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.

OPENING AND ANNOUNCEMENTS

Hollis Kara: All right. Welcome, everybody. We're back in a real room. And we've got folks online. This is ARIN 48 and we're really, really happy to see you here today.

My name is Hollis Kara. I'm the Director of Communications at ARIN. I'm going to walk you through a few items for today's meeting. First, I'd like to thank the Board of Trustees for all their hard work, some in person, some online.

If you see them, they have ribbons on their name badges. If you see them, grab them and have a chat. They're all glad to be back and able to interact with the community.

Advisory Council as well. Today is their easy day. We're just doing a Member Meeting, we don't have any policy discussions but they're here both online and in person. It's a great opportunity to reconnect with those folks if you get the chance.

And then also our NRO Number Council, thanks for being here both in person and online. We're glad to have you and thank you for all the work you do for the ARIN

community.

Let's talk for a second. This is -- we're back in person, which kind of seems like, okay, we're getting back to back to you. But this different. This is the first time we've ever done a hybrid meeting. I want to thank you for being online to be part of this grand experiment.

I'm going to walk you through a couple steps because this will be a little different than how we've handled virtual meetings over the last two years.

For our folks online, the options are a little bit different today. Obviously we've got chat available to you and we're hoping you'll use that. Your virtual host, Amanda Gauldin, will be there with you helping you through the meeting today if you need anything. And that's great. We want you guys chatting in that chat.

For any questions you want posed to any of the speakers, you do need to put those in Q&A. Those will be moderated into the dialogue in the room. If it lands in chat we're not going to be able to grab it. And please make sure you put your name and affiliation when you put those comments or questions in for those opportunities.

We will also be having a virtual help desk today for our folks online. If you go to the ARIN 48 home page, you'll see, it's circled, a new thing that's appeared in the menu, and that's a virtual help desk. If you click on that link it will pop open a zoom meeting and you'll find friendly ARIN faces there if you're having a technical challenge or need information.

They're there if you need them. Don't hesitate to stop in and say hello. They'd love to see you.

In person, we're really glad to have you back. I'm asking if any of you are choosing to log in and be watching the stream or in the Zoom session, please make sure your devices are fully muted.

Otherwise it's going to get really weird in here really fast. For safety sake, because we want everybody to go home healthy, we have stationed Clorox wipes and a trash can by the microphone when we open the mics. If you could please wipe it down when you're done with the comment just to keep all our cooties to ourselves.

A few chat reminders -- as always we want to keep our conversations professional and on topic and always adhere to the ARIN Standards of Behavior, which you all promised to do when you registered. So, we're holding you to it.

A few more reminders, the producer over on the riser, Beverly Hicks, will be helping me out with hosting duties. We're going to be moderating our virtual attendees and our in-person folks when we get to those discussion points. And we're asking that everyone please make sure that they are providing their name and affiliation when they come to the mic or pose a question in queue so that we can get that on the record. We want to make sure that we capture everything properly for posterity.

All right. And as always, we are live streaming. This session is being recorded and will be published later for our archival history.

Slides are available on the meeting site. And live transcription is also available. All of that can be reached on the ARIN 48 Meeting Materials page.

I do want to remind you, once again, not to beat a dead horse, but this is the first time we've ever done this. So we're excited but also a little bit nervous. Bringing presenters in virtually and having folks here live and doing all this is a far step past what we've done for our remote participation in the past.

And I've got a great team backing me up told. They've been working really hard. But we're really looking forward to your feedback at the end of the event to let us know how we can make this better going forward.

Special thanks, again, to Beverly Hicks on the riser who is going to be our moderator extraordinaire. If you've been in our virtual meetings, you know Beverly well. And Melissa Goodwin for all of her on-site and hybrid meeting support.

I'll be here on stage as your host. We have our virtual host, Amanda Gauldin, in chat with our virtual attendees. Ashley Perks and Kerry Carmichael will be on the virtual help desk, and Tommy will be wandering, getting pictures because we can get finally stuff that's not just screen shots.

I'd like to take a brief moment to thank our sponsors, USI and Lumen, for making this meeting possible.

And per policy or per regulation I have to walk through the evacuation procedures, which basically -- it's a lot of words -- boils down to if something really bad happens, there's going to be an announcement. Listen to the announcement, follow directions. If you see someone that needs help and you're in a position to give them a hand, try to do that because that's friendly.

On to the day. We'll start with a keynote address and move into a panel on Internet governance. And we'll follow that up with an ARIN Operations Report before we break for lunch.

We'll have box lunches available outside. We welcome you to bring them back in after the break or sit wherever you like.

After lunch we'll move into updates. We've got a presentation on the progress on fee harmonization, membership changes, our Advisory Council Report, then a Financial Report, Board of Trustees Report. And then we'll be opening the microphone to hear from you guys. We're anxious to get to interact with you again in person.

And I think that is, that's everything. I'd like to

welcome John Curran to the stage to introduce our keynote.

John Curran: Thank you, Hollis. I'm John Curran, president and CEO of ARIN. It is my privilege to introduce a legend in cybersecurity.

Chris Painter has been at the forefront of cybersecurity policy, leading US and international efforts in making the world and the Internet a better place.

He's had a very long and privileged career, starting out as a prosecutor on some of the highest profile cybersecurity cases there were.

If folks remember Kevin Mitnick, for example, working in DOJ, the FBI, eventually the National Security Council and in the State Department.

In the State Department, he became the nation's first cyber diplomat, our top cybersecurity diplomat with a portfolio set up for that, and went around the globe working to try to work on our international and diplomacy efforts to make a secure Internet.

Truly he's been involved since the beginning. I've run into him on many a forum when I've had to travel. He's certainly the president of the Global Forum on Cyber Expertise Foundation. He serves on the center of Internet security as a nonresident advisor, senior advisor at CSIS, the Center for Strategic and International Studies.

He's a fellow at the Chatham House and he's on the Public Sector Board at Palo Alto Networks. He's also a co-chair of the recent ransom task force. And he's been a commissioner on the Global Commission for the Stability of Cyber Space.

Truly an in-depth person who has been involved in all of this. I'm honored to have him here this morning. I think you'll find him quite interesting. I'd like to now turn it over to him, and I'll come back afterwards

to help moderate the questions. Thank you.

Chris, take it away.

KEYNOTE: "CYBERSECURITY AND THE INTERNET: THE ROAD LESS TRAVELED"

Chris Painter: It's great to be here with all of you today, although virtually sadly, as most of us do these days.

I am, as was said, a recovering lawyer. I don't think you ever recover from being a lawyer. But normally, especially in the beginning of a session like this, you would tell a joke to kind of break the ice. But the problem with lawyer jokes is that lawyers don't think they're funny and non-lawyers don't think they're jokes. So I've decided to forego that. Maybe I'll tell a different joke later on.

As said, my background, I've been doing cyber -- various aspects of cybersecurity and cyber policy for about 32 years, which is a long time, well before the Web existed, certainly not before the Internet existed.

And I have really seen an evolution of both the threat and our response over that time. And I think, just tying into the theme of this keynote and really the panel afterwards, which is interesting, the robust travel.

And in a sense I think it may be the road that is not prioritized as much. Because I think we've traveled, I do think we've talked about cybersecurity. But there have certainly been challenges over the years.

Even when I was at the State Department as the world's first dedicated cyber diplomat, I was not the coordinator for cybersecurity. I was a coordinator for cyber issues, which tried to tie together not just the security issues but the human rights issues, the economic issues, the governance issues, because these are all interrelated, and need to be, particularly in

the times we face now.

In terms of the threat, all of you know we've seen an evolution over even the last 10 years of significantly amped-up technical threats and policy threats. The technical threats are what you all see every day, what we talk about every day -- the kind of large, espionage attacks, including supply-chain attacks like solar winds, Microsoft Exchange Server attack, criminal attacks that go after financial and personal information, theft of information by both state and nonstate actors.

You have state actors, you have nonstate actors, you have transnational organized criminal groups -- a real range of threat actors who are getting more sophisticated and more challenging over time as we become more dependent on these technologies.

So that has continued to grow over time. And I think our recognition of it as a threat has grown over time. I don't think we've taken it as seriously as we need to. But certainly we continue to see this evolution of attacks and most recently capped off by ransomware which I'll get to in a minute.

This is all exacerbated by the pandemic, where the bad part of the pandemic is that you have, just like in almost in any other crisis, criminal and even nation states groups targeting these systems because we're even more dependent on these technologies than we had before.

The silver lining is that I think a lot of folks who didn't realize that cybersecurity was important before are now realizing it and they're now focusing on it, particularly in developing-world countries, where they're more focused on connectivity and Internet policy and haven't understood why cybersecurity is the foundation to having both of those things.

And then we see the policy threats. And the policy threats range from everything from more repressive governments who want to impose a different system of

governance on the Internet, who want it to be state controlled.

These are not surprising actors -- Russia, China and others -- who believes that speech itself or content itself can be a threat to their stability and therefore like the idea of a state-controlled system rather than the multi-stakeholder system we have now, including by folks like all of you who are involved.

They'd rather have a state, top-down, controlled approach, and who have even gone so far, as I think many of you know, as to suggest in various standard-setting bodies, the ITEU and others, of coming up with an alternative system for connecting the Internet, an alternative to the DNS system that will allow them to exert more control, which is a real danger. It leads to greater splintering of the Internet or vulcanization of the Internet. And that's a real policy challenge as well.

So, we have both the technical challenges, sometimes the same threat actors, sometimes nation states, and sometimes others in the policy threats.

And I think we've been hampered in a couple of different ways. One is there is this gap I've seen over my time, I saw this in the White House, too, between different communities of interest.

So there's the Internet policy community -- economic community, the governance community -- who talks about Internet policy.

There's the cybersecurity community who talks about cybersecurity. They have a different lexicon of talking about things.

Once, when I was at the State Department, and at the White House, one of the things I did was convene 16 different government agencies to talk about an international strategy for cyber space, which we did put out in 2011.

And at first it was creative cacophony. They weren't even speaking the same language. It's important that the security issue is not some boutique side issue, but part of the larger things we're trying to achieve in cyber space, the economic growth and social growth, and not see them as conflicting or as different groups.

And that's been a very hard thing to bring those communities more together.

The other issue, and I think you all know this as well, there's a gap between the technical community and the policy community. The policy community is often folks in governments and others who are negotiating in places like the UN. And there's not as much of a tie or understanding of the technical community.

And vice versa -- the technical community often doesn't understand why the policy community is important and doesn't have that tie as well.

So strengthening both of those ties and really bridging those two gaps, I think, is critically important as we look at this.

The other thing that I think has hampered us is for all of you, like I, who have been involved in these topics for years and have been sort of laboring in the fields and thinking about cybersecurity and why it's important and why we need to prioritize this, to be sure, we've gotten attention in the past. We've gotten attention in terms of greater attention when major incidents happen. Every time there's a major cyber incident, there's a lot of press attention.

But unfortunately it seems to go away quickly. Yes, our governments have paid more attention, especially in the US, to this issue, starting with President Obama -- really starting with President Bush, but amped up under President Obama because his campaign had been hacked into. He did a lot to try to organize into this issue and make progress.

Less under President Trump where it wasn't really a priority for the administration, but still some progress was made.

And then finally, now under President Biden, who came in with the promise that cybersecurity would be a priority at every level of his administration, easier said than done. But I think they have been walking the walk recently in terms of executive orders, in terms of appointments of key people.

So there's always been the sense that cybersecurity has been this back-burner issue, the second issue, whether it's fighting cyber crime or securing systems or going after state actors.

And one of the things I hate the most in the press that covers this or even some people who speak about this, is when they use terms like cyber 9/11 or cyber Pearl Harbor, which they've used frequently, to say we're worried about this incident.

But what ends up happening is we don't have a cyber Pearl Harbor, we don't have a cyber 9/11, we don't have an event we all are worried about, which is a massive takedown of our infrastructure, our electrical infrastructure, water, financial, et cetera.

And therefore it's somewhat become the boy who cries wolf or Chicken Little, where people keep hearing this and it desensitizes them. They don't understand why security is important because these massive events haven't happened.

Where in fact the events we see have been incredibly serious and affect us in lots of different ways -- espionage events on one side, theft of personal information, disruptive attacks, ransomware attacks, botnet attacks, all these things. And even attacks against the domain system have all, I think, posed serious issues. But it hasn't really risen to the level until recently of a real national security priority.

It's been thought of too often by, both in government among ministers and other systems, among cabinet secretaries and other senior government officials; and in the private sector among CEOs and others, has been seen as a boutique technical issue.

I remember at one point, with some exceptions, I remember Janet Reno was really into cyber crime and understood it, very early adopter on that.

But most of the time you go in and you try to talk about these issues, and if you're talking to a high-level official, their eyes would roll back in the back of their heads and they want to get away from it. They'd say, that's a technical issue or law enforcement issue; you guys go deal with this.

When it's not. When it really is much more important, given our dependence on these systems. It really is a core issue of national security. It's a core issue of economic policy. It's a core issue of human rights. And it's ultimately a core issue of our diplomacy of our foreign relations as well.

And although we've worked and traveled that road and pushed this for a long time, with some successes and failures, with that sinusoidal little wave of people talking about the recent event and then going away. I think we've seen a change recently. And this is I think a really good thing that we haven't seen before.

And the other thing I hate in the press is when they say something is a wake-up call because we've had about 80 different wake-up calls over the years.

Every major cyber event has been a wake-up call. And we seem to easily go back to sleep or not have the attention of the public or the policy makers, that political-level attention.

I think what's changed that, interestingly, and it was a surprise to me, was ransomware and some of the recent

ransomware attacks. As was mentioned, I was part of the Ransomware Task Force report that was put out by about 60 different folks, former government people, present government people, law enforcement people cyber insurers, cybersecurity companies, really a great group.

And I was one of the co-chairs of this group that put together a report, including over 40 recommendations, that was issued just before the Colonial Pipelines attack.

And of course we had nothing to do with Colonial Pipelines, but that attack, I think, raised the attention on this issue in a way that I've never seen before. And in a good way.

I think once people understood that a cyber attack that actually affects their everyday lives, when they had to line up for gas, when their hamburgers were in jeopardy because of the meat-packing plant cyber attack. When healthcare was in jeopardy because of what happened the Iris healthcare system and has been replicated in other hospitals.

That brought it home to the average person in a way that we hadn't seen before. And that also translated it to a higher political level. And that promise we saw from the Biden Administration that it would be a priority at every level was translated into action in a major way.

A lot of attention. I think it went from being, the ransomware part of it went from being a back-burner issue to one where you have the president himself talking about it, to a series of meetings, first at the G7, where you already had a crowded agenda that included climate change and financial regulation and the pandemic.

And it became a priority there, where the G7 leaders agreed to take action. Where it was brought up to NATO and EU and finally in the summit with Putin, it being one of the major issues.

So that transformation, I think, is critically important if we can sustain it because we'll have sustained interests, resources and priority on this issue which we desperately need.

So, how do we respond? That priority level, that taking it seriously is number one thing to do. I think we're there at least for now and I hope we continue to be.

One clear thing that we need is these are, as you guys know, these are always international issues. These are, even if you have a hacker in one apartment attacking someone in the apartment next door, they're likely to route their attacks through other countries to make sure it's harder to find them and harder to have accountability. That's true of nation states and sophisticated individual and criminal hackers too.

What we need is unprecedented international collaboration and cooperation. We need to break down those silos that I talked about before so we can have that cooperation between all these different communities, including the law enforcement and the technical community.

So, there's been a lot done on two different areas that I'll just briefly touch on.

One, on the policy front, I think there's been quite a bit of work done to set the rules of the road in cyber space. The UN has been focusing on, among state actors. Is it a wild, wild west or a wild, wild web out there or are there some rules?

And the great answer is even among countries who disagree on many things, like Russia, the US, China and others, there was agreement in 2015 that was reinforced just recently in two UN processes that first international law applies in cyber space, that's critically important. It's not devoid; you don't need a whole new legal structure for cybersecurity. International law applies when you get to that area of cyber-level conflict at war, which we haven't had --

despite all the hype we haven't had.

But also there's been agreement on some voluntary norms of cyber space. Don't attack the critical infrastructure of another country when you're in peace time. Don't go after the Computer Emergency Response Teams, or CSIRTs, because they're like the hospitals or the ambulances on the Internet.

These sets of norms or rules I think are really important.

And the third part of this is confidence-building measures, the ways that you can coordinate and communicate with each other during a crisis and de-escalate.

But those norms I think are critically important, because if countries abide by those norms we'd be in a much better place just in terms of nation state actors.

Interestingly another one of those norms was that countries should not allow their territory to be used by malicious actors to attack targets in other countries. And if another country asks them for help they should give it.

If you think about the ransomware issue this is one of the core issues that we have there, which is the proliferation of a number of safe havens for these actors so these actors can act with impunity.

Despite all the things you can do to cooperate with law enforcement and others, if you can't reach those actors and they can do whatever they want, that's not sustainable.

And we have to figure out how to persuade countries like Russia to change their calculus. That means telling them they already agreed to this and holding them to that accountability. It means putting pressure on them. It means figuring out how to go after these groups even if you don't get that cooperation.

That level of UN activity has been helpful in terms of setting what the rules of the road are.

Now, there are some deficiencies in it too. I talked about bringing the two communities together. It's hard in the UN because it's a system built for states by states. But there's been some efforts to bring in other stakeholders including the technical community to the deliberations to help them evolve these thinkings.

That has to increase significantly. It's still relatively in its infancy.

I talked about the UN. But there's lots of other activities. There's regional organizations in this region. The Organization of American States has been active in this.

I was on something called the Global Commission for the Stability of Cyberspace with a number of folks, Vint Cerf and others, and we came up with suggested norms, including one that I think is relevant to this community, which is -- I talked about these other norms and restraint; don't go after critical infrastructure.

We also said countries should not go after the backbone that public core of the Internet. The thing that makes the Internet work. The addressing and naming system, the routing system, that that serves a greater interest, and no countries should go after it.

What the UN did was they said, we're not going to -- we're not going to adopt that because we don't want new norms. We're going to say an example of that critical infrastructure norm, because the Internet, although it's cross-national, is a critical infrastructure. I think that was a big issue.

As I said there's been lots of work in G7 and even the G20 and others.

Now, operationally, obviously, the policy is important.

But if we don't have operational cooperation, you're lost. So there's been a lot of stepped-up international cooperation among law enforcement authorities, among CERTs and CSIRTs.

There's something called the Budapest Convention, so countries have better cyber crime laws and have them all around the world. There's still some countries that don't.

The first group, the Forum of Incident Response Security Teams, brings a lot of the CERTS together. We just need much more cooperation among those, the ransomware task force report. And now the US has launched various task forces to deal with that issue internally but also with foreign partners. And so that collaboration is important.

And part of all of this is capacity building. I'm president of the Global Forum on Cyber Expertise, which is a worldwide capacity-building foundation that now has 145 members, private-sector members, civil society members, academic members in over 60 countries to promote cybersecurity capacity building around the world.

I recommend you look at our website, www.dgfc.org, for more information. But that's critical to making sure that we don't have the weak link problem. We're dealing with countries around the world who do.

That's important, but another part is breaking down the silos, including using the term, which is often an overused term, of public/private partnership. Public/private partnership is a great term, but it's often used as a talisman without content. We really do need it in this space.

That means information sharing with others. It means collaboration between industry and government.

Again ransomware has provided a fairly good template for that. There's been good work between Europol and the

private sector. The US is setting up ways to deal with the private sector on this issue.

The task force was a very public/private partnership undertaking that we were part of. That's really important. Bringing those together is important.

But all this is great, and we need all these things. And I know the panel will discuss these more and I'll take some questions in a moment. But we also need accountability in cyber space.

I talked about rules of the road. I talked about the bad actors out there. If there's no accountability for bad actors, if there are criminals, if we don't actually disrupt their operations and arrest them, if they're nation states, if we don't take actions to make sure there are consequences for their actions, all the rules of the road, everything we write down are just words on paper.

They'll violate them. They'll say there's no reason not to because they feel it's in their interests and there's no consequences. Other countries on the fence will say, why shouldn't I do that too. And we're ending up with a much less stable cyber space than what we want.

Making sure there's consequences, that we act not just unilaterally but together as countries and other stakeholders to impose those consequences and that accountability is really important.

With that, I'll stop because my time is up. I'll say, after the questions and answers, I'll tell you what my background is unless you guys can guess and why it's important.

But I'm actually not sitting in the room with a giant computer behind me, by the way. But it is a significant computer which we'll talk about in a moment.

Let me now open it up to questions from the audience. We have ten minutes for that.

John Curran: Thank you for that great presentation. Round of applause for Chris Painter.

We'll open it up for questions. Please approach the center microphone if you're in the room. If you're remote, please talk to the remote moderator.

Beverly Hicks: If you're approaching or a remote participant please state your name and affiliation as you're speaking. And I'm looking for questions virtually as well. Looks like we have a question in the room.

Ron da Silva: Thanks, Chris. Appreciate you being here today and your perspectives on cybersecurity.

Ron de Silva with Quantum Loophole. My question, just to bring the broader issue of security to this audience, I think about Whois data and how that is important in prosecuting criminality and chasing down bad actors and trying to coordinate that across different domains.

We've seen how in the domain namespace that's been pretty much turned useless because of GDPR compliance issues and trying to find ways to protect privacy but also still have data available to help facilitate law enforcement.

And I think about here in the namespace we have a similar challenge. We have all this data that's available and it could be used to help facilitate addressing cybersecurity issues. But what lessons do you think can we pull from, what has happened in making Whois information useless in the DNS, and how that could potentially impact the numbering community? And what do we do more broadly and how do we deal with that issue?

Chris Painter: I think it's a prime example of communities not coming together. I think when the GDPR was passed, it wasn't intended for it to have this effect. If you talk to the people involved with it, they were focused solely on privacy.

They really weren't talking robustly to the law enforcement community, or even the technical community on the cybersecurity side. They were focused on the privacy issues.

And like any other policy, you're better informed, if you talk to those communities, you understand what the second and third order effects are.

They're trying to address it. ICANN has been trying to address it. There have been discussions in Europe to address it. Generally the reception is that's not what we wanted to happen, so maybe there will be some solution.

But you're quite right, especially in the beginning of an investigation, that kind of data is critical because it helps you get further on to the point where you're using other kinds of legal processes. You're cooperating with other countries.

So I hope that doesn't spread to this community as well. But what I'd say is it's important to have that dialogue with the other parties involved, including the privacy advocates and the privacy parties to make sure that they understand what the issues are.

I remember years ago, long before the GDPR, we were negotiating, I was then representing the G8. I was the G8 High-Tech Crime chair. And I participated in a meeting in Brussels about a prior version of this, which basically said all data had to be anonymized or destroyed.

There was no exception for security. So you can imagine if you got rid of all your data it would be very hard to trace criminal and other incidents.

There was small participation of the law enforcement community or understanding between those communities. I think we need to build that bridge, and I would urge you to do that.

I don't think that it's all lost on it. I think there's still efforts. And I hope those efforts succeed to make that a usable and available database for law enforcement. Safeguarding as we need to the privacy issues as well.

John Curran: Excellent. Thank you, Chris, center mic.

Alison Wood: I'm Alison Wood. I'm a network architect for the state of Oregon and I'm on the ARIN Advisory Council.

I have spent a lot of time working with local law enforcement in the state of Oregon. They very rarely investigate cyber crime and even less rarely prosecutor cyber crime. What can we do to work at the state level and other states to improve that?

Chris Painter: That's a good question. First, there's a number of task forces out there that are federal/state task forces. So, the FBI and Secret Service will work with states and localities too.

The other thing is I have some sympathy for state and local officials who are dealing with lots of different issues and not given the resources or training.

So they need to make sure they're getting that as well. This is a role that you guys in the technical community can help. You can help like sensitize them, train them on this.

The third thing is, even if they think it's small potatoes in a particular case they're looking at, if you aggregate these cases it turns out it's often the same actor.

There's a number of databases and law enforcement tools -- the National White Collar Crime Center and others -- who try to aggregate this data in a way so that then local authorities will say, yeah, this is worth pursuing because it's here.

The fourth challenge is it's often multistate or international and they're not usually equipped to deal with that. And that means you get a partnership between the state and federal authorities.

It's not an easy answer. There's some really good local authorities out there. LAPD has been very active, the New York PD -- there's a number of the bigger departments. But this has to be, given that we're going digital and this is going to continue, this has to be a priority for local actors too.

And part of it is also just working with state governments to make sure they're funding and priors prioritizing too. And maybe the ransomware is another leverage point to do that.

Alison Wood: Thank you.

Beverly Hicks: We have a question virtually.

David Huberman from ICANN. Chris, what would you say to a regulator who thinks that the root server system needs to be regulated to ensure availability and security for the regulator citizens? What do you find is a useful tact to disabuse the regulator of this notion?

Chris Painter: First, I would drill down what the hell they mean by that. What do they mean by regulate? How does that actually provide that protection they talk about?

It often boils down to not really that, but they want some control. They want the root server to be in their country, or a root server or a number of root servers.

It's more of a political issue often than a security issue.

The way I combat it, talk about the security issues. Talk about why the name system is set up, why there are mirror servers out there, why it's survivable, why

there's security built in.

And also talk about the fact that even if you added a main server in their area, that doesn't give them much more control or ability, given the way the system is architected.

I think the best way to fight back against that is with the actual real true technical arguments.

Now because of the political issue, you only get so far with that, but I do think a number of countries, like-minded countries to the US and others, are attuned to that and understand that, if simply giving a country a domain server doesn't cure their issues then it's more of a political statement, and that needs to be part of our policy is to have those discussions.

And maybe say to them, look, here's other things you can do and here's other things, in terms of capacity building we can do for you, that will actually help you substantially, instead of the symbolic thing of having a server, a root in your country.

John Curran: Thank you, Chris. Center mic. Center mic.

Leo Vegoda: Leo Vegoda, And Polus LLC. You've used the phrase "cyber 9/11." We had a health 9/11. And that saw a massive diversion of people who went into the office to -- doing all of their work over the Internet.

Did that create what will become your cyber 9/11? Or is the out-of-the-box security configuration for all the online services we use good enough?

Chris Painter: So, as I said, I don't like the term "cyber 9/11" because it puts all of your expectations on one giant event that will change everyone's attitude.

Yes, that happened with the pandemic, to some extent. We'll see over the years how much we stick with this.

But you're right. I mean, the fact that we are now so reliant on these technologies to do everything -- to work, to even talk to each other -- I think has put a greater emphasis on it.

But it's also a vulnerability. If you can go after these systems, if you can take it down, I think that you can see that.

Now, the good thing is, folks, yes, criminals have capabilities, but they don't have capabilities to have a sustained takedown. They can't do it for weeks and months.

Nation states may have that capability, the sophisticated ones. They don't have the incentive to do that unless we're actually at war with them. At a high level, deterrences work because we haven't seen the takedowns of the electrical power systems or others. We've seen things in Ukraine and other places where there's already conflict.

But we haven't seen that and I think it's because the nation states who can do that recognize that if that happened there would be a very, very strong response and so they step back from that line.

The under-the-radar stuff, the stuff that is the norms we're trying to address, that's more problematic.

My short answer to you then would be, I hope not. I hope we don't have a cyber 9/11 at any point. I don't think we need it to call attention to this. And maybe the ransomware Colonial Pipeline, which is an isolated event, was enough to get people interested.

John Curran: Thank you, Chris.

I'd like to tell people if you have questions now, remote or in-person, get them lined up now because we'll close the mics very shortly so we can stay on schedule.

Beverly Hicks: Virtual is clear. We can go to center

mic.

Kevin Blumberg: Kevin Blumberg, The Wire and member of NRO Number Council. We've been in an interesting time over the last 18 months. The security posture, when we went into what many have to full lockdown, really showed the weaknesses. And the miscreants definitely abused those weaknesses.

A lot of companies improved their security posture. A lot of them did it not because of the usual reasons. A lot of them did because insurance companies got sick of paying out. And it's actually good now that we're seeing industries that have been quiet about it -- yeah, we'll handle it; it's a risk; it's an actuarial table -- going, no; we need to see this, this, this and this for your regular company.

My question though is many of the things that you mentioned seem to be not the actual root-cause problems except for one, which is the safe haven issue. Is that your opinion as well, that if safe haven got addressed and there were no safe havens for what is going on, many of the problems that we have today would become much easier to solve or more importantly would dissipate out to much smaller groups of gangs?

Chris Painter: I don't think it's as simple as that. I think safe havens are a major impediment certainly, especially with these ransomware groups and going after them.

They can act with impunity because Putin doesn't really care if they're not attacking Russian targets. That's a huge problem.

But I also don't think if we got rid of safe havens that would be the end of the game. It's still difficult to go after these criminals. We still have nation/state actors. I think it's a big step.

To your earlier point, I think companies and others are taking cybersecurity more seriously, but they're still

not in some sectors.

The fact is when we talk about critical infrastructure, it's critical for a reason. We need to survive -- we can't survive without it or it creates a major crisis.

And maybe the time has come, and I know this is controversial, that we need to set standards for critical infrastructure. The market hasn't worked in that sense, and we have to actually do something.

So I think that would be a big part of the solution, too. It's not just getting rid of the safe havens; it's hardening the targets and making sure we're not wide open to attack.

John Curran: Thank you. Remote questions? No? We're all done. I'd like to thank --

Chris Painter: Let me finish with what the background is. So for those who know me, I'm fond of movies where computers or hackers are the main characters. I had, like, 30 different movie posters on my wall at the State Department, including "War Games" and "Terminator" and "The Net" and all those others.

But this one is -- the story behind this one is my favorite movie, computer movie, it's a very dystopian one as many of them are, called "Colossus: The Forbin Project." 1970, I saw it while I was in grade school. Sat through it twice -- tells you something about my personality.

It's the first movie where computers took over world. The U.S. Post Colossus controls nuclear arsenal, have perfect deterrence, man in the middle. Soviets steal the information. They build one too. They talk to each other. They become self-aware. They take away all civil liberties to protect humankind from itself.

Now this is the actual Colossus in Biloxi Park. If you ever have a chance to go there. It was used to break the Nazi Lorenz code, so higher than the Enigma code.

The first digital, electronic, programable computer apparently in the world, kept secret by the Brits since the mid-'70s until they lost the commercial advantage.

But unlike the movies, this is actually something that will save the world. So I'll end with that and look forward to the panel discussion.

John Curran: Chris, wonderful job.

I'd like to turn it over to Leslie Nobile who will moderate our upcoming panel.

EVOLVING CYBERSECURITY, STRATEGIES FOR THE NEW NORMAL INTERNET GOVERNANCE PANEL

Leslie Nobile: ... internationally by all actors. Awesome talk. Thanks so much.

This sets the stage for the next session, which is entitled Evolving Cybersecurity, Strategies for the New Normal.

During this session, we have a panel of experts. They represent both private and public sector perspectives. They'll be discussing some of the ways their organizations are devising and implementing strategies to deal with this ever-evolving -- these ever-evolving issues surrounding cybersecurity.

The way we'll run it is each panelist will have 10 to 12 minutes to present their views. And once they're all done we'll move into our Q&A session.

Before we begin the panel, I really would like to ask all of you and invite you to review our panelists' bios on the ARIN 48 webpage. It really gives a good sense of their background and the wealth of knowledge and experience our panelists bring today in areas such as Internet technology, infrastructure and governance, information security, law enforcement, cyber crime and Public Policy, to just name a few.

So with that, I would like to now introduce our first panelist, Chris Elverson.

Chris is a supervisory special agent with the Federal Bureau of Investigation's Cyber Division. I'm now going to hand the floor over to you, Chris.

Chris Elverson: As Leslie said, I'm Chris Elverson, a supervisory special agent with the FBI's Cyber Division. I've been with the FBI for 11 years and with Cyber Division for five of those, mainly focusing on cyber criminal threats.

When it comes to evolving cybersecurity, I wanted to highlight simple examples of innovative programs that we've developed to assist with investigations and victim notification and mitigation. But the common thread in all of these initiatives is partnerships.

All of the most successful cases and operations that I've seen in cyber have involved strong partnerships whether between multiple government agencies nationally, internationally or government and private sector.

The reason for this is that no single entity has the entire visibility necessary to tackle the cyber threats that everyone is dealing with.

Private-sector partnerships are the main focus of my unit, so much so that I actually sit at the National Cyber-Forensics and Training Alliance, or NCFTA, instead of FBI headquarters. The NCFTA is a 501(c)(3) nonprofit and was formalized in 2002.

They have over 155 formal partners including the FBI, Secret Service, HSI and Postal, in addition to all of their private-sector partners such as major financial institutions, retailers, cybersecurity companies, universities and others.

The NCFTA provides a common space for all of us to collaborate, albeit a little less face to face since COVID. But we are still able to get together, share

data, share threat intelligence and understand which threats are impacting industry the most, all within a framework that keeps everyone's lawyers happy.

And in fact this integrated, in-person collaboration has been so successful over the years that we've created another hub recently to work with the defense industry, called the National Defense Cyber Alliance, or NDCA, where another FBI unit and cleared defense contractors sit together and share intelligence in real time.

But the real secret to all of this, all of these partnerships and sharing is true bidirectional sharing and not the one-way street that we as government have sometimes been guilty of in the past.

This sharing takes on many forms, but might include bank-sharing accounts where they've detected fraud, the FBI sharing IOCs associated with an APT group in a format that industry can actually use to defend their networks, or researchers sharing online accounts linked to human trafficking or other crimes.

Lastly, we're always trying to expand our circle of collaboration by hosting conferences or summits on the big topics of the day, like business email compromise or ransomware, speaking at events such as this one to hopefully meet new partners who are equally passionate about fighting cyber crime and defending their networks against cyber adversaries.

With that in mind, feel free to reach out to me after the panel today if you have ideas on how we can collaborate to make a bigger impact.

The International Task Force is an effort that began in 2011 with a handful of countries and has grown each year to include over 20 countries in 2019. The concept is that we invite a representative from each participating country to live in the United States and work with us and our NCFTA partners side by side for 30 to 45 days.

While our foreign law enforcement partners are here,

sharing the same office space as us, we're able to collaborate in a very close and continuing way on common cyber threats.

With cyber you can have victims in one country, actors in a second country, an infrastructure in a third country and lots of other things in lots of other countries. But the power of bringing all these countries under one roof really cannot be overstated.

But in addition to what gets accomplished just in the short time that our foreign partners are in country with us, we also build powerful, lasting relationships that often last the rest of the participants' careers. When cyber criminals can create and tear down infrastructure daily, the speed of traditional international cooperation is not sufficient.

Formal legal process between countries can take six months to a year -- sometimes, if we're lucky -- which is just not fast enough. By developing personal trusted partnerships we're able to action international components of an investigation in minutes instead of months.

To top it off, every foreign partner that we work with has unique expertise and capabilities, and we all get stronger by sharing best practices with one another, from how to conduct certain types of investigations to sharing custom tools and analysis techniques.

It also helps to understand who is in the best position based on each country's local laws, capabilities, to conduct arrests or seize assets and proceeds of these crimes.

We all know that phishing continues to be a major problem and is one of the leading ways that victims get compromised. One private-sector partner we work with was trying to tackle this problem in part by collecting phishing kits from all the phishing sites they were discovering across the Internet.

When I say phishing kit, I'm referring to the collection of HTML, PHP, images and other files that make up a phishing site.

When this partner explained to us what they were doing, we thought it was a great opportunity to build something. And the NCFTA began creating a repository to store all the valuable intelligence that's contained in a phishing kit, like the URL it was hosted at, the monikers used by the creator of the kit, and in many cases a link to where all the stolen credentials are being stored.

To make the repository as useful as possible, they included an API that allows partners to connect to the source of intelligence. If any of you out there are collecting phishing kits, please reach out to me and I'll put you in touch with the NCFTA so you can contribute and get access to this resource.

Partners can submit phish kits that they encounter, they can search for kits that match certain criteria to help them with their own investigations that they're doing. And they can download kits of interest for further information and intelligence gathering.

For us as law enforcement, the most valuable data in the kits is where the stolen credentials are being sent, which is most often an email account.

Having access to the kits to be able to make the link between the phishing website and where the stolen credentials are actually stored is huge for us and enables us to do search warrants on those emails where we can learn more about the bad actors behind the account and get access to the stolen credentials, which is a great segue to my next topic.

So one example of using our partnerships to solve difficult problems is the initiative we've developed with the Have I Been Pwned service. During the course of an investigation, as I mentioned in the last example, we might uncover anywhere from thousands to millions

compromised victims' passwords. These often come from search warrants served on email accounts or servers under the control of bad actors.

The challenge for us is how do we notify so many victims? Traditional approaches don't appear to make sense. Even if we could send letters or emails, knock on doors or call millions of victims, would any of it look credible to a victim, or would they think it's just another scam?

And more importantly we need actionable items. So, for anyone not familiar with Have I Been Pwned, they provide a free service where they host public breached data and known compromised passwords in a hash format separate from any other identifying account information.

What the FBI has agreed to do is to provide compromised passwords in the same hash format to Have I Been Pwned so that they can include these passwords in their dataset.

This is a very different approach to victim notification that we've taken in the past, but we believe it will be more effective than any other method at this scale.

Because the data is freely available it's incorporated in many services that people already use, such as password managers and browsers. If a victim whose password has been stolen attempts to log into a site using that stolen password and we've previously provided a hash version of the password to Have I Been Pwned, that victim will get a prompt in their browser or password manager to change the password because it's been seen previously in a data breach.

We feel this gives us the best possible chance of notifying and mitigating victims of stolen passwords at scale. And we're excited to begin rolling out this new capability.

The last example I'll give today is the Internet Crime Complaint Center, or IC3, which you can access on the

Internet at Ic3.gov. It's the FBI's main complaint intake point for cyber crime and related Internet fraud schemes.

Reporting crimes via IC3 is really important because it's one of the best ways for us as law enforcement to know which crimes are causing the most damage and where we should focus our attention.

But specifically for any fraud like BEC, romance scams and others where money has been wired to a fraudulent bank account, the faster a victim files an IC3 complaint, the best chance of getting the money back and preventing a loss.

When a complaint with a loss amount is filed with IC3, it gets automatically triaged. And if certain criteria are met, it gets passed to analyst for additional action.

In cases we're likely to be able to stop a fraudulent wire transfer or have it recalled, the analyst reaches out to the affected financial institutions in an attempt to stop the funds.

If the victim did not provide enough information to the IC3 complaint the analyst notifies the closest FBI field office to the victim so the office can attempt to contact the victim and get the missing information to hopefully continue the process of stopping the wire or getting it recalled and minimizing the loss.

In 2020, based on over a thousand incidents that met the criteria, due to IC3's partnerships with all the major financial institutions, they were able to stop the fraudulent transfers 82 percent of the time, which amounts to $380 million in loss prevention.

Besides this being a great success story to highlight, what well-developed can do, I want to use it as a reminder that if anyone who is watching this falls for one of these scams or knows someone who does, please file an IC3 complaint as soon as possible to increase

your chances to stop the wire and getting your money back.

In summary, those are just a few examples of how we focus on partnerships to evolve our approach to cybersecurity investigations. Some of our partnerships with other federal agencies are more involved and involve more complex responses, especially when dealing with challenging problems like ransomware. And I think you'll see more examples of those in the future.

With that, I can either take questions or maybe questions are being held until the end. Thank you.

Leslie Nobile: Thanks so much, Chris. Really appreciate that. It was great to hear about some of the FBI's initiatives to combat cyber crime. It was particularly interested to hear about your partnerships with industry and private sector. So, it's very interesting and great stuff.

We'll change the order of speakers. One of the speakers having issues getting on. That would be Niel Harper. So we're going to put him toward the end.

And I'm going to introduce Richard Leaning. Richard is the director of trust and safety with Cloudflare. We're going to hand the mic over to him. Thanks, Dick.

Richard Leaning: Good morning, good afternoon. Shame I can't be there. At ARIN, normally I go with the people who know me, and I've seen some usual suspects at the mic already this morning. Hello, Kevin, and the rest of the guys there.

I'm from Cloudflare now. Before I was with RIPE NCC for four years. Before that I was a law enforcement officer at Europol dealing with cyber investigation. So, I understand the frustrations of law enforcement community and obviously now industry who I work for now.

And it was interesting to hear Chris Painter, because we used to do the G8 together many, many years ago when I

had hair and he was the chair and I was the UK delegate.

I just want to briefly touch on some of the bits that both Chrises have just said. Then I'll just talk about what the industry is doing at the moment.

It's interesting to hear about cyber threats and policy threats. I don't think the industry will call them policy threats. They're policies that come in that we have to deal with as a global company and see how we navigate and maneuver ourselves through those.

But one thing that Chris Painter mentioned, which is highlighted in my career and this is part of my job at Cloudflare, is stakeholder engagement, which includes law enforcement to open community, government policy, CERTs -- is there still a gap between some community and the government community when it comes to the Internet.

And I still find that amazing in this day and age. Even though so much effort has been put into that, there's still that gap. Understanding of how the Internet works and how the governments want to introduce policy, regulation, legislation on the Internet. That's been a challenge. And I don't know how to solve that.

One of the things that -- what keeps popping up is this ransomware and how do we stop that.

It's not ransomware particularly. It's all crime. And one of the challenges when I was a police officer and I'm sure law officers are having now is identifying individuals or group individuals that commit these crimes online.

And maybe the focus should be preventing these crimes to happen in the first place. Prevention and disruption is the way forward. Not prosecution, purely. Obviously prosecution is important. But let's try to stop it happening in the first place rather than focusing on catching the people after it's done.

We saw -- brings me on to what the industry are doing,

especially in the last two years, where overnight we've gone from securing workplaces, places of business from cyber threats to individual harms.

Instead of having one building, suddenly these companies, no matter if you're small, medium, large, had to look after hundreds of buildings, thousands of buildings, depends what size your company are.

And that was a huge challenge for the Internet industry because companies like Cloudflare and others, overnight we had to try and work at how do we protect our customers who normally were in one place, now in hundred thousands of places all over the world, basically.

All different places. So what should industry be doing? I think for companies, they're no longer -- they're moving away from having their own internal security departments, IT departments, into moving towards companies that look after the whole footprint, the whole infrastructure they have and letting them deal with it.

Letting them deal with the attacks, the DDoS attacks, the malware, the ability securely for an individual in one location, maybe in a different jurisdiction from the headquarters, to access the databases to do their work securely and efficiently and speedily.

Even from having Zoom calls like this, this is the new norm. Hopefully it won't be the new norm completely forever. How do you make these conversations secure, whereby normally you'd just have a meeting in an office and discuss company's details, sensitive details and then you've moved on from there? Now it's all over the Internet. So how secure is that Internet?

And I can remember because part of my role is speaking to law enforcement. And when COVID happened, trying to find a communication medium that I could actually speak to law enforcement was a challenge.

They didn't like Zoom or they didn't like Teams or they didn't like Skype. It was even harder to speak to law

enforcement because they didn't know how to -- they weren't allowed; they knew how to use these systems but because of internal security policies, they couldn't speak to the outside world using things like Zoom or whatever that is. But that's obviously now changed.

What the majority of industry and what our customers especially are asking is that we look after them, we look after the whole footprint to prevent them being attacked in the first place.

And we do that. We have this thing called Zero Trust Services out there that looks after the whole portfolio of customers no matter what size they are, small to the big ones, to make -- it takes their Internet footprint, their Internet properties, their website properties -- they're looking after the whole infrastructure with one place.

Obviously there's challenges with that because after you have seen some of the outages that -- you know, Facebook have had recently, they're all internal issues not cyber attacks.

But the difference between centralized and decentralized and how that works and making sure they're always available to our customers' customers and so forth.

So that's what the industry has done. And I'd like to finish up on this collaboration that Chris Elverson was talking about. We do, at Cloudflare, and many other companies do this is we do collaborate. But not in the way that you probably think.

We collaborate in the educational side more than anything else because the Internet is so dynamic. It changes weekly if not daily.

It's very hard for law enforcement globally to keep up with the changes. And we get asked numerous times, can we take a website down. Can we block an origin IP? Can we do that? It's just not technically possible.

Or we get this request: Can you tell me who was using this IP address six months ago, a year ago, the date stamp? Well, yeah, that could be a thousand people depending, is it a dynamic IP address or not.

So we spend an awful lot of time collaborating with law enforcement, educating law enforcement on how the Internet is moving, where it works and how they -- to stop them wasting time and going down investigation avenues that isn't going to take them to where they want to go. So that's how the collaboration with what we do.

So I'll stop there because we'll take questions at the time. But if there's any questions now or any comments, then please ask.

Leslie Nobile: Thank you so much for your presentation, Dick, and for sharing how Cloudflare and others in the industry are devising new strategies around cybersecurity. Really just hot topic and obviously needs to happen.

We're now going to go back to Niel Harper as our next speaker. Niel acts as an advisor to the United Nations Office for Project Services, or UNOPS.

I'm going to hand the floor over to you, Niel.

Niel Harper: Thank you very much. I'm going to share my screen just briefly.

Basically I'm in the position of chief information security officer at the United Nations Office for Project Services.

We're a unique United Nations agency from the perspective that we're self-funded. We are paid by other United Nations agencies, by governments' international funding organizations like World Bank, International Monetary Fund and other private partners to implement peace and security projects.

So we're currently implementing around 1500 projects in

120 countries. And that's in addition to our staff which is approximately 10,000 staff. So you would well understand this is a very complex environment to secure.

I want to touch on some key themes in terms of what we've been doing around security. In the last year, as we've transitioned to a remote working environment, we've had to look at how do we better secure our workforce.

And I think what was very good or what we had planned in advance that we had moved to a cloud first strategy. So we were very prepared to manage a secure workforce. We had basically implemented all cloud apps, federated identity, single sign-on.

So a lot of our transition was really focusing on building additional capacity to ensure that all our staff better understood their responsibilities in a working-from-home type of environment.

And we have conducted a traditional mix of information, security awareness training, but also to buttress that with privacy and data protection and training, because part of our concern was around how sensitive data moved, both inside and outside of our organization, especially in a work-from-home environment.

And we've shifted to a number of different types of interventions. We had traditional awareness and training with phishing attacks, newsletters, different types of interventions.

And then we also started to look at focus groups, focus groups, looking at higher risk functions like our technology functions -- who had different training needs. So we had a tiered training for that.

We also train our recipients as well because we do a number of projects around the world. And we looked at how could we expand our security awareness and training to our field offices as well, because we did have a lot of recipients who would be managing some of our projects

on RB that have.

So how to integrate them through different form-factor types of training, using tablets and mobile devices. And what was also important was the multilingual approach because we do the work in several languages.

We've also had a number of projects looking at capacity building as well in Eastern Europe, South Africa and other places where we were supporting the training of the recipients.

For example, in certain countries we're building out new data centers. We would train their staff on building secure data centers, looking at physical security, helping them to progress to becoming certified in ISIL 427-2001 [phonetic] and SOC 2. So really focusing holistically on both our own internal workforces but also the recipients of the projects that we were delivering in the field.

We'd also partnered across the United Nations agencies and we formed a United Nations information security steering committee, where all of the various United Nations agencies, like up to 27, we would come together and we would develop norms and standards for different security, whether it be technologies, whether it be processes or training to better develop the United Nations system personnel to better respond to these cyber threats.

And we also had interventions of course more at the UN Secretariat stage in terms of the GA as well as the open-ended working group where we were looking at international cyber norms and cyber diplomacy, ensuring that state actors understand what behaviors were needed or expected online, and ensuring that they not just understood those behaviors, but they committed to those behaviors through policy changes and national political advances as well.

I also want to talk about the development of our secure applications ongoing development as well. We had

focused a lot on, as I spoke to before, on our cloud first approach. And we looked at how we would refactor our on-premise systems to be cloud native. Then we were looking at how we apply benchmarks or hardening standards to different environments whether it be the AWS, Google and cloud platform in our multicloud environment.

But we also developed a robust end-to-end process for embedding privacy by design and security by design into our system development lifecycle, ensuring that we were developing systems to secure first and that we didn't have to go back and secure systems afterwards.

So looking at static and dynamic coordinate analysis tools, looking at peer reviews, building a more robust environment in terms of how we use our development environment.

We would also conduct penetration testing before we moved our systems into production. So really focusing on that we're delivering customer-oriented services, whether this be to internal or external customers, we were always looking at security by design.

We have a very robust technical architecture and triage process. And this is both for UN-specific systems but as well as for the systems that we're developing for our end recipients. So out of those 1500 projects, many of them include delivery of IT solutions.

So we wanted to make sure we weren't leaving our customers, especially experienced recipients in developing nations, we weren't leaving them to their own devices. We're providing our own in-house expertise to support the robustness and resilience of their solutions.

I want to talk about the sustained sectors (indiscernible) collaboration. Sorry. Our supply chain at the United Nations Office for Project Services, we have tens of thousands of suppliers because we're working in 120 countries, and because of our project

density we have a number of contractors and subcontractors, and they do expose us to a lot of risk.

So we really had to retain our supply chain and third-party risks. So we would have looked at how we refreshed our procurement procedures as well as introducing a security and privacy and supply chain process where we would take a lot of our contractors that were focused on delivering either information systems or data-centric solutions and taking them through this process to assess them for compliance with international standards like ISIL 427-2001, SOC 2 ensuring that we had data protection agreements in place to ensure that we could respond to any regulatory requirements like GDPR or other GDPR-type regulations across the international footprints where we worked.

We also spent a lot of time working with developing countries, helping them as well to understand the supply chain risks affecting their governments as well, especially when there would be developing national solutions such as digital IT platforms.

I want to touch quickly on our sustained sector collaboration as well. This is something that's very important for us at the United Nations, really working with public and private sector actors to share threat intel, to share information, working with law enforcement to look at multilateral-type exchange of information to support crime fighting.

We've done a lot of that especially in jurisdictions where we were helping with each judicial reform or helping with the law to employ and train law enforcement.

We participated with NISSA in terms of looking at public/private partnerships. We've also worked with FIRST around supporting the work with Computer Security Incident Response Team. And we also engaged in a lot of national, regional and global discussions around how to build capacity to respond to cyber threats.

And these are just some of the things we've been doing at the United Nations to really support building resilient and robust online systems.

Leslie Nobile: Thank you so much, Niel. That was very informative. Really interesting to hear about some of the ongoing work and projects at the UNOPS and at the UN in the areas of cybersecurity.

Our last speaker on this panel will be Doug Montgomery. He's the manager of Internet technology research for the US National Institutes of Standards and Technology, or NIST.

I'll hand the floor over to you, Doug.

Doug Montgomery: Thanks, Leslie. Tell me if the slides are up.

Leslie Nobile: We see them.

Doug Montgomery: I wanted to take some time this morning to talk about one example, one instance of government response to sort of the evolving new normal and cybersecurity policies to address sort of the changing landscape.

One of the things I wanted to point out is we talked a lot about evolving use cases, cloud first, remote work. Certainly that is something that's part of our landscape nowadays.

Something we haven't talked much about this morning is evolving technology, where when you look at today what's going on with software-defined and programmable networks, networking as a service, new management and control paradigms, many things that used to be a single device of playing some role in network-critical infrastructure, today is a dis-aggregated software implementation, some of which is running in public cloud.

It's a much more complex and dynamic technology

landscape that we're trying to protect. We talked a lot about the use cases and the other panelists have already talked about the use cases, the cloud first and remote work.

The prevalence today of operational technology, be it IoT consumer or industrial IoT, that presents technology end-use-case challenges where the types of devices and the deployment scenarios are really significantly different than commodity IT systems.

And the threat space is evolving too. There's a greater recognition of vulnerabilities in both the software and hardware supply chains. All these new use cases and technology scenarios post significant challenges to traditional approaches to cybersecurity.

And in many cases, many of these points are borne out in recent news, greater use of automation, there's a lot of focus nowadays on AI and machine learning systems to try to automate issues of control and security. But we can't forget that that actually just shifts the complexity and the robustness issues someplace else, right, to these advanced automation and control systems.

One instance of looking at a government's response, if you will, to the changing landscape is the new, relatively new, from May of this year, executive order on improving the nation's cybersecurity. I work for NIST as part of the federal government. This executive order representatives the marching orders for government agencies, both those involved in the technology recommend and normal mission agencies in addressing sort of this evolving landscape.

And the executive order has tasks in it for many agencies, not just NIST, NIST/EHS, Federal Trade Commission, trying to address many of the issues that have been talked about so far in the panel, removing barriers to sharing of threat information between the government and private sector. Many of the panelists talked about that.

Modernizing federal government cybersecurity, really taking significant new steps to look at software supply chain security, addressing issues of cyber response and detection and improving our ability to detect vulnerabilities and incidents.

I was going to talk about a couple of these areas that are related to NIST activities. One is supply chain. No doubt inspired by many of the incidents that made headlines for a while, you know, the realization that a software update was a threat vector really hit home recently.

And so NIST has been tasked with looking at two specific classes of software and taking measures to improve the supply chain trustworthiness, if you will.

One is to look at what is labeled critical software. This is basically the kinds of control software, software that runs at elevated privileges, management software, software that is involved in the critical operations of network infrastructure. And there's a series of activities here that you can follow the URLs and look at -- we were tasked with defining what we thought that subset of software was, of what would be thought of as critical software, producing metrics and techniques to characterize the security properties of critical software and develop minimum recommended standards for vendor development of verification of software. So this is looking at the most critical components of network information systems.

The other area that has received lots of attention, once again there are news events that might inspire this, is looking at consumer-grade Internet of things devices.

And there we've had a long series of activities of developing baselines of recommended required security capabilities for IoT software. But the executive order has also challenged us to work with the Federal Trade Commission to devise some means of raising consumer awareness of the security properties of IoT devises and software. There's this notion of developing labeling

programs for consumer products.

The second area we're active in is the area of Zero Trust. I think Richard mentioned the move to Zero Trust architectures. NIST has been taking somewhat of a leadership role there and basically trying to define and codify the notions of Zero Trust. And Zero Trust is one of the hotter buzzwords in the industry. Almost everything is labeled "Zero Trust" as far as I can tell.

But getting to a position where the basic tenets of Zero Trust architecture can be realized, which is migrating to software-defined parameters in which both policies and the integration of all sorts of information sources from outside sort of the traditional network operations realm of threat intelligence, behavioral analytics, cyber hygiene data to both affect very find-grained policies on every instance of communication.

That's something new. And so there's lots of discussions of instances, parts of that puzzle -- cloud access brokers, multifactor authentication -- but really looking at what it takes to get to a real and complete Zero Trust architecture is the focus of a couple of projects we're working on.

Our National Cybersecurity Center of Excellence is conducting Zero Trust pilot projects and developing guidance in this space. This is a public/private partnership project with lots of players where we're really decomposing at a much finer level of detail what the fundamental aspects of these Zero Trust principles are for individual use cases like enhanced identity governance and micro segmentation.

And so these projects are meant to demonstrate to our users, our stakeholder base what the fool realization of Zero Trust architectures could and should be like, and the fact that you can't achieve those kind of architectures with commercial products.

The other thing I would like to talk about, which may not be thought to be specifically cybersecurity related,

but I think is as a basis of ongoing infrastructure, is we're also involved in the US government's transition to IPv6-only networks.

This is a government initiative that was announced in November 2020. There are lots of details to it, but what we're trying to convey to industry is that it's our strategic intent for the federal government to deliver its information services and operate its networks and access the services of others using only IPv6.

There are various milestones in the proposal. But we are trying to move the technical basis of government network information systems to a v6-only posture.

Why do it now? Some people might ask why would the government do that. Often thought that we have a reasonable amount of IPv4 addressing.

Why now? Certainly we've had initiatives in IPv6 going back, frankly to 2005. But a major effort was launched in 2010.

Getting there now is, in short, significantly easier than it was in 2010. We think the product base, in terms of major operating systems and their support of IPv6, is reasonably mature. Certainly IPv6 support in ISPs and other service providers has significantly matured.

And to some extent v6 deployment is advancing at a rate where government agencies who have v6-enabled, public-facing websites are seeing the majority of their traffic come over v6.

And this isn't just an initiative that is undertook in the US government. There are other certainly large enterprises and service providers, ARIN has a nice repository of use cases, example use cases that are trying to achieve the same goal.

Why are we trying to get there? For me primarily this is about removing technical and economic barriers to

innovation.

On the right are the logos and references to various innovative efforts in networking, be it for consumer IoT, SRv6 for core network switching and service enablement, disaggregated radio access networks.

There are all of these areas in which the innovation in network technology is occurring in v6 and not so much in v4. So, our goal is to provide a modern network protocol as the global barrier service for interoperability.

There was a previous panelist that talked about the issues of identifying who is using addresses and whatnot. And we see globally unique network addresses as a significant requirement for new security architectures -- things like doing Zero Trust. We'll rely on the ability to identify in our current disaggregated world, where half of the users are at home, they're accessing services in the cloud, they're accessing services within the enterprise and all of those environments. We need to be able to express policy and look at behavioral analytics that transcend all of those places.

So we're hoping that -- we see globally unique addresses as a key enabler of that. We think it's also an enabler for innovation in network security technologies. And finally, the goal is to reduce cost and complexity in networks.

You could ask why go to IPv6 only. Clearly we'll have to migrate between the ubiquitous dual stack but we think that's possible nowadays. The goal is to get to the strategic goal of operating one network stack.

We think that there are enough pieces in place to get there or on the horizon. We know getting to v6 only will require work in some areas, primarily in what I will call adjunct functions of software installation, maintenance, management, monitoring.

But our intent here is to send a message to vendors that we want to get there. We want to buy products that operate on v6 only networks.

And with that I'll conclude.

Leslie Nobile: Great, I'll take it from there. Thanks so much, Doug, for your presentation. It was really interesting to hear more about the technical aspects of securing our networks and about the US government's initiatives towards improving the nation's cybersecurity. Really good stuff.

Before we move into our Q&A, I'd like to extend a sincere thank you to all our panelists for sharing with us how their organizations are working to identify and defend against the ever-changing nature of cybersecurity threats.

Unfortunately it's very evident that cyber threats and attacks are becoming increasingly sophisticated, malicious and disruptive, and that they'll continue to present challenges to the global community for the foreseeable future. So this is where we're at today.

With that, I'm going to -- I think we're going to move into our Q&A session. And I'm going to turn it over to Bev for help with our audience questions.

Beverly Hicks: Sure, thank you so much.

Hollis Kara: Absolutely, let's wait a second and see if we can get everybody up on screen.

Beverly Hicks: They're working on that now. Those in the room that may have questions can approach the center mic.

Hollis Kara: I want to extend my thanks to Leslie for all her hard work in putting together this panel and get our speakers together and get this great content out for you today. It was a great add to the meeting. And I hope everyone enjoyed it.

Beverly Hicks: Mr. Montgomery, can you stop sharing your slides?

Hollis Kara: Bear with us one moment. Okay, so we've lost Mr. Harper, that's okay. Wait, he's back. Yay!

Are we ready to start with some questions?

Beverly Hicks: We are. Want to start with center mic?

Hollis Kara: Yes, center mic, all you.

Leo Vegoda: Hi, Leo Vegoda, And Polus LLC. I have a question relating to my experience in receiving abuse reports --

Beverly Hicks: Could you possibly speak a little louder into the mic?

Leo Vegoda: Sure. I have a question based on my experience of receiving abuse reports when I've worked as an RIR and when I worked on the IANA team. These were always reports about addresses that weren't actually allocated or were reserved in some way.

And typically these reports came from people who did community policing and have no specialist expertise. So the panel has talked about cooperation at the high level between federal agents, UN agencies, industry and government.

I'd like to understand what kind of cooperation is happening so that the people who really understand how to investigate cyber crime are passed those reports or the people who do community policing are trained so that they can investigate those reports competently.

Hollis Kara: Leslie, did you hear that question?

Leslie Nobile: I did. It seems to me it might be directed to Chris Elverson. Chris, do you mind taking a stab at this?

Chris Elverson: I'll be honest, I think that's a tough one for the community policing. We certainly appreciate every group out there that's able to have a hand to help make the Internet safer and help identify scams and frauds. And we've definitely worked with some of those groups in the past.

I don't know that I have a great blanket answer to that, but I think maybe, if you're aware of specific groups or specific instances where that's come up, I definitely would be happy to connect with those groups. And maybe through some closer collaboration we can make sure we're on the same page and on the same technical expertise level and that we're actioning those to the full capability. That's probably where I would start.

Leslie Nobile: Thank you, Chris.

Dick, you've been on both sides of this as well. Do you have anything to contribute to that?

Richard Leaning: Yes, the challenge is that all crime now has a presence on the Internet. So investigations that are conducted by law enforcement officers globally, no matter where you are, there's always a presence on the Internet.

So therefore, for us, we do have community police officers, we have police officers from very small units asking us those types of questions because it's no longer just a realm of specialist cyber crime units investigating crime on the Internet. Now it's across the whole board.

We spend an awful lot of time -- I spend a lot of time educating those officers, hoping they get it through their unit and for a bigger audience. It's always challenging over the last two years because ideally we'd love to have face-to-face conferences and educational seminars with whole groups of officers to cascade it down. But it is a challenge.

And law enforcement, even where I'm from, the UK, they're not very good at speaking to each other and sharing that type of information. So it's trying to hand pick how we can cascade that information, because you can't educate every police officer on the globe obviously. So we are looking for collaboration with federal -- Chris is with the FBI or the NC in the UK or the BK in Germany, and we kind of look at how we can state that information down. That's definitely a challenge.

That's part of the educational piece is the understanding of how the Internet works. Because it's no longer officers in specialized units. It's every police officer needs to know how about the Internet and how it works to conduct any investigation.

Leslie Nobile: Great, thank you, Dick. Hollis, are there other questions?

Hollis Kara: I see Mr. Harper has his hand up. If he would like to contribute to this before we move ahead. Unmute.

Niel Harper: I'll start with the work that's been ongoing at the international communications. To begin, there's a particular project focused on capacity building around law enforcement. And this looks at a number of different things, like support for legislative reform, both around substantive and procedural legislation.

They also look at training on computer forensics, both in terms of accessing devices and content, but also on guidelines for engaging with online service providers to gather information so that you can successfully prosecute cyber crime.

I've also been working with a project at the European Union level called the Artherious [phonetic] Project, which really focuses on across-the-board access to electronic evidence.

And that's being delivered through Europol, Eurojust and European Judicial Network. And that's really where a large number of capacity building sessions, both face to face as well as online seminars, are around developing capacity within law enforcement to really prosecute cyber crime.

And the last thing is while INTERPOL have a number of projects working with a number of different stakeholders and key partner countries who have law enforcement.

Finally I'll speak on the regional security system in the Caribbean region, which is a group, I think, of seven countries, which includes law enforcement and military. And they're also involved in capacity building and training to support fighting cyber crime.

Hollis Kara: Wonderful. Thank you.

If we have any questions from the floor, if I could ask you to line up now because we'll be closing the microphones soon. But I know we have a few virtual questions that are waiting in queue. So, Beverly, if you want to take those away.

Beverly Hicks: We do. The first one is from David Huberman from ICANN. His question is for Chris Elverson.

Sir, thanks for the awesome and informative presentation. I'm curious how often the FBI cyber division relies on the public Whois records during the early part of investigations. Is it still an important tool, or has the law enforcement community moved to a post-Whois stance because of things like GDPR? Thank you.

Chris Elverson: Yeah, that's a great question, and it's certainly not the first time that we've been asked that. I know there's been a lot of effort over the last couple years, since GDPR, to try to get a better idea in the community, how important is this Whois tool and what kind of effect is it having to try to justify making

Whois closer to what it was before versus is it really fine and people are kind of upset over nothing.

Unfortunately, it's really challenging on our part because Whois lookups, I would say, are very much kind of at the early stages of an investigation typically. It's hard to measure how big of an impact did that have.

Of course, individual stories will come up here and there, how that's been a frustration of it being more challenging to link different Internet infrastructure together like we traditionally would.

But I don't have any solid numbers on that unfortunately, so it's hard for me to give kind of a quantitative answer. I will say, as far as moving past Whois, we've definitely gotten a lot better and, I think, improved our skills with using tools like HASP, DNS and other internet infrastructure tools to try to better link infrastructure that's likely related together and to go that route.

And we've certainly had participation in ICANN and the Public Safety Working Group and those kinds of entities to try to have a voice in that discussion.

As a whole, the more information that we can have available to help us do our job is certainly appreciated. But there's obviously differing viewpoints there. I don't know if I helped.

Hollis Kara: Thank you. Do we have one more question, Bev?

Beverly Hicks: We do have another question from Louie Lee, ASO, Address Council, Google Fiber, whether the criminal activity is a true cyber crime or is the Internet just a component of that overall activity? Is cryptocurrency now the predominant way that money is transferred between criminals of all sizes and scale, and also between the criminals and their victims? How is the IC3 approaching cases where money transfers happen via cryptocurrency?

Hollis Kara: Chris, this looks like it's back to you.

Chris Elverson: I think that was a three-parter. I should have been keeping notes. Can you repeat the first part of the question.

Beverly Hicks: Sure -- whether the criminal activity is a true cyber crime, or the Internet is just a component of the overall activity? Is cryptocurrency now the predominant way the money is transferred between criminals of all sizes and scale including criminals and their victims? And how is IC3 approaching cases where money transfers happen via cryptocurrency?

Chris Elverson: All very good questions. Honestly, is something a, quote/unquote, cyber crime versus what we would designate another category we've used, say, cyber-enabled crime?

This is a topic that has come up for at least the last decade, probably longer that just predates my time. And if you can believe it still comes up today. It's a bit of an awkward thing.

I think on one hand, people want to label something as "cyber" because it's important to have -- obviously there's a lot of different levels of expertise and nuance for anything that's enabled by the Internet.

And it's helpful to label something as cyber so that we can develop that expertise and have people that know how all those different aspects work to assist in investigations.

But at the same time it's important to not lose sight of the fact that almost every crime is essentially cyber enabled at this point just because of the reach that the Internet has.

So we have to be careful not to -- we can't label everything "cyber crime," per se, or then nothing is cyber crime. So that's something that we try to balance

internally. And I'm sure over the years and decades to come you'll see fluctuations and how organizations label that.

At the end of the day the most important part is we need to work it, whether it's significant crime, whether it's truly cyber, cyber enabled or something else, if that's significant and it's impacting victims we need to work it and let's not worry about what we call it.

As far as cryptocurrency, definitely there's been a huge upshift in when money is moved. How much of that happens through crypto versus traditional money-exchange methods.

Again, I apologize I don't have specific numbers to point to. But you referenced IC3. I can tell you from their data, typically the next hop, if your money is stolen and it goes into, probably a temporary fraudulent money unit account, the next hop out of that account is likely either an exchanger to send the money overseas or a crypto exchanger to convert it into cryptocurrency and continue processing it from there.

And I can't speak to a specific effort from IC3 on how they're handling that, but we certainly have cryptocurrency teams and more traditional money-laundering teams that definitely help out with all investigations that involve money, which is most investigations, to try to track that money down. It's really case-by-case how successful we're able to be with that.

Beverly Hicks: I have one last question, from David Huberman of ICANN. My question is for Doug Montgomery.

I hear you that NIST is studying ways to better educate consumers on security standards. In your expertise in this area, do you think it's a practical and achievable goal to try and get manufacturers to incorporate baseline security measures in their devices, or is that not realistic.

Also wanted to say a quick thank you for your public RPKI measurement tool. It's super useful in the research purposes.

Doug Montgomery: Thank you for the last comment. Delivering useful test and measurement is our goal.

So this issue has been discussed a lot. I should say that our tasking so far is to outline the framework of how, in particular, if you're talking about the consumer space, outline a framework by which we could raise consumer awareness of the security properties of IoT devices. I think it's a big challenge in the consumer space.

We've had workshops on this in the past. We've discussed analogs to things like energy-awareness labels. During one of those workshops on the fly I sort of went to Amazon and tried to see if any attributes of security is something that I could search on for IoT devices, which of course there isn't.

So I think it's a big challenge in that space. But the first step is having some way of characterizing the effective security level of a project.

I think time will tell. In communities in which you can control acquisition, Federal government being one, certainly you could have acquisition requirements to buy devices and products at a certain security level.

So in those environments, through the power of purchase, I think you could influence vendors. The consumer space is more difficult. I mean, you can go on the typical e-commerce sites and search the energy efficiency of appliances, but that affects the consumer's budget, right. It's an attribute that's -- ramifications are directly to the consumer.

So, I think it's a challenge to have real impact in that space. But the first step is to be able to characterize some level of security properties at the different levels.

Hollis Kara: Thanks. I do see that we have one more hand raised from Mr. Harper. I did want to ask --

Beverly Hicks: There's timing.

Hollis Kara: Yes, we do need to wrap up, in the interests of time, but I just wanted to give Mr. Harper an opportunity if he had a briefly comment that he wanted to add to that question.

Niel Harper: Just a quick point about embedding security in so many devices. You're seeing a number of ways, one has been through Trustmarks and we have laboratories, if you look at Europe -- NSA is building out a Trustmark type of framework where they're validating certain products such as from a privacy and security perspective.

You're also seeing kind of market pressure through consumer advocacy groups to better inform consumers to make better choices around which products are secure and privacy enabling.

And finally you're seeing some industry standards as well, as you look at them. But there's TSACs, which is a standard for connectivity vehicles, where in Europe you're seeing the standard being enforced on any partners in the supply chain. You have to be PSAC compliant to provide software to a connected car manufacturer.

So we're seeing a number of different ways. And the final way, of course, can be through regulation where it's mandated by new law.

Hollis Kara: Wonderful, thank you for that contribution on that.

I think we'll close the microphones with that, and move on to our next presentation.

I'd like to invite our chief operation officer, Richard

Jimmerson, to the stage to give a brief ARIN operations report.

ARIN OPERATIONS REPORT

Richard Jimmerson: Hello, everyone. I'm Richard Jimmerson. I'm really happy to be with you in person today. It's been a long time. The last time I was on an airplane was January of last year. I drove across. So I'm glad to be here. Glad to fly in with you.

I also want to thank that panel. That was an excellent panel. And thanks to Leslie and all the panelists for an excellent presentation.

I'm going to move pretty quickly through my slides to keep us on time.

Just a little bit about ARIN operations. Some of you might be curious, how is the ARIN organization running through the pandemic. And largely that's what I'm going to talk about here.

Our staffing at remote operations, in March of 2020 we transitioned pretty well. We actually surprised ourselves how well we could transition, but we went 100 percent.

But since last summer we've had people coming into the office on a regular basis. And that continues today. However, we're not 100 percent back into the ARIN offices yet. However we strive in this remote participant work environment to continue to provide great customer service to you guys. And I trust that you're finding the results of our efforts there.

We continue to watch guidance from the CDC and everyone else about when we might go back into the office and what that looks like. We also have some discussions lined up with the ARIN Board about what that's going to look like, so that we can share that out to staff.

After some research that we've done with an external

firm about what that will look like, post pandemic, and some polling that we've done with the staff organization about what's important to them.

Some organizational highlights, since last time we met. The 2021 work plan is fully engaged. And we continue to operate in this pandemic work environment. We've got -- typical in-person outreach continues to be delivered virtually at a lot of events that we do throughout the year, where you can log in and do those virtually. Not much in person this year, but we expect we'll have a lot more of that next year. Hope to see you guys there.

We continue to enhance our ARIN online product and our routing-related services for all of you, and we hope you've seen the results of that. And I want to let you know that the demand for registry services continues to grow. It's not shrinking, it's growing.

I know a lot of us wondered what it would look like in a post-IPv4-depletion environment for the operations of a regional Internet registry. The answer is that there's more work, not less work with an IPv4 market and continued interest in routing security services and other services we offer. The demand for the services continues to go up.

I wanted you to know, since the last time we met, we did add a vice president of information security to the senior leadership team inside the organization. His name is Christian Johnson. He's been with us just for about two months now. You'll get to see him at an upcoming ARIN meeting once he's been on board a little bit more. But he's already starting to make a very strong impact inside the organization.

ARIN 49, the next ARIN meeting, we'll be meeting in April 2022. Right now that's planned for in-person participation in Nashville, Tennessee. It will likely be delivered just like the meeting that we have here this week.

And we're going to continue with enhanced remote

participation facilities, understanding that not everyone will want to come to the meeting even in April of next year.

And, of course, these plans are subject to changes, depending on what happens with the pandemic. We're very hopeful that we'll be in a state that can meet in person.

With that that's the end of my presentation. Happy to take any questions that you have and answer those. I'll also be available at lunch. If you have any questions, happy to answer them in person. Thank you, everyone. I'm going to transition -- do you have a question online?

Beverly Hicks: There are no questions online or in the room, so we're ready to go forward.

Richard Jimmerson: Thank you, Beverly.

I'll introduce John Curran. He has a few words to share with us just before lunch.

John Curran: Okay. I want to take a moment here because we're on -- some major changes going on. This is a big year for ARIN in terms of some of our volunteers, some of the members of the community.

I don't want to spend too long between you and lunch, but I want to highlight the fact that we have some people who have been serving in the ARIN community who won't be serving with us because their terms are ending or their period of service. So with that, I'd like to first say some of these people you know and love. I have -- there we go. Thank you.

Gary Giesen, from the ARIN Advisory Council, served a term this year, filling in another year. And Gary will be ending his term this year. A round of applause for Gary.

(Applause.)

Thank him for his service.

A name we all know on the ASO AC, also known as the NRO Number Council, Louie Lee. Louie Lee will be stepping down after some-19 years serving for ARIN.

He literally has defined the ASO AC. And we all know him through the years. And Louie's hat will also be stepping down after 19 years of service.

(Applause.)

Quite a few Louie shots. Really instrumental to the organization. Someone who we could not have had a successful ASO AC without Louie's leadership and guidance. So just very pleased to do that.

Finally, Paul Andersen. Another long-term person at ARIN, Paul served 18 years both in the ARIN Advisory Council and then on the ARIN Board of Trustees for 11 years, and the last five years as chair of the ARIN Board of Trustees.

Truly another person who we cannot live without but we're going to try as Paul's term is ending and he's stepping down as a trustee.

We've had many, many years with Paul. And very happy to have his leadership and guidance. ARIN really matured as an organization throughout these years. It's become much more professional under his leadership. He's brought the voice of the members to the organization.

And so I'm just very pleased to recognize his enormous service. Paul, if you could come up for a moment. Many years with Paul. Come on up, Paul.

(Applause.)

In honor of his many years of service, I'd like to present this to Paul, recognition of -- recognition of your fine service on ARIN. It's been wonderful to have

you. You've made a huge difference. If you want to say some words you can say them now or later. We have an opportunity then.

Paul Andersen: I'll just thank John for the opportunity. I'll have some more words later, because I don't want to be between me and lunch, and I'm still recovering from those pictures.

But honored to engage on behalf of the membership. And I look forward to watching from afar.

John Curran: A huge round of applause for Paul.

And with that, we're going to head to lunch. I will now have Hollis come up to do the final.

Hollis Kara: All right. Lunch break. It's lunch. For folks that are here with us, we've got box lunches that will be out the doors and around the hall. Please help yourself. You're welcome to bring them back in here to eat.

For folks who are doing this virtually, you can leave the stream up. It will keep running. And we'll be back with you in about an hour. And we hope you're enjoying the day.

Box lunches, I covered that. Virtual attendees, you don't need to leave. I said that, too. I need to remember to use the clicker and we're at ARIN. Thank you, enjoy your lunch.

[Break]

Hollis Kara: Welcome back. Here we go. So first off for this afternoon I would like to welcome John Curran back to the stage to give an update on fee harmonization.

FEE HARMONIZATION UPDATE

John Curran: Thank you. Okay. Welcome back. I'm John

Curran, president and CEO. I'm going to talk about the fee harmonization project we've been doing this year. So let me be pretty brief.

We're changing the fee schedule in January. We're transitioning the end users from an annual per resource fee to registration fee schedule. The fee that all ISPs have been paying. This way an address block is an address block is an address block.

We provide the same services for them. We don't want to get into a circumstance where someone wants to use an ARIN service or wants to use their address block in a different way. We tell them, no, you're a lesser -- you don't have the same set of services.

For equity, we already have people now who are using the address blocks in a lot of different ways. They might have been assigned in one way. They're using them another.

We don't want ARIN services or fees to be an impediment. Policy? You can decide whatever is appropriate in policy, but services and fees are now the same. So everyone has the same fee.

These start at $250 a year and as your resources go up by four the fee doubles -- so 250, 500, a thousand, two, four, six, eight -- that's what the ISPs have been paying all this time. Now the end user is paying on the same schedule.

If you're a typical end user, and you've got an ASN and an IPv4 block, you are paying 150 and 150 a year. Now, you're probably -- you could be paying only 250. A lot of people dropped in their fees $50.

If you have a lot of address blocks, then it depends on what they sum up to in total size. Again, you're category is based on the sum of your IPv4 addresses and the sum of your IPv6 addresses -- we look at whatever category fits that. And that's the fee that you pay. Transition legacy resource holders, the same schedule

for those who signed an LRSA, only we're maintaining the legacy resource holder cap.

When we did legacy RSA, they added in the fee schedule, a cap on the total fees paid by legacy holders. And we're enforcing that -- we're still honoring that, and that means that even though the fee schedule says you'll pay 250 or 500 or 1000, if you're a legacy resource holder, you'll pay 100, 750, soon to be 175, 100 -- 200 the year after. That cap applies if you're a legacy resource holder with resources under agreement.

Some day, year 3022 or something, all the legacy holders will pay the same as everyone else. We just have to get there, $25 a year until we add it all up.

We maintain the temporary IPv6 waiver, organizations in the small X category. So, by the fee schedule, you'd be asked to get something smaller than you may like. And this allows you to get a larger block without incurring a larger fee for IPv6 people who thought that they shouldn't be artificially restricted in block size.

We implemented fees for recovery transactions, and after the community consultation people said a hundred dollar Org-create fee is an impediment, so we lowered it down to $50. We increased the transfer processing fee to 500 to better reflect costs.

Your transfers are all funds, squirrelly and hairy. There are exceptions, but you'd be amazed how much work the transfers are, to make sure we're doing a good job keeping track of who has the rights to a block.

70 percent of the end users either have no change or reduction in fee. 49 percent of them pay the same. 21 percent pay less. There are 30 percent who are paying more. There's some that are paying remarkably more.

If you're holding on to a /8, you've already heard from me; I've already called you. I've made a number of the calls. A number of the customers are aware that their

address sizes create some very large fees. But this is, again, the same fees that others in the community have been paying for the same services for the same block size.

Actually, the reception has been more rational than we've probably hoped for. We're expecting a lot more heat and light. And when you tell people you're moving everyone to the same schedule, they understand, even if their personal circumstances may be awkward.

Timeline, we did the consultation. The Board adopted next year's fee schedule in June. We announced it. And then we started to do the outreach I just talked about.

If you get your invoice starting in 2022, if you get invoices starting with your fees due in 2022, you'll see these changes. We give you two months in advance. The invoices are going out now. We'll begin to reflect these changes.

That's all I have. The last slide is questions. The microphones are open, at the mic and remote.

Beverly Hicks: Just a reminder to state your name and affiliation before you speak, that we have a live transcription going, so everyone can try to speak to the speed of that. And if you are at the center mic, if you could please make sure you're close enough and loud enough for our virtual audience to hear you. And you're welcome to go with center mic. We no questions virtually.

John Curran: Go ahead, Chris.

Chris Woodfield, Twitter, ARIN AC alumnus. What financial modeling has been done to project the impact of this fee change to ARIN's annual income for the coming year?

John Curran: As it turns out, and this actually showed up in the online consultation and some of the materials we sent out, ARIN's fee schedule is, when we do the

change, we end up, if everyone were to pay, some people may consolidate as a result of this and that would reduce it.

Some people may transfer to another region. But it would be about $3.6 million of increased revenue. We go from 22 to 24 and change.

Now, ARIN hasn't raised the fee, that basic ISP fee schedule, in many years since it was established. Actually we added lower categories.

So this catches us up on that. And it also addresses a gap that we had. So this puts us slightly above our costs, not materially.

The gap that we have is that we've been instructed by the Board -- the Board made a very good planning decision that said, we shouldn't rely on investment proceeds in making our budget. Every year ARIN generates between a million and 3 million in investment proceeds.

And we used to calculate that into the budget and spend that money. Starting this year, we no longer build in the investment proceeds. So suddenly there's a gap. We'll talk about more of this later when we have the treasurer's report.

Paul Andersen: We've also changed our risk profile.

John Curran: Right. And we changed our risk profile to make sure the investments are well preserved. But we no longer are focused on the investment return. So we want to have operating expenses aligned with operating income. That's substantially what happens with this change as well.

Anyone remote?

Beverly Hicks: No remote. Go ahead.

John Curran: Center mic.

David Farmer: David Farmer, University of Minnesota. When I read the 25 percent increase cap, I always assumed that was compounded annually, so it's not 25 percent of the initial.

John Curran: $25, not percent.

David Farmer: I thought it was percent.

John Curran: I'd love it if it was percent. I'll look to see if there is a typo, David --

Paul Andersen: If you could just sign the amendment, we'd love that.

John Curran: But it's $25. If you think about it, we had initially about 130 --

David Farmer: The other was the --

John Curran: It was actually in the first LRSA for about a hundred customers. We got rid of it, but it's always been on the fee schedule. It's A $25 cap.

David Farmer: It was in mine. It was $25? Okay.

John Curran: Yeah, so if you've got a /16, it's going to take us a while.

Anyone remote?

Beverly Hicks: No remote. Go ahead.

John Curran: Center mic.

Lee Howard: Lee Howard, IPv4.global. The change in transfer fee, all the fees are effective the start of the year, right?

John Curran: Right.

Lee Howard: Are they effective as of the date that a

transfer ticket is submitted or the date that the invoice is generated?

Paul Andersen: We'll get back to you on that.

Lee Howard: Cool, that would be great because I have some systems I need to update.

John Curran: The effective date is the date you initiate the transfer or the date you close the transfer. Oh, when you put it in.

Lee Howard: The date of the ticket.

John Curran: Submit early and often. All right. And remote participant?

Beverly Hicks: There are no remote participant questions, but a beg from the transcriptionist that we try and make sure we're speaking -- you're actually doing good -- they were just making sure that even those who are asking questions speak at a pace that she can keep up with.

Paul Andersen: I apologize to the transcriber in advance.

John Curran: Understood. And we're going to be closing the mics soon. So if you have a question get to the mic. Center front.

Ron da Silva: Ron de Silva, Quantum Loophole. My question is, in your /8 example, what's the new fee for a /8 holder?

Paul Andersen: What's the fee for a /8, or someone who has total holdings?

John Curran: You'd have to look at the table. I don't have it off the top of my head. John, for /8?

Paul Andersen: Gonna be two XL? Would it not?

John Curran: 120 -- 250, it might be 256, 250 -- the top of the table is $256,000 annual fee.

Ron de Silva: I was just doing the math, if somebody has a /8, and I'm looking at the brokers in the room, that's an asset that's probably six, 700, maybe $800,000,000 dollars in value, maybe.

So it's an ongoing expense against that. Not that much. I guess I was just wondering if you anticipate this increased fee for people sitting on big blocks would encourage more recycling, but maybe it's not a big enough fee to encourage that.

John Curran: Let's talk about this. First, there's people paying that fee right now for their blocks registered. So, again, this isn't anything new.

The question is, is someone -- someone who is an end user, who is a legacy end user -- because that's probably someone with a /8 -- can come under the LRSA and right now they'll pay $175 because there's a cap of legacy users who come in.

So the invoice would show, yeah, you're paying 256, but you're only paying -- 256,000 -- but you're only paying 175. If I was a legacy user, I would try to take advantage of that ability. We're still offering it for new people, new legacy holders coming under agreement. That may not be the case forever.

So if anything, Ron, it's probably the other way around. It's an incentive, if you're a legacy holder, to very quickly get registered, because I'm not sure if ARIN is going to provide the cap to incoming new legacy holders going in perpetuity.

Paul Andersen: Just adding to that, to kind of answer your question, it's possible, maybe just not in that example, but any of the larger holdings that there could be an incentive to that, but it wasn't the driving factor from the Board. It was equitability. That just might be a side effect, good or bad.

John Curran: John, did you want to correct something?

John Sweeting: Just to correct that, up to a /8, not exceeding it, is 64?

John Curran: Right.

John Sweeting: From a /8 up to and including a /6, is 128. And anything over a /6 is 256.

John Curran: 256, right.

Paul Andersen: I assume that Ron's question was just for those large --

John Curran: Yeah, it's on the website for the fee schedules. That's the fees it's been for 10 years. The only difference is they now apply to end users as well.

Okay. If there's no remote questions. No?

Beverly Hicks: No remote questions. We're all clear.

John Curran: Thank you very much. I'll turn it over. The next speaker is Paul, and he's going to give our membership update.

MEMBERSHIP UPDATE

Paul Andersen: Thank you, John. I don't think this will be a long one either. So we have a consultation open right now. And it ties into, this is a bit of an output of the fee consultation in that certainly we heard from a lot of end users that if we were going to harmonize the fee schedule, that the benefit should be -- and obviously one of the benefits that comes from being on a Registration Services Plan is membership.

Having said that, we also heard from a lot of end users that they did not necessarily want to be active in ARIN's governance.

There are certainly a lot of customers of ARIN who come, want to use ourselves, want to pay their bills and that wants to be the extent of their involvement.

This causes some issues when we look at our governance because there are lots of thresholds throughout bylaws and the Virginia Nonstock Corporation that involve quorums and quotas and thresholds.

So, we've decided to try and make a second-class member. The first is everyone who is a member today is a general member. And to be a general member today, you're either on a Registration Services Plan -- that's all our ISP customers today -- or you're an end user who has voluntarily paid a fee $500 a year to become a member.

We're suggesting to create a second class, which will be called Service Members. This is a concept for those that wish to not necessarily be involved in ARIN's act of governance. And our proposal is that all the end users that -- all the end users who will be harmonized, will become Service Members upon January 1st. But having said that they'll have the option to move to a general membership. They'll simply need to, I believe it will be through ARIN online is the goal, pending the amazing engineering team which, pending this consultation output, will implement that. But assuming the consultation continues generally on (indiscernible), that would be the expectation. If you are an end user and you want to become a general member, you'll go click. You'll make some attestations that you will be involved. And you'll become a general member and have the right to vote.

The one thing we'd like feedback on is what we've proposed, there's going to be a responsibility not just on end users but also on RSPers to maintain your general members. Because we'd like to have it that the people who are in that general membership are people who have an interest to be engaged.

And we've suggested at the end of 2023, if you have not participated in one ARIN election, that you will be

automatically moved back to a -- you'll be moved to a Service Member at that point. And you'll have to remain there for one year before you can switch back. After that you can switch back by going through the process.

The feeling was that there should be some bar. We think the voting, which only takes a couple seconds, was a fairly low bar and that you only had to do it once out of every three elections.

There would be warnings from the ARIN staff if you were starting to get to the point where you were going to lose it, so you knew you had to vote. And that's generally what we've put in.

Having said that, there's a community consultation in the ASCPE. So we encourage those that have not already to go look at some of the good feedback we've already got on ARIN Consult or to approach a microphone, virtual or not, right now.

With that, I'll take any questions.

Beverly Hicks: Thank you so much. For those who approach the microphone, or those who are typing their comments in, we remind you to speak clearly, type name and affiliation into your comments.

There are no virtual at the moment. You can take center mic.

Paul Andersen: Center microphone, name and affiliation.

Kevin Blumberg: Kevin Blumberg, The Wire.

Paul Andersen: A little louder, Kevin, because I can barely hear you.

Kevin Blumberg: Kevin Blumberg, The Wire. Good governance is not easy. None of what you're putting up here concerns me overall, except for removing somebody as a member because of nonparticipation.

I would recommend don't tie it to just one thing, the elections. Give as much latitude and leeway as you can, whether that be participation in meetings, whether that be -- because some organizations actively don't want to vote but want to participate as members.

So you're on the right track, absolutely. Having people that do nothing doesn't really help. But at the same time, try to give as much latitude to those who are participating.

Paul Andersen: I think that's good feedback. I think the struggle is we were trying to keep simplicity. And given that the main -- again, they're not losing membership. They're simply transitioning to a different membership class. And those that are able to participate in the election are the general members.

And I guess the question we have is if you're not voting in once every three years --

Kevin Blumberg: There are many reasons for organizations not to vote in a given set of years. As long as they're participating, do not refuse them the ability to exercise that when it is important.

It's absentee that you're trying to deal with. So I realize it's more work, but try to give as much latitude.

Paul Andersen: One thing we discussed, and I'm curious, was -- do you think those members, is the concern that they don't want to vote because they don't want to endorse or whatever they see as a candidate. But would you be fine if you could go into the voting booth and just say, I wish not to vote this year, but I'm here?

Kevin Blumberg: I'm here to participate. My participation is no vote would be just fine.

Paul Andersen: Can I get the gentleman behind, because I think he wishes to either add or subtract what I just said. Name and affiliation, please.

Warren Kumari: Warren Kumari, Google. Guys, thinking if you could have an abstain option in the voting. That way you've at least shown that you've done your stuff.

Paul Andersen: That's been some internal feedback that we bantered around. Because would it be that you would not vote and then make some attestation that there's a reason? Or could we just make that as part of the voting process to keep the engineering and the flow simple. That's great feedback.

I think we have a Q&A. So let's go to that.

Beverly Hicks: At the moment looks like he's attempting to type. There it goes.

Louie Lee, ASO, Address Council, Google Fiber. Would an abstention vote be counted as a vote?

Paul Andersen: We would -- speaking only in my theory, because that is still something to be fleshed out, I'm sure we'd report on it. It would not increment any of the vote tallies, but they would have been seen as a voter.

John Curran: You participated. You participated in the election.

Paul Andersen: It's an abstained, spoiled ballot, whatever. I think the specifics we'll get into as we get deeper -- but, yes, thank you for that question.

Any other questions? Otherwise we'll close the microphone and move on to try and make some time.

Again, if you don't have some feedback you want to give now, please -- on the Mailing List is great. Grab any of the board members or staff. We'd love to get your feedback. We want to try to find something that works here for everyone from a governance perspective.

With that, thank you.

John Curran: Thank you. I'm now going to have our next -- I'll invite our next speaker.

Hollis Kara: Next on our docket, I'd like to invite Leif Sawyer. Is he queued up and ready to go? Let's give us a moment to get Leif live on the feed.

ADVISORY COUNCIL REPORT

Leif Sawyer: I'm Leif Sawyer. I'm the Advisory Council chair for this year. Next slide.

We have 15 members on our Advisory Council. They're all up on here, some of them in person. They've all done a great job working this year through the pandemic, dealing with the virtualized reality that we're living in right now. I want to give them a big hand for everything that they've done and everyone that's standing up for reelection this year. Good luck and I hope everyone in the room has planned on voting or has voted already. Next slide.

So on our plate, currently we have six draft policies, one new Policy Proposal and one Recommended Draft Policy. Next slide.

We have three working groups that we formed in January of last year to tackle specific tasks: The Policy Development Process Working Group; Number Resource Policy Manual Working Group; and the Policy Experience Report Working Group.

We take feedback from staff regarding how the meetings have gone and trying to wrap them back into the experience.

I said response from people for the policies coming from the meetings. Next slide.

Our PDP working group is currently reviewing the PDP. They've had some relevant updates that they've sent off to staff and legal. We'll be doing an internal review

with the Board of Trustees. And then it will go out to the ARIN community. So you'll have a chance to look over the changes that the working group is proposing.

If everything goes well and we'll submit it back to the Board for adoption and then to the staff for implementation. Next slide.

NRPM Working Group has been reviewing the current policy manual and has focused suggestions in sections 2, 6 and 12. They are working very strongly on this, and they've got some editorial and noneditorial changes that are coming up. So we're looking forward to seeing some more of those. Again, those will also go out to the community for your review. Next slide.

As I mentioned about the Policy Experience Working Group, they're reviewing the latest Policy Implementation and Experience Report from the last meeting. And then also they'll be reviewing from this meeting. And they'll conceptualize those changes. Next slide.

Lastly, please vote. Your vote is important. The voices out there are critical to maintaining the growth and function of the ARIN community. So I'm looking forward to seeing the results of this year's voting.

And that is all I have. Last slide, please. Any questions?

Hollis Kara: Beverly, are we ready?

Beverly Hicks: I'm looking to the virtual poll as well as in the room. Looks like we have someone ready, center mic.

Hollis Kara: Center mic, you're up.

Tina Morris: Tina Morris, AWS, ARIN Board. It's not really a question, but a comment. Many might not know how much the AC does with other RIR meetings. In a typical travel year they'll attend the meetings and

learn how policy is working or not working in other regions to try to bring it back educationally for ARIN.

During this time they've been attending remotely, dealing with time zones and still going to them meetings and doing that hard work. I just wanted to make sure they got credit for that. Thank you.

Hollis Kara: Thanks, Tina.

Leif Sawyer: Thank you, Tina.

Hollis Kara: Do we have anything coming in?

Beverly Hicks: I currently have nothing virtual.

Hollis Kara: If there are no further questions, I think we can close the microphones and move on.

Leif Sawyer: Thank you, all.

Beverly Hicks: Thanks, Leif.

Hollis Kara: Next up, we'll bring in Nancy Carter. She's our treasurer on the Board of Trustees, and she'll be giving our Financial Report. Do we have Nancy ready to go?

Beverly Hicks: She's ready.

Hollis Kara: There's Nancy. I'll step away and let Nancy take over.

NANCY CARTER

Nancy Carter: Thanks Hollis. And hi, everybody, good afternoon. Sorry I am not there with you. I'd much rather be there than here. But I was unable to attend.

So I know, as always, the ARIN treasurer's report is the highlight of this meeting. And I know that's what you're waiting for and why you're still on this Zoom webinar. So, here we go.

With no further ado, I just want to acknowledge that I could not serve as treasurer without the help and support of the ARIN staff and my colleagues on the Board of Trustees.

I'd like to really thank the Financial Services Department for their continued dedication to evolving financial reporting in metrics and their commitment to providing remote financial services over the past year and a half.

So thank you and a big shout out to Brian, Ray, Tammy, Melissa, Tanya, Cathleen, Amy and Amaris. Congratulations on all of your accomplishments this year. This is the team that makes my job as treasurer so easy. And I'm happy to share some of their accomplishments in my presentation. Next slide, please.

Today I will update you on this year's activities of the Finance Committee. I will then review the 2021 revenues, operating expenses and budget variances, look at ARIN's financial position, provide highlights of the investment portfolio and then finally look at the net assets. Next slide, please.

As you can see, the CFO and I continue to keep the Finance Committee extremely busy. So far this year we've met nine times. We managed the move to our new investment consultant earlier this year and transferred all the ARIN investments to the new custodian.

The portfolio was rebalanced during this transition process to align with our revised investment objectives that were alluded to earlier.

We reviewed the investment policy statement again very recently and made a small wording amendment to align with how we manage our budgeting process.

The committee met earlier this year with our new auditor, BDO, to review the 2020 financial statements. Those statements were then recommended for Board

approval. We heard very good things from the auditor about their experience with the ARIN team during the audit.

They were very complimentary about working with Brian and his team as well as others in the organization. As a fiduciary for ARIN, this positive feedback is important and welcomed.

As an extension of that audit process, with the new audit firm, we also reviewed and the Board subsequently approved the 2020 IRS 990 Form for submission.

And finally, you should know this is my favorite time of the year. It's budget time. Management presented the 2022 budget to the Finance Committee in October.

The Finance Committee recommended approval of that 2022 budget at a very recent Board meeting. And the budget was approved. So more on that at ARIN 49. Another reason to attend ARIN 49. Next slide, please.

This chart shows you total revenues for 2021 to the end of September. You can see that our revenues are tracking to budget. Annual registration fees are the largest product line in the ARIN revenue portfolio.

These revenues were 14.3 million through the end of September, making up almost 90 percent of total revenues. The revenues have grown by $400,000 compared to 2020 amounts.

Initial registration fees are the next largest product line in the portfolio. And those revenues were 1.1 million through September, which is unchanged when compared to 2020. In aggregate, by the end of September, ARIN's revenues were 3 percent ahead of 2020. Next slide, please.

This chart shows some statistics about our resource holders. You can see that the nonlegacy IPv4 and IPv6 resource holder customer increases continue to occur mostly in the small categories.

The number of organizations with IPv4 or IPv6 resources have grown by 368 since March of this year. And that's an increase of two and a half percent. Most of that growth occurred in the small to 3X small categories as expected. Next slide, please.

This chart illustrates ARIN's billing activity, which may be interesting to some of you. Financial services prepares a lot of invoices, averaging approximately 2300 invoices per month.

Next slide, please. The operating expenses. The increase in year-over-year expenses through September was $1.2 million. This increase was expected given budgeted increases in the number of ARIN team members.

The staff head count increased from a year-to-date average of 80 in September 2020 to a year-to-date average of 86 and a half in September 2021.

As I reported in April, the pandemic continues to limit the spending in several other ARIN expense categories.

This resulted in a total $1.1 million under-budget variance by the end of September. In total operating expenses were 15.9 million to the end of September, which resulted in a 6.5 percent variance from budget.

On the next slide I'll highlight the major variances from the 2021 budget. If we could move -- as I noted, the material budget variances are depicted on this chart. The largest operating expense variances occurred due to limitations on travel and in-person outreach activities during the year. This is not surprising. These limitations drove the budget variance of $1.1 million.

Next slide, please. The statement of financial position or the balance sheet continues to represent ARIN's highly liquid financial position. ARIN has more than $39 million in liquid assets as represented by cash, accounts receivable and investments in order to meet its

ongoing operating needs.

Our health cash position means that we're in a good position to manage fourth quarter expenses and will not need to draw on our investments in the short-term.

Next slide, please. ARIN's investments. Even with the transition to a more conservative investment objective, as you heard Paul and John talk about earlier, the long-term reserve fund increased almost 10 percent during the nine months ending September 2021.

We ended the third quarter of our fiscal year with total investments of$34.5 million. The Finance Committee and ARIN staff continue to work closely with the ARIN consultants to manage our investments.

That will be the focus of our November committee meeting when we're scheduled to review the consultant's performance and that of the portfolio.

Next slide, please. Net assets are shown in this chart. So our net assets grew to $30.3 million at the end of September. This is 2.8 million or 10 percent more than net assets at the end of 2020. This favorable net asset position was driven mostly by the impressive investment returns over the year, but also by the lower than budgeted expense in the first three quarters of this fiscal year.

Next slide, please. The net asset coverage ratio is illustrated on this chart. The increase in net assets and the underbudget operating expenses are expected to result in an improved operating expense coverage ratio by the end of 2021. This is something that I reported on at the last few ARIN meetings.

The impressive investment returns this year are expected to grow the operating expense coverage position by about seven percentage points.

And with that, I turn to my last slide, please. Thank you so much for your attention. I'm more than happy to

answer any questions.

Beverly Hicks: We also have Brian Kirk on to answer questions as well.

Question at center mic. Go ahead.

Lee Howard: Lee Howard from IPv4.Global. Thank you very much. Nancy, you always say, sarcastically, I know everybody's waiting for the Financial Report. I was going really I was -- can you guys keep it down, please, thank you. Because I was here for this. Right?

Now I forgot the question I was going to ask you.

Paul Andersen: It will come to you.

Lee Howard: Since we have Brian, who I haven't met, a question more staff, rather than treasurer question. If that's okay.

When we're in the process of doing a transfer, sometimes the recipient will be pushed into a new fee category. They're receiving more assets. They move up a fee category. Or they're just a new member.

And at the end of the transfer process, RSD approves the transfer and then we wait for the recipient to notice that they have a new little due bill from the ARIN for their new fees. It would be really nice if we could have that review done at the beginning of the process so the recipient knows ahead of time they may have to approve some funds and get a contract LRSA approved.

John Curran: We can work on that. That's a valid issue. It's something we can calculate while the transfer's going on and there's no reason we have to surprise you at the end.

Mike Burns: Mike Burns, IPTrading. I noted it was noticed that there was a change in the investment profile and you said it was a change to make it more conservative.

I was wondering if you could share the reasons for that change.

Nancy Carter: Sure, I will. Then I'm going to call a friend and call Brian, who is right there.

So there were a couple of reasons. We were perhaps exposed to more risk than we would have liked based on our previous mix of investments. And when we changed to a new investment advisor, we worked through that quite diligently to understand how we could better protect ourselves while still being able to take advantage of significant returns.

So we just balanced it a bit in a way to make sure that we didn't suffer from huge changes. Does that make sense?

Brian, help me.

Brian Kirk: I would reiterate that as well, both in '18 and earlier in 2020, the investment portfolio took rather large hits.

And when we brought on the new investment advisor, we thought it wise to go through an exercise to talk about the appetite for risk and the appetite for that volatility.

And given the level of the investments, it was decided to really take a step backward in terms of our risk portfolio and be a little more conservative.

Mike Burns: Thank you. I think it should always be a conservative portfolio. That's just my opinion. Thank you for the information.

Beverly Hicks: No questions virtually.

John Sweeting: John Sweeting. To Lee Howard's question, we started doing that two months ago.

John Curran: Lee, we implemented your request before you asked for it.

John Sweeting: I have to give credit to Lisa for that information and actually for initiating that and getting it done.

John Curran: Thank you, RSD team, for being on top and initiating that before it was asked.

Lee Howard: Fabulous. I'll go check our transfers and see why they're not ready for post approval.

John Curran: Any other questions?

Paul Andersen: I like this is good way to go out.

Lee Howard: Lee Howard, IP4global. I remember my other question, which was I did a count and I think there's about 20 people in the room who are not either ARIN staff or official volunteers.

And I'm kind of wondering, you noted, Nancy, that the expenditures are down because, of course, we didn't have meetings. I'm wondering if maybe we'd like to see a cost per participant report on doing the face-to-face meetings.

I'm wondering if maybe we're spending a lot more than we might think we are for the participation we're getting.

John Curran: Let's ask the question just so I understand. Let's presume the cost per participant is $5,000, though I didn't see the caviar out in the break room, would you then suggest based on that cost that we not hold these meetings?

Lee Howard: I think there's a number where I would suggest we not hold the meetings. I don't know if the number is 5,000 or 50,000 or five million.

Looking at staff time, it's not the caviar, it's the hours that people are here. Even more than the travel.

John Curran: I'm a big -- there's a lot of cost, particularly people may not know it, but the hybrid format, as we noted earlier, has a lot more moving parts. So the people who are here are very busy making this all work.

Lee Howard: Amazing job.

John Curran: Having said that, I guess we do feel a certain obligation to have an annual meeting and let people talk to one another and talk in the halls, if we can have one safely.

And I would like to think that hopefully we'll see a higher attendance. I'm just wondering -- I'm all for data, and we can figure it out. It would be interesting. But I'm hoping it's a transitory condition.

Paul Andersen: If I could add a bit. We already do publish some costs, travel reporting costs, for a lot of these travel support that we provide. Because I think you're homing in on the travel support or the cost to hold the meeting and it just doesn't make sense given the nut to cull the meeting -- I think we'd be very hesitant to count it on this meeting, because I think we knew this was always going to be a transitionary -- one of the things we found out holding virtual meetings was that the policy meetings actually went very successfully virtually and was the reason we didn't go hybrid this time.

Because at the heart of what we do is policy and that was successful. That's why we chose to at least leave that one. I think you make a valid point. Now that we've had that experience, we've been forced, like the rest of the world, into more virtual, that whether we need two in-person meetings a year or is it one, or do we find a more economical way to cover. I think that's going to be a challenge for the next board.

Lee Howard: To John's point, we're legally required to

have a Members Meeting, part of the charter.

Paul Andersen: We could hold it virtually.

Lee Howard: We should continue that conversation, A. As I was looking around, it's 20 people. We agree we want to be colocated with NANOG that's a good thing, we get good participation, and that's the right thing to do. And until you're here you don't know how people show up. It's a weird time. I'd like to pay attention to that particular kind of metric.

John Curran: Thank you.

Nancy Carter: Thanks for the feedback. It's hard to know how many people are in the room, it's good to know and something we'll dig into.

Beverly Hicks: No questions virtually. I think the queues are clear.

Paul Andersen: Okay. I'll go into the final presentation before we get into our --

John Curran: Let's thank Nancy.

BOARD OF TRUSTEES REPORT

Paul Andersen: Oh, and thanking Nancy. Thank you, John. I'm out of practice, clearly.

I have a very, very short Board report because, first of all, most of the stuff that the Board has been filtered up you've already seen through the presentations you saw this afternoon and with Richard just before the break.

Having said that, the first thing I'll say is please vote. I don't have a slide. But I'll just say please, please vote. Please take as much time as you can to dig in. There's lots of information on all the candidates.

It's very important to our governance that people go read the applications, read the -- review the campaign

form, which is online and the speeches. But please vote.

It's just the more that vote, the more that that system as I know as a Board member in what we do and having the support. Some of the things we've been working on since we last spoke was some minor stuff such as the attestation document that was required has been phased out.

Obviously you heard about the fee harmonization numbers update, which we continue to get feedback on the numbers update.

We have obviously been very closely watching the developments in AFRINIC, and John has put out a statement to that effect. But we obviously continue to watch that.

And a small but important logistical item, we were able to hold our first hybrid meeting in the summer, actually early fall. We were able to get the Board or much of the Board in person. Thanks to the staff that pulled that off to make sure that the in-person and those that could still not travel, that we had a very successful meeting.

So we, as Nancy mentioned, it's budget time. She already covered that. And the other thing that we've been working out that I've been speaking about that's been in our midst for some time is that we've had a Governance Working Group working on a lot of governance issues starting actually January of last year.

It's been a longer process. But it's actually now coming to fruition. We expect to have consultations hopefully coming late this year.

A reason you may not have noticed, obviously we acknowledge there's been heightened awareness to governance in the last two week. The entire Board is aware and very thankful for the feedback that the membership and community's put on the Mailing List.

To give an update, also from the standpoint, it's standard practice to do a review of all the committees and we'll be doing that for some communities tomorrow, as you can see on the agenda that we published.

So we acknowledge there's room for improvement for sure there. And we look for feedback today on the Mailing List or directly, whichever you feel most comfortable on any issues.

And it doesn't have to be related to nomination committee. It could be Board selection processes or size, the feedback that the Board has been given in previous years and this year to the Nomination Committee. We really look for that feedback on that.

With that, I'd like to give some thanks. This is, as I said, my final Board chair report tomorrow as part of our succession planning, which is one thing that the Board has been working on, both from a staff and a Board level. Not just from the proverbial best approach, but how do we continue to make sure that the organization all around has new people coming up executing the succession plan from a Board perspective.

I'll be stepping down as the chair tomorrow and the Board will be selecting a new chair. Having said that, I'll take this opportunity just to say a few words before I get off.

When I became chair it was big shoes to fill. The guy before me, apparently he did a few things in terms of the Internet.

I tried to figure out what we were going to do in terms of a mantra perspective when I took over. As John alluded, we just tried to find ways to raise the level of professionalism and energy and just keeping as a world-class registry. And it's important to see that we never saw that ARIN wasn't great, had a very professional staff. We just thought that since ARIN's inception, the Internet had grown considerably, both

just in terms of scale, the number of members and customers we'd had had grown. But also the complexity as we see the Internet as we all know has become quite intertwined.

We've been trying to push that strategy. By the way, all the accomplishments, by the way, I'll take all the credit for it, it's very important to understand that this was never possible without staff.

And staff, I want to be very clear, when we came and started to try and bring up new ideas, they're very receptive. They gave their suggestions and most importantly they executed it and did all the hard work. We'd not be able to stand up here and toot accomplishments without the staff. So John and entire staff, I thank you for that.

Through tenure, it's been very important to elevate the game. We made it through IPv4 runout. Even though I know it was the longest story and all the issues that came up creating and maintaining the market. And I think we've been very successful at streamlining that, making it more efficient even although there was more room to grow.

We made it through the transition of the US government oversight of the IANA function, which was a very big issue. We've heavily invested -- the organization, when I joined the Board, was half the size, roughly, from a head count. And that was because there was a clear need to put more resources all around.

In outreach, with IPv6 coming and IPv4 runout, the communication team did amazing efforts and hitting conferences, launching ARIN on the Roads, just to name a few, that allowed us to make sure that the engineering team stepped up when we said we wanted to deal with the massive backlog of requests, not just from dealing with those requests but prioritizing them.

The idea of the word of a customer, that we have people who just want to come and use our services, making sure

they get treated that way.

The concept of trying to see what are the products that ARIN offers and trying to enumerate that and from a lifecycle standpoint was something we pushed.

Getting ready for the fact that we're a more 24/7 operational nature with RPKI. We enhanced fiscal planning and management. And we did try wherever to put more transparency in outreach from publishing minutes and agendas.

We put guidance to the Board needs, and we posted travel expenses. And we really have taken a mantra with staff that if there isn't a good reason to expose it, we should try and be public. And we've had very good support from that.

And from a Board perspective, I'm very proud we've increased diversity from background -- and at the Advisory Council, actually, from background, gender and geography.

And the Board, most importantly, has transitioned to a more strategic role. We've tried to get out of the operational issues that the early Board had to deal with when it was a much smaller organization. John leads, as I said, a very professional staff.

And the Board has just tried to be looking longer. So we've moved to a much longer term strategic planning process.

We're now doing a much longer outlook to give them perspective where we think things need to go. And tri to let them deal with the day-to-day stuff.

I'll stress again, it was very appreciative of staff. We had a very large agenda.

There were some, I think, initial trepidation. But they took the list and ran with it. And I really, really appreciate that.

From a thank you standpoint, it's been a long time. I've met many of you, become good friends. I've watched many grow, date, get married, kids.

We've unfortunately had some losses. But that's the one thing I will definitely miss is the many of you that I call friend and have met and also from a professional network.

I won't try and name individually. I try to think of who I might thank, but I realize the list will be too long.

So I'll thank my family who I think is happy that I'm -- I guess that's one test that we had during COVID, was my wife decided that, I think, she could put up with having me home more often, because I think she did enjoy having me out of the house every so often on travel.

But that's good. So to my family for all their support. And to -- I think I heard it said by Kat Hunter -- everyone who has heard the sound of my voice over the years, I thank you because I could not have done it without you.

And a few closing thoughts. I'd urge you all that I think it's obvious that we do struggle from a community that there's a smaller, I think Lee mentioned, again it's pandemic-driven maybe now, but a smaller number.

I think I urge and challenge the community to find ways to get people more engaged. That's not just getting more people into our process, but let's be open to finding different ways to engage in general to get more people active.

18 years ago, when I came here, I found it very daunting. And it took several years before I could approach many people in the room, the idea of talking to the CEO was just unheard of at that point.

Let's always be careful. We're a very tight community.

And that's beneficial, but for newcomers, let's just make sure that we welcome them.

As I said, as a community, let's challenge ourselves to keep raising the bar, not just as an organization, but as a community that we can continue to improve how we do and how we execute our mission.

With that, that's my closing remarks. I thank you all for your time and with that I wish you adieu.

John Curran: Open Mic. You've got one more final Open Mic.

OPEN MICROPHONE

Paul Andersen: One final Open Mic session. It's a good thing there's nothing on people's minds they might speak.

The microphones are open. Approach a microphone if you wish to tell me how wonderful it's been the last 18 years, or anything else that might be on your mind.

Beverly Hicks: Doesn't look like we have -- I'm sure they're frantically typing.

In the meantime, we have somebody at center microphone.

John Curran: Center microphone. Name and affiliation.

Mike Burns: Mike Burns, IPTrading. I was reading a book at lunch, and John Sweeting came over, asked me what it was.

The title was "Geniuses at War." And he said, Ow, you shouldn't be reading that before open mic.

So, John, I accept the compliment. But I'm not here to go to war. I'm here to go into a battle. It's just a skirmish.

It's a change from the NomCom to remove their ability to

exclude qualified nominees, candidates.

I think that it's a perversion of the traditional NomCom role which, after all, was beating the bushes for candidates. To have them, instead, act as a gatekeeper. They operate in the dark. It's totally unnecessary, in my opinion, to have, at the core of a stakeholder governed entity, a black box of this sort.

And today I've posted my explanatory letter from my rejection. And I invite the community to read that.

It's evidence of the darkness of the process. And I think it needs to be changed. Thank you.

Paul Andersen: Thank you for the comment. Of course I do appreciate the feedback. I would note that, first of all, like I said, the governance workgroup has done a lot of investigation of other organizations' structure in these areas, both within the iSTAR sphere, RIR sphere and elsewhere, other not-for-profits of like sizes and potentially missions and such. And there is a wide range.

There are certainly nomination committees that select boards. There are nomination committees that put recommended candidates, if they're ones that do, as you say, do a very simple evaluation.

I think the feedback is very important. And we certainly see that there's improvement, if not to the level of change I think is something that the Board will consider. And I think that feedback is useful.

So thank you for that. I don't think we have another Q and A.

Beverly Hicks: We're still clear virtually.

Paul Andersen: Next question.

Actually, I wanted to add one thing, while you're pausing. And Mike and I definitely agree that we could

do better on the feedback. So thank you for raising that on the list. Next person.

Marlene Martes: Marlene Martes with AWS. On a more positive note, I just wanted to give a special thank you to Amanda, Bev, Hollis and Leif and the rest of the ARIN Advisory Council for putting together a spectacular Fellowship Program.

I for one am very grateful that there is an in-person meeting at this time. I feel for newcomers, especially, considering wanting to expand the ARIN community, having the in-person meetings are vital. So thank you.

Paul Andersen: Thank you for the feedback. The Fellowship has always been well received. Center microphone. I can see, too.

Patrick Gilmore: Deep Edge Realty. I'd like to comment on the NomCom.

Paul Andersen: And former ARIN Board member.

Patrick Gilmore: Former ARIN Board member, who has been through the NomCom. I was nominated three times before I got onto the slate.

I'd like to preface this by saying I would like to make a statement that I'm greatly displeased by the structure of the NomCom, but the people on the NomCom are following the rules.

And I'm sure they did that with careful consideration and integrity. I'm not trying to blame anybody for what they did, but the rules around how they were forced to do it.

At the end of the day -- and if you read the documents, this isn't in there -- but the NomCom's idea was to ensure only qualified candidates made the slate. But we had six spots possible.

And we have a former ARIN Board member and a former

ICANN Board member who were not selected. So clearly it had nothing to do with whether they satisfied the qualifications. There's some other reason.

And the fact, as Mike said, that this is a hundred percent black box. It's not that they don't publish, they're not allowed to publish the reasons.

And turns out even the candidates themselves can't get the reasons that they weren't selected. So this is bad in many ways. Not only can the candidates not improve so they can get through the next time.

But from an external point of view, like if we were looking at this, for instance, as a third world country, it could be seen as the Board picking two board members and those board members also picking a few community members by themselves, following rules that are published but not any actual feedback given as to what rules were followed or why the selection was made.

And then people on the outside looking in going, it looks to us like the rules weren't followed. I mean, I'm sure there were reasons. But nobody knows them and nobody ever will because we cannot at this point. And this is not how a community-driven organization can possibly sustain itself.

It needs to change. I've been asking for it to be changed for nearly a decade. And I think we've finally got enough community support to make a change.

I have suggestions, lots of people do. But it's Open Mic. I'd like to say it's got to change now, please.

Paul Andersen: Thank you for two points that you raised. First of all, the NomCom is composed of community volunteers. People who can see the list. They're well-respected community volunteers. And we can disagree with the output that they had, the parameters they worked in.

And that's correct. I certainly see as the Board that

it's a Board issue, that we have to look at the structure going forward.

And to the second point I want to raise is I agree with you that certainly we've highlighted the transparency issue and how to approach it. Thank you.

As we have no virtual questions, we'll take the next center microphone. Name and affiliation.

Ron de Silva: Ron de Silva, Quantum Loophole. And I also rise to speak to this governance and feedback for NomCom. It's in that light that I stand.

And I, first of all, commend you all because I think some of the governance leadership that's come into the Board has been directly because of your leadership as Chair.

And I'm encouraged to hear that there's a regular ongoing sort of self-assessment and that's good, healthy behavior for a board to be doing.

What I'm sharing now is really meant to be feedback and to that ongoing work of the Board to figure out how do you continue to do your work and do it effectively.

And going through the petition process and going through the NomCom process and all those other things to get here today on the ballot, I've had a lot of you approach me personally and share stories and issues and concerns. And I'm really grateful for that.

I put together a number of scenarios that I would like to share. And this is in no way intended to be some reflection on the existing NomCom or the process that may or may not have been used by the NomCom. Because we don't know. As everyone said, it's a black box. And that's okay.

The things I've heard from people that I don't think they want to stand up and talk about it, I thought why don't I make these generic scenarios so I can share them

and everybody can think about them. And as you take it back as a board, what are some changes and improvements you can make to address them.

Scenario one, it's this: What if a NomCom member has conflict? You've got a small group right now working in the black box. What if one of the NomCom members has a conflict, maybe a prior relationship or a personal vendetta against a candidate? There could be character attacks. There could be libel, even subtle duplicity, doubts, issues done in closed doors, and the other members of the NomCom don't have an opportunity, really, to explore those, address them, understand them, raise objection to get outside information because it's the nature of a closed box.

I think requiring the NomCom to interact with candidates, okay, issues have been raised, so why don't you have the NomCom then interact with the candidate in the process of the evaluation?

In particular, I think, Mike, you were saying the NomCom shouldn't be deselecting candidates. That's one issue I think probably good for you guys to take back and think about.

But assuming the role of the NomCom is still to ensure you're putting forth good candidates, and one of the things that the NomCom does is assesses background information and gets character information, but you need to take that, I think, in an accountable way back to the candidates and have a dialogue and explore, here are issues, what say you. Scenario number one.

Scenario number two illustrates the same thing. What happens if a member of the NomCom has a direct material business relationship with somebody outside of the NomCom, let's call that person Richard.

And the NomCom member is being held hostage or being pressured into certain outcomes of the NomCom process that are in the interest of outsider Richard.

Again, this previous or future promises of business can be used and held against that NomCom member. And if other members of the NomCom see one representative behaving in a way and don't have an opportunity to get the candidate's perspective on, hey, what are these being raised, why is this pressure being applied? I think that's unfair. And it doesn't really provide that accountability of the NomCom to the membership and specifically to candidates.

Scenario number three. I have four. Thanks. Number three, what if a NomCom member knows nonpublic information about a candidate, let's call that candidate Merv, where another member of the Board was, say, a prior victim of Merv.

Is this information discussed in closed doors about Merv and the prior behavior? Is that appropriate? Is that something that Merv should be called in and held accountable to and asked to explain, these are the accusations we're hearing? And these could be private accusations, things that are not known in the public domain.

But, again, it reflects the need of the NomCom to be able to vet that with the candidate and understand this is what's being presented, this is what we're being told, this is what we know and this is the reason why we're not going to advance you, what say you? I think that's fair.

Scenario four, slight variation on that. Let's say the victim in scenario three was named Mary. And Merv was being accused of some bad behavior against Mary. But in fact the roles are reversed and maybe there's a standing relationship between Mary and Merv, and this is a reverse discrimination from Mary because not liking the way the relationship fell out. Again, you've got all this stuff that can happen in a closed door situation.

And I think the one relief valve that's missing is a requirement that NomCom engage with candidates.

Right now NomCom does stuff all by themselves. Candidates have no idea what's going on and have no opportunity to explain issues or concerns that may be raised.

Paul Andersen: I thank you that and for stressing that the hypothetical nature. And I assume -- as someone said, genius is in a war, there's some scenarios as people evaluate that.

Obviously if there's any data that people had that that stuff occurred past or present, I urge you to approach us and let us know.

I think I heard, to summarize, you talked about communication with the candidate, of which there is now, in the sense there's an interview.

For those not aware, it's actually done by a third-party, third-party professional, HR professional, who does an interview and reports back. So perhaps that could be factored into that process.

Second one, I'd summarize as you'd like us to review strongly, and probably involve our counsel and ensuring that we have the strongest conflict of interest processes in place.

I think that was two and a little bit of three. And remind me your fourth one, sorry.

Paul Andersen: 18 years, I guess I can't remember --

Ron de Silva: It's okay. I think they all illustrate the same. These are hypothetical things I was hearing from conversations amongst the community. And it's just illustrating the --

Paul Andersen: The fourth one was also a bit of a conflict of interest.

Ron de Silva: Yes, there's a conflict. You resolved some of those conflicts by having dialogue between --

Paul Andersen: The candidate. Yes, I think I took that -- the two main ones, just ensuring that data that NomCom is using, that there's an opportunity for the candidate to have a response, is what I'm hearing.

Ron de Silva: Yeah, I've heard asked about how is ICANN's NomCom, how do they do it? Used to serve on the board of ICANN. And seeing that process is it's a little different. I'll take a moment to share that difference.

Paul Andersen: Please.

Ron de Silva: Because the ICANN NomCom, for one, they do have interactions. They interview directly with the candidates. So there's this dialogue that happens. That's different. I just talked about changing that.

But also they make the final decision. They're not creating a ballot, not creating recommendations for somebody else to go elect. They're actually doing the decision process. So it's a little different than what happens here.

Paul Andersen: We do, and I know there's disagreement on my position on this, we do obviously have the built-in safety valve which is the petition process.

I know some people feel that shouldn't need to be there, in the first bit. But obviously we see that as a success from that standpoint. But I take your point. I think the main challenge that's been is timing.

Elections at ARIN really get off the ground in January. So not to say that couldn't be incorporated.

But that's always the struggle, is that these processes open up. I think in order to do that interaction, it's just expanding the amount of time that would be required. And we just have to factor that in.

Ron de Silva: The second half that I've heard feedback

on is really regarding transparency. And that's a very simple one. Having a list of candidates published. This is a list of nominees, right published.

And then later the list in the ballot provides some visibility to the membership on kind of the input of the NomCom and the output of the NomCom.

That's the level of transparency that's missing today. So that plus the accountability requiring dialogue, requiring some interaction, some explanation, especially if the NomCom for some reason is electing to not forward somebody on to the ballot.

I think those are the two key things to take back to the Board, as you think about better ways to conduct --

Paul Andersen: Certainly I think the transparency item is something we've taken note. I can explain the reasons why there's obviously the candidate discussion which you'd still want to have some but the inputs and outputs exposing. I think there's reasons for that.

I think this discussion certainly has given good argument as to why that may no longer be valid. Again, I don't want to prejudge the Board output. But that's certainly something we're taking into account.

I have a growing line. So if you have other ones to pass in the interest of time.

Ron de Silva: Just a quick thank you for your long time of service.

Paul Andersen: Sorry, we don't have time for that. (Laughter.)

We have a remote.

Beverly Hicks: We have a remote: Rob Seastrom, ARIN AC, ClueTrust, Capital One but speaking for myself, just in case things are not on official record in chat.

I wish to add my plus one to the sentiment that something's got to change in the NomCom process. And I'm hearing good ideas here and hope to hear more.

Paul Andersen: Thanks, Rob, for that. I appreciate and agree. Go to center microphone.

Chris Woodfield: Chris Woodfield, Twitter ARIN AC alumnus. Ron mentioned one aspect of what, the suggestion I was going to make.

I fully understand -- I like the idea of showing the inputs and the outputs. There is a concern over privacy. Not every nominee wants the world to know that they were not selected.

Paul Andersen: Yes. You've hit what I believe the original founding of that and something we're going to have to balance.

Chris Woodfield: Where I'm going with this is could there be transparency in aggregate, like list the number of nominees received, possibly the number of nominations that were not put under the slate for broad categories of reasons.

That could provide additional transparency without compromising the necessary privacy that goes into the NomCom process. Want to float that as an idea.

Paul Andersen: Certainly possible. We're trying to balance those who have had a chance to review the Board guidances, we're trying to make sure we are a membership and open organization. But at the same time I think we said we benefit having diverse thought around the Board.

And that's I think one of the goals that people want to hear from the NomCom. It's not just about qualifying or not, it's also about ensuring that we have different skill sets and also just different industry backgrounds, that we have people who can, again as I said earlier, it's a lot different than it was 25 years ago when it was the ISPs and end users that were mostly large co and

academics.

We have a much blurrier set of organizations using that. And we just try and fit it in what is currently our very small board. That's what they try and outcome. Certainly it's within the realm of possibility.

Chris Woodfield: Thanks. And thanks again for your service.

Paul Andersen: We don't have time (laughter). Thank you for that. I appreciate it.

Microphone.

David Farmer: David Farmer, University of Minnesota, ARIN AC. I wanted to get up and thank you all for coming to Minnesota. And if you have some time before you go out to the airport, enjoy some of our parks or lakes or take a nice walk over by the river.

And I will assure you that it's not cold out there, that's just a normal November day out there.

Paul Andersen: Thank you. As someone from a northern climate, this is a balmy warm day. Thank you. It's been very good to end here out in Minneapolis.

We should start closing in a time perspective. So just so I can manage time, if you are going to respond please either get in line or start at least typing so I can make sure I allocate -- I may have to cut down on response times.

Center microphone.

Kevin Blumberg: Kevin Blumberg, The Wire. David, could you turn up the thermostat?

NomCom, I've got two things. I'll start with that. One is NomCom.

I've been on the ARIN NomCom a number of times. I've

been on a number of other organizational NomComs over the years.

Please thank the people that do a job that is a painful, that they never get thanks. They get a lot of grief. Things go bad one year. Things go great the next. But ultimately these are people that are volunteering their time to get shit on.

Now, that being said, that being said --

Paul Andersen: However.

Kevin Blumberg: However, this is an organizational, not just an ARIN problem, there are absolutely things that can be done to improve the process.

Most of that is not having the organizational historical information from year to year. Not about the candidates, about the process.

You have to have a lot of predone, really well done by previous NomComs that get added on and added on, so that the NomCom isn't wasting its time trying to come up with how do they gauge this year or those candidates.

Have a good matrix. Allow a good process that can be run. And this whole thing about, oh, transparency this, transparency that, have how it's done transparent.

But the actual secret sauce that goes into that work, you have to have the privacy for the candidates and for the NomCom members because otherwise nobody's ever going to want to sit on a NomCom.

Paul Andersen: Yes, I'd like to echo that. Regardless of your views, if you do feel it, please find your local NomCom member and thank them for their time.

They spend a huge amount of time on that. And I would hate to see us discouraging people, saying there's no way I'm going to sit on that committee.

So we need to encourage that, whatever it is. Certainly, as I've said, the feedback is well received and the Board sees it firmly as an issue and problem to solve. It's not.

Just NomCom's problem to solve.

Kevin Blumberg: Second one is about RPKI and IRR. At NANOG, end of March 2022, nonauth IRR is going away, which is great.

But we have a lot of people that are sitting under legacy without any services, no, IRR auth, no RPKI. And that's a detriment to the routability of the Internet. It has an operational impact.

I know there are legal reasons why you don't want to offer the services to an organization that hasn't committed to a contract. I understand all of that.

But it is a massive detriment and this game of chicken that is going on between legacy holders who won't sign and the routing security that has to go on is reaching a stalemate that's going to have a negative impact.

I don't have a solution. But the current stalemate that we're seeing where we have all of the space that cannot be authed in IRR and cannot be put into RPKI is problematic.

Paul Andersen: This is John --

John Curran: You say you don't have a solution, though.

Kevin Blumberg: I do not have a solution because it's a stalemate. In this region.

John Curran: It's been a stalemate for decades. There's many IRRs and many alternatives. The ARIN one has 10-, 20-year-old stale data in it that people routing on probably shouldn't be routing on. But we could continue this indefinitely. We can keep bad data out there for people to route on. But the right thing

is to get accurate, updated information for people who want their address blocks routed. In ARIN's authenticated IRR or any of the other IRRs that people are using.

Kevin Blumberg: The point is that entities that use the IRR data are going to move towards, thankfully, using the auth data. That is a wonderful thing and that is good for the Internet.

Using the RPKI data is good for the Internet. Nobody's disputing that. The problem is, in this region, there's a class, the legacy class that cannot use auth and cannot use RPKI.

John Curran: Why can't they use them?

Kevin Blumberg: Because they are not signed with an LRSA. Correct?

John Curran: So you're talking about you can't use ARIN services. They could use another IRR right?

Kevin Blumberg: They cannot use another auth IRR unless they transfer the space which would require them to...

John Curran: The question is, do you want an accurate registry or not?

Kevin Blumberg: I'm saying it's a stalemate.

John Curran: Not going to be a stalemate long. It's going to change over the next year fairly significantly.

Kevin Blumberg: So maybe those people need to be aware very aware of not being an auth database or having RPKI would entail for them. That is an education campaign because when their routes suddenly start disappearing off the Internet, they're not going to understand why.

John Curran: Right. The question is how do we do that? They're all connected to networks. They're not connected to ARIN. They don't have a relationship with

ARIN.

They're connected to networks. Okay. So we need to figure out how to get to the people connected to networks and tell them they need to decide what they're going to do.

Paul Andersen: It's not like that we've not done outreach on this issue, but it's a joint issue. The providers who are relying on that need to help us.

John Curran: The problem we have is that our contact information for some of these is 15 years old.

They've gone through three providers and only their current routing provider is the one that actually has good contact information. I don't know how we overcome that, Kevin.

Paul Andersen: John, I think, wants to add something.

John Sweeting: I want to point out to Kevin and everybody else that the vast majority of nonauth is proxies, not legacy space. That's not under some kind of agreement. It's the bigger providers that put those objects in for their customers that now their customers need to put them in to be authenticated.

John Curran: We're working with the largest organizations to have that happen. The people who have the most amount of data are the proxy registrations that they've done on behalf of their customers and those are individual, and handful of ISPs represent the majority of that data.

Kevin Blumberg: Thank you.

Paul Andersen: Thank you. Okay. We're going to close the microphones in a second. I'd ask you to either start typing or line up at the center microphone. We'll close at the end of this comment if you're not already in queue.

Patrick Gilmore: Patrick Gilmore, Deep Edge Realty. I want to comment on what you called the safety valve. The petition process is nice that it's there. But I think that it is actually a failure of the process, if somebody believes that they were either incorrectly or however else excluded and they thought they should be included, and we don't know why they were included and then they have to go do work to be included on the slate.

That's still the same problem that we had before. Whether you select the slate and everybody else doesn't get it, or you select the slate and you create extra work for everybody else, you're still creating a two-tiered system.

It's nice that the safety valve exists, but the fact that we have to use it is a failure of the system in my opinion.

Let's make sure that the next one we don't do something where there's some black box and you go, oh, but there's another way with extra work we can correct the problem.

Paul Andersen: Understand. I take the feedback. We'll close the microphones. I'll add again that the Board ultimately will make decisions on these issues. We take all the input and understand that we're not going to make everyone happy.

We try and make sure -- one of the things that we've tried to do over the last few years is not get too distracted. We do have an annual plan where we try and make sure we stay focused on issues.

Thankfully good timing we can now consider that without getting off track on a lot of the other things that need to be done, but we'll take that in and we will, of course, communicate. So with that we'll close the Open Microphone.

John Curran: Round of applause for our Chair.

(Applause.)

We tried to arrange rotten fruits and vegetables in the back for them to throw at Open Mic but it didn't arrive on time. You did a great job.

Hollis, do you want to close or do you want to come up?

Paul Andersen: Why don't you, you're there.

CLOSING ANNOUNCEMENTS AND ADJOURNMENT

John Curran: So thank you all for coming to the ARIN meeting. We actually -- this is wrap-up. Do we have a small set of slides?

Survey reminder. This is very important. This is how we find out what works and what didn't. Please fill out the survey reminder, a 10.9-inch iPad Air 64-gigabit will be given away to some wonderful survey person. Fill it out when you get a chance.

Next. The polls are open. So we have two polls going on. First, if you attended NANOG or ARIN, you're able to participate in the NRO NC elections, open to meeting attendance of NANOG and of course all the ARIN members have the ability to vote.

So you can vote for the NRO Number Council. And that's also known as the ASO AC. That's been open for a day. Feel free to start voting on the NRO NC. We also have the ARIN Board and ARIN AC elections that have opened up.

They opened up at noon today. You can cast ballots. You must be the voting contact for an organization. Your organization has to be in good standing. But you should be able to go to ARIN Online, click on Vote Now and you'll be taken to the voting system.

Next. I'd like to thank our network sponsors USI and

Lumen. Big round of applause.

(Applause.)

And remember -- next slide. We're going to see you in Nashville. ARIN 49, again a nice in-person meeting in a fun city. We look forward to seeing you April 24th through the 27th. And registration will open up early next year.

That's it. I'd like to thank everyone. Last slide. I'll see you in Nashville. Bye-bye.

[Meeting concluded at 3:22 PM EST]