribbean you think vacation or rum punch or some single territory that you went to that for you is the Caribbean.

But the truth is, ARIN has a footprint that spans 22 countries in the region. From Bermuda in the north to Grenada in the south, from Jamaica in the west to Barbados in the east.

To put it in perspective, that will be the equivalent of Toronto to Miami. Maine to Chicago-ish.

That's the geographic spread that we are talking about when we say the Caribbean. Big difference, of course, is that there are no roads between these territories. And there are not as many air routes to get between different places. So when we look at ARIN's Caribbean initiatives and the investment and effort involved in reaching and servicing this region, I want us to think about it in those terms.

So we're going to look at what we're doing and why engagement matters. I think that's a good place for us to start.

So Hollis would -- everyone, Nate, Leslie, would have covered a big part of why ARIN is doing outreach we're building and trusted relationships, strengthening resilience, supporting Internet policy development. Enabling local capacity, all of the major points for which ARIN is doing outreach anyway in the service region happening in the Caribbean.

There's one aspect of it I want to put my finger on for this presentation. That is the issue of building the trust relationships because for a region that has had a history of being underserviced, that is one of the things that we've had to overcome in terms of establishing really persistent relationships within the region. And so this outreach that we're doing in the Caribbean is important to ARIN for several interconnected reasons that will all make sense when you think about what we're actually doing in the region. One, of course, is to strengthen our credibility and legitimacy in the region.

For the North American network community, ARIN may be a very well known entity. For a lot of the territories we cover and service in the Caribbean, we are not.

So one of the things that we've had to do over the years and that we're continuing to do is to demonstrate that we are respectful of the culture, history, values, needs, priorities of our members in the Caribbean territory.

It also means acknowledging some of the more unique contexts within which they build networks and within which they go about trying to develop and advance the Internet.

So strengthening our credibility and legitimacy in the region is a big part of why we have outreach programs. The second reason will be getting them to getting persons from the region to engage and participate in not just ARIN activities but activities related to Internet development generally.

So we have a big investment in ensuring that if they trust us and they invite us to participate in something, go to a meeting. Join the AC. Participate in our board of directors, that they know that it is coming from a genuine place of care and concern, not just for ARIN's need as an organization, but for their own needs to contribute as the Internet development. That's why we place such a big emphasis on trust in the region.

The other point related to why Caribbean engagement matters has to do with facilitating cooperation on critical Internet number resource management.

So we sit in the policy discussions here. We take for granted that we know things about things. And for those who are joining the Fellowship Program programs or who you're trying to get to come into the policy contribution space. We have first have to ensure we have some basis for understanding what we are, who we are, why we do it in a way that matters. To do that is to actually bring them into the ARIN family, requires them to believe we actually care, and we do.

Part of that care has taken a long time to build the trust because there has been historic marginalization as I said. We want to build long-term alignment and demonstrate through taking the long, invested root in saying that we are not just from North America doing something in the Caribbean but we're part of the Caribbean and the Caribbean is part of ARIN. That's a huge part of why these activities really matter for us. As the ARIN community.

So the target stakeholder groups will be the very same groups Hollis referenced. We have the technical community, law enforcement, public sector governments, civil society players. For the outreach in the Caribbean the connections for these groups are there Caribbean partners. For technical community we have a very close and long-standing relationship with CaribNOG, representing Caribbean engineers. In fact, ARIN was a first player in the Caribbean union meeting. It will be held in Dominic in September. Long term hem investment in building the technical in

region through the governments we work through the CTU. They would be the primary Point of Contact for our engagement with regulators in the region and for ministers related to telecommunications and related portfolios.

Wider public sector -- wider private sector engagement is to a more recent relationship with artificial intelligence the network for achievement of commerce. This gives us access to heads of business who play a critical role in ensuring that the technical communities get the time off permission to participate in ARIN events. We have some very significant things planned for that new partnership in the coming year.

With law enforcement, Leslie went through the importance of that group for us. Our partner there would be the and we move towards having the groups understand the Internet development and the role they can play in supporting Internet policy and enforcement through the region.

The last is a more recent group Connected Caribbean Foundation responsible for the Connected Caribbean Summit through that group we get access to everyone else dimension of SQL. It's where leaders across the region discuss matters related to general development. ARIN plays a big part in that forum in terms of supporting that conversation.

So three areas of strategic focus. One, this is where we are targeting our outreach for the next 12 months. Internet Number Resource management. We're back on the road through the ARIN on the Road in the Caribbean. Reaching out directly to the technical community. So in addition to our collaboration with CaribNOG we're going directly with territories that invite us and have need ensuring that the technical community can get access to training and understanding of the ARIN Number Resource management policies. This is also the vehicle through which we would be promoting v6 and route security and responsibility to stewardship.

Second area would be cybersecurity and public safety, Leslie covered that. Third would be government Public Policy engagement, which we have also spoken about.

So what's next? Well, more work. We have a number of things planned for the coming period. The ARIN on the Road continues. We already had the ARIN on the Road as part of CaribNOG through ARIN engage and through the year and ARIN diplomatic forum first time gathering coordinating the diplomatic officers through the Caribbean region through different countries talking to them what's happening on the Internet space. We have the public trust and safety workshops, the flagship

of which is is justice forum that Leslie spoke to. And we have our participation in CTUs, ITU week events and other forum. And the participation would be the Connected Caribbean Summit collaboration with the intergovernmental organization care com and that come together. A lot more engagement planned. A lot of it is connected very much to the ideal that the more participation we have from around our region the stronger our community becomes. Thank you.

(Applause.)

Hollis Kara: Thank you, Bevil. If anyone has any questions for myself or any of the other presenters, happy to take them.

>> First question is to Leslie my name is Caleb Ogundele, and I'm a Fellow. You talked about government engagement and I've done a couple of government engagement and I realize something about government engagement that when you talk to most of the real policy makers, like legislature or those in the legislative, the turnover they might be run out of power very soon which you mentioned early on. But I found out if one really wants to make impact more, this is more of a comment or maybe a suggestion that you it's advisable that you talk more like the senior directors, the career civil servants. That's what I have realized working with these guys, and they are more likely transitioned between the old government officials and the new government officials and so the LPU carrier agenda which you have carried forward to the next government and all of that. So that's one of the things, I realize perhaps maybe if you have a comment about that, it's fine. Else, my next comment is to Bevil.

Leslie Nobile: I agree with you, and I think that's something that we do try to do. We're looking for the continuity. We were trying to speak to the right audience. We do typically speak to the higher level diplomats, but I think you said those are the ones that are more likely to turn over with the next government, is that what you said. Career staff tend to stay. We reach out to all of them. I think that's something that Einar and Nate and Bevil are all doing from our government affairs perspective and our team. Yeah, so we make sure we cover all of that. But it's good advice.

Caleb: Thank you for all the work. Next to Bevil. Excellent work in the Caribbean as well. My question to you,ings I understand that in the Caribbean a lot of natural disasters and emergencies that happen.

P I don't know how best maybe you would be the person to answer the question or maybe John, but during the emergency period, I know that ARIN has like some form of grants, but when I was reading through the grant stuff, I do not know if ARIN has something that they use in supporting the technical community specifically during emergency, natural disaster emergency period that they need to help them keep their networks active. I don't know if it's something that can be accommodated. I know this is more of a Internet number conversation, right? But I'm looking at it if you have a grant that supports some of these guys during this critical natural disaster period, it would go a long way to also help them have more inclusion and participation in the coming --

John Curran: Let me pick it up. On two tracks, first, pushing for resilience for disasters is a big part of what we're doing through crib-0 to get them to work in advance to make sure there's resilience for networks, more connectivity, more exchange points because when a disaster strikes, even if the traditional telephony is down often the Internet is up and running. So that's what we do. And that's not a grant. That's working in funding a bunch of initiatives with crib nothing and outreach and, et cetera, et cetera, we consider it capacity building as our jobs. I've been on calls for hurricane Hugo particularly large there's not much for us to do. If there is, we have emergency relations with both the Caribbean and the United States and Canada. They'll ask us if there's something we can do. But you don't often get someone asking for address space in a short notice in an emergency. They're generally attempting to reroute existing deployed infrastructure, which has existing numbers. The thing we do have on occasion when there's a disaster we will waive collection of fees for all organizations affected because you can have a situation where they're unable to do anything for five or six months while they're rebuilding infrastructure, and that happens too often. It does happen and we do that as a norm close of business.

Caleb: I like the idea of waiving the fees.

Hollis Kara: Thank you. Actually, Bevil. I'll have you stand there because did you have a final comment? Woods one addition to John said we play typically for hurricane season we play a critical part between different agencies and individuals who may be able to assist ways outside of our agreement. That's also significant.

Hollis Kara: Stay where you are Bevil we have an online question directed from you.

Beverly Hicks: This is from Altie Jackson ARIN Fellow what is the plan to have more engagement in the Caribbean especially in Jamaica outside of crib nothing I don't see much involved with the ISPI work for.

Bevil Wooding: That's a different question and a different statement our plan outreach generally we have a program of activities and then we also take requests for where somebody may want a workshop or some kind of intervention. We haven't had one such question from Jamaica our focus this year into the next is the under served less served ARIN territories. It doesn't mean we won't be doing anything in Jamaica if there is a need. If there is a need, then that should be raised. In terms of the Internet service providers in the region, they typically have not.played an active role in either ARIN or crib nothing activities and we're trying to change that. We're taking both the top-down approach as well as the bottom approach to ensure we can find new points of contact and interface with the ISPs in the region. Hope that helps.

Hollis Kara: Go ahead, Kevin.

Kevin Blumberg: Kevin Blumberg, The Wire. There's a friendly organization that we cojoin the conference with in October called NANOG that actually has all the active operators and there have been a number of presentations over the years about work that's been done by the operators to help but when there's a disaster in not just the Caribbean but all over the place. So I think that the numbers community and the operator community working together happens all the time. Keeping the resource piece of paper not wet is your job. The network is our job.

Thank you for this presentation. I think it's very helpful for everybody to see the type of outreach that is done and from all the different people and all the different levels of bureaucracy and government that you engage in so we don't have to. I definitely round of applause for that.

The only thing that would be really cool is the one part that was missing from all of this is all the collaborative work that you do with the other stars or RIRs you mentioned ARIN only, I know you do a lot of work, collaborative work with those organizations. Just a couple of minutes to talk about that -- you're not in a bubble just ARIN doing this work, it's been done across many different avenues. Thank you.

Hollis Kara: Thank you. Do we have anything else online? No. Seeing nothing else in the room, that concludes the outreach panel. Thank you to all my fellow panelists. Many.

(Applause.)

(Applause.)

Next on Open Microphone. I'd like to welcome up John Curran and our vice chair of the Board, Tina Morris, to conduct the open mic.

OPEN MICROPHONE.

Tina Morris: I get to sub in for Bill who had to step away for his day job. We'd like to welcome any questions you have to open mic. I know there's things we delayed from earlier today that you might want to bring up now.

Is it me, you don't want to talk to me?

(Laughter.)

Kevin Blumberg: I'll be quick.

Tina Morris: Who are you, sir?

Kevin Blumberg: Kevin Blumberg, The Wire.

Tina Morris: Just checking.

Kevin Blumberg: It's between me and the beer, except there's no beer. One thing that I have noticed -- I wanted to comment on -- I have seen a significant improvement over the last five years in the Fellowship Program, both in the caliber of the Fellows that are coming, the attendance of the Fellows, the involvement of the Fellows, and more importantly, the involvement of staff in making the Fellowship Program a solid program.

I was involved in the last five sessions of doing a little webinar, being asked for that alone in and of itself was a big departure from the previous scenarios of dump the Fellows in a room and let them go wild.

Having been a mentor back in those days. I want to say thank you to the staff and the Board and everybody else that's involved in improving and making a big difference to the Fellowship Program.

John Curran: It's the staff. Go ahead, John.

John Sweeting: John Sweeting, chief experience officer. I want to point out that Amanda Gauldin is the whole energy behind the Fellowship Program and she has brought all these wonderful changes. She puts so much of herself into it.

(Applause.)

Leif Sawyer: Leif Sawyer, GCI, ARIN AC. I wanted to add on to what Kevin said. So forgive me if I get this wrong, but I believe you can apply to the Fellowship Program two times, more than once, right?

John Curran: I think so, twice.

Hollis Kara: Yes, twice.

Leif Sawyer: I hear talk in the hallways about people wanting to stay involved in the community but not sure how to do it. So I encourage all of you first-time Fellows to reapply for the Fellowship Program for this fall, it will be a joint session between the operator group, NANOG, and ARIN following directly after. So get on that.

Tina Morris: Thank you.

Hollis Kara: We have a question or comment from online. Go ahead.

>> First comment from Katie Gerry for cases for names individuals or married names RSA from their first name if it changes ARIN accepts court updates point of records correct updates since they're not public I don't believe ARIN needs to be concerned.

Hollis Kara: Thank you, Kate.

John Curran: Thank you for the comment.

>> Also have a question from Kate actuate has there been any discussion of forcing an RPKI ROA for 4.10 space limiting the ROA to have Origin AS under the control of the Org ID in order to reduce the risk of leasing that IP space.

John Curran: Forcing organizations to issue ROAs, just the term boggles the mind.

Tina Morris: What if we rephrased as requiring that.

John Curran: We cannot force ARIN members to do anything, but if you wish to make it a requirement to have forced 4.10 space it be announced you put in policy

and make it clear because we'll enforce it. But we don't create other interesting requirements out of whole cloth. You guys have enough to do already.

Tina Morris: To the microphone.

>> Caleb Ogundele: Again I'm Caleb I'm circling back to what Kevin mentioned about the Fellowship Program. For me the big thing during this particular Fellowship Program that I think I liked most is the diversity. And it reflects the last publication I think came from ARIN about diversity. I think you probably wrote that publication that ARIN was serious about.

So I'm really happy about it because it's walking the talk and making sure that it's reflected in every sphere of what you guys are doing.

More importantly, perhaps since we all give an applaud to Amanda and John and all the guys doing all the good work, maybe we should give them a pay race.

(Laughter.)

Tina Morris: Thank you. I believe we have another online question.

>> We do. From Brandonness ton VPS can CG and AT be a reason to obtain a /24 under 4.10?

John Curran: CGNAT for 4.10 or Brad.

Brad Gorman: Brad Gorman ARIN RPKI guy. I want to remind everybody I've not received a correct answer of who is the third person who --

John Curran: Very good.

Tina Morris: I thought you were answering the question.

John Curran: Question came in use of CGNAT could that be used in 4.10 space. CGNAT should be an acceptable IPv6 technology.

John Sweeting: CGNAT is absolutely justification.

Tina Morris: Do you have a follow-up.

>> I ask because service providers are hesitant to provide NAT64DNS64, 464XLAT because service disruption could be an issue provide an IPv6 only network is my understanding.

John Curran: CGNAT isn't the only justification. If you can come up with an IPv6 network using NAT64 DNS64 that's acceptable too.

John Sweeting: Let me give a real quick.

John Curran: Go ahead.

John Sweeting: For the very first, if you have IPv6 and no IPv4 you could use to help deploy that v6, the very first /24 you ask for, if you just need v4 to dual stack your DNS server so you can use IPv6 is plenty of justification for that first /24. We would love you to do some other translation services with it as well. But if you come back for a second one and all you want to say is I want to do some more, I want to dual stack a whole bunch of DNS servers, the answer is no.

John Curran: That's no. Agreed.

Tina Morris: Back to the microphone.

Kevin Blumberg: . Kevin Blumberg I wanted to comment on Kate's required doesn't have to be required, special blocks 4.4 and 4.10 and should have requirements when we talk about those requirements and I definitely implore the community to maybe look at strengthening the requirements in those blocks, not just RPKI valids that are specific to the block and AS number in the case of critical infrastructure, maybe RPKI invalid so that the block is not routed, then that's sort of an allowance.

Having things only on PPML -- this is really where I'm getting at -- having things only on PPML and only at a meeting isn't necessarily the most conducive thing in 2025. There are newer technologies. There are also webinars. There's also having group chats about a specific topic, setting up a time for a call that you can do things. I have been around a long time I'm sorry I'm getting tired of replying to PPML and following up with the 84 posts bashing a singular word used I don't like e-mailing Mailing Lists anymore. I am old I think there's better ways of having discourse I think Kate's idea is brilliant and should be worked on. I think if we leave it to the PPML void it won't go anywhere. Let's try as a community to find better ways facilitated discussions may be the first way of having that happen. Thank you.

John Curran: Your point's taken. First, much like almost any other body out there, it is possible for any number of you to get together on your choice of platform and do what would be called a design team and come up with an initial early proposal for something and then submit it to ARIN. Nothing precludes that. You don't need to

send just the thought dashed off to PPML if you want. You can refine it with a group of like individuals and you can use anything you want to do that.

If your preference is Slack or Reddit or whatever your poison is, Discord, get together with people and do it.

If you want the ARIN AC to use some tools in certain phases -- I don't know if that's the whole PPML -- the whole PDP or just the beginning or whatever -- then come up with a proposal what tool and when and talk to the AC. We are not constraining them. They get to set the tools and if some of that requires a PDP change, we'll run that past the community. We'll figure out how to update the PDP. But I don't think it does.

Kevin Blumberg: I think you missed the one word I said is facilitated. Yes, that would probably be the ARIN Advisory Council as a way of not changing the entire process, John, but just giving some more useful spaces to have discussion before things get into the policy process. This would be a good example of let's have a policy discussion because I'm going to submit a one letter draft that says whatever and then they're going to right away the ARIN Advisory Council is going to come and say we have a policy draft, or policy, it hasn't yet reached draft status we don't understand it let's talk to the author. I'm saying at that stage before it's there, there can be some facilitation in other means, Zoom or whatever, to let people talk.

John Curran: Flesh something out. Let's get it to us. Happy to support such.

Tina Morris: I want to comment on that real quick. Some of you may not know, NANOG is trying Discord, and as a stop gap between the younger communities that don't communicate on Mailing Lists anymore and maybe Kevin we can talk about that.

Sumon Ahmed Sabir: I just want to make a clarification that probably a little about the legacy historical policy at APNIC, Kevin mentioning that APNIC is reclaiming all the IP addresses. Not that actually. Legacy address holder can be a APNIC member they can join with a small amount of fee or they can live without agreement but they're missing this RPKI and other facilities. They'll get the DNS service as it is like before.

What they're claiming if we see those IP addresses are not announced for a certain period of time and they're uncontactable, those IP addresses we give it a certain time and we're reclaiming those and putting it into A.0.

John Curran: I do understand. That's your current approach for running that.

>> Sumon Ahmed Sabir: Yes, exactly.

John Curran: So far you're ahead of us in terms of working on cleanup in this area but you've seen what we're going to do with the current policy. To the extent the community wants to change the policy to do more, we'll do more.

Sumon Ahmed Sabir: Thank you.

Hollis Kara: We have one more question or comment online.

>> Matthew Forbes, ARIN Fellow, minor question on the topic of engineering teams Kubernetes migration. Will the community experience any increase in the number of maintenance activities after the migration is complete? The backdrop for this question is the release calendar for new major and minor versions of the Kubernetes software.

John Curran: Okay. I'm not going to opine on ARIN's Kubernetes deployment. But I will scan the room to see if Mark wants to. Is Mark hiding here.

Hollis Kara: Mark, were you listening? He wasn't listening.

John Curran: So as we switch to Kubernetes, will doing that change the frequency or duration of our maintenance windows?

Mark Kosters: So the answer to that is most likely actually they're pretty short now. The only time we really have taken an outage lately is with our database. That type of outage where we have to upgrade the database, then yes we'll have to -- that won't change. But as we go forward we'll be able to do more frequent updates and we'll not be impacting the community.

John Curran: Thank you.

Tina Morris: Anymore questions? Do we have anything else?

Hollis Kara: Nothing online. Anyone else in the room? Going once, going twice. I think we're done.

(Applause.)

Thanks for hanging in there. I know today was a little bit long. Look forward to welcoming you back tomorrow. Before you leave, we've got to do the thing. Can I get a round of applause for our Network Sponsor, Spectrum.

(Applause.)

Our Webcast Sponsor, Google.

(Applause.)

Our Platinum Sponsor, AWS.

(Applause.)

And our Silver Sponsor, IPXO.

(Applause.)

Just a reminder, we do have one half day left on this meeting. We'll be back here at nine AM stop by to grab breakfast before you head in. Thanks for another great day. I appreciate everyone's patience and understanding as we worked through a very long and well-packed agenda.

(Applause.)

[5:16]