ICANN72 | Virtual Annual General Meeting – GNSO: BC Membership Meeting
Tuesday, October 26, 2021 – 12:30 to 14:00 PDT

BRENDA BREWER: Good morning, good afternoon, and good evening. Welcome to the Business Constituency Membership session at ICANN72 on Tuesday, 26 October 2021. My name is Brenda Brewer, and I am the remote participant manager for this session.

Please note that this session is being recorded and follows the ICANN Expected Standards of Behavior.

If you would like to ask a question or make a comment verbally, please raise your hand from the reactions icon on the menu bar. When called upon, kindly unmute your microphone and take the floor. State your name clearly and at a reasonable pace and mute your microphone when you're done speaking. And with that, I am pleased to introduce Mason Cole, chair of the BC. Thank you.

MASON COLE: Thank you very much, Brenda. Good morning, good afternoon, and good evening, everyone. Mason Cole here, chair of the BC. Welcome to our call on 26 October during ICANN72. It's a pleasure to have so many guests with us today. It looks like we're going to have good attendance so that's good. Thank you all very much for making time to join the BC.

All right, you see our agenda slide on the screen. We have quite a crowded agenda today and only 90 minutes to get through it. So quickly, just let me review item number two. We have a presentation from the folks at InfoNetworks. This is due to some interest on the part of BC members who would like to hear a bit about more what InfoNetworks is developing in light of EPDP developments. Frank Cona is going to lead that discussion. Then items three and four will occupy the second half hour of the meeting. That's our policy discussion led by Steve, and an Operations and Finance report led by Lawrence, both as usual. And then item number five will occupy the last half hour of the meeting. That will be a presentation of Interisle's findings on phishing, their most recent report that was published in the last couple of months. Greg Aaron and Lyman Chapin will join us in one hour's time from now to kick off that discussion.

So before we begin, any updates or requests relating to the agenda? Okay. I see no hands raised. Very good. All right. With a welcome again to our guests. Thank you for joining us. We're going to begin the meeting. Frank, are you on the line?

FRANK CONA: I am on the line, Mason. Thank you.

MASON COLE: Very good. Thanks, Frank. The floor is yours. So take it away.

FRANK CONA: Great. Thank you. So I'll just share my screen here. Can everyone see my screen okay? Mason, can you see my screen?

MASON COLE: Yes, sir.

FRANK CONA: Okay, great. Thank you very much for giving us the time to speak today. For those who don't know me, I am Frank Cona, who, along with Michael Palage, own and operate a company called InfoNetworks. We appreciate having this opportunity to speak with you about our SSAD sandbox and upcoming larger pilot that we are launching. We realize we have limited time today as Mason had noted. So to make the best use of that time, we just want to provide an overview of some of the key elements of what we're proposing for industry pilot of our SSAD implementation, and also to highlight some of the key benefits, what we think are the key benefits of that approach. We would be glad, of course, to schedule additional time with each and any of you individually or collectively to discuss the sandbox, the pilot, and various aspects of our approach in greater detail.

As many of you know, InfoNetworks, is going to be conducting a pilot of our approach to SSAD and verified credentials with .music when that TLD launches shortly. While one of the primary objectives of our approach is to provide a compliant, sustainable SSAD system, our approach also considers other needs of various stakeholders in the ICANN community, such as incentives for improving the accuracy of registrant data. We've spent over three years soliciting detailed feedback from members of every stakeholder group within ICANN, the ICANN community, and from related organizations, and have actively participated in the EPDP process. We provided updates on our approach at previous ICANN meetings which some of you might have participated in.

From this outreach, we've developed what we believe is a holistic approach to provide a solid foundation for a compliant and sustainable SSAD. This slide provides an overview of what we think are some of the key benefits of this approach. We've got limited time today, but again, we're glad to schedule more time to dig into the details of the technical, legal, and policy aspects of our approach, and why we think it provides these benefits. We believe that this approach lowers risk and simplifies compliance, particularly with GDPR and other data protection laws. In particular, we believe that our use of what we call due process rule template for SSAD request. And the other legal mechanisms that are built into the credential governance model that we've fleshed out addresses the need for consistent access to registrant data, while also minimizing the risk to the contracted parties and other data controllers when disclosing registrant data under those due process rules. We also believe that our approach to pseudonymization enhances privacy while still providing appropriate access to registrant data. By design, we've incorporated standardized and open technologies and uniform processes into this approach that minimize implementation needs and lower cost for both data controllers and for requesters seeking access to data under the cost recovery based fee model that we're proposing.

So what we're doing—and I apologize because I think I skipped this note previously—beyond the .music pilot that we're launching later this year, we're also extending out with other interested parties, Microsoft and DigiCert in particular, to form what we call a coalition of the willing, to launch a sandbox and larger pilot to create an industry-led working SSAD. Very similar to what I believe Verisign led with their RDAP pilot a few years ago, we want to open up what we're doing for .music to a larger sandbox and pilot to test the technical legal and policy aspects of our approach. And, obviously, we'd love for your participation in that process.

As part of our system that we're building for .music, we actually submitted a 60-page data privacy impact assessment, going through all of the details, technical, legal, and policy-wise for this approach to the [inaudible] data protection commissioner. And so far, we've actually received very favorable feedback and are continuing in that dialogue so we can obtain actionable guidance for our approach.

So the technical model for our approach is based on the use of verified credentials that are subject to an established credential code of conduct and other legal mechanisms that are outlined in our governance model. And the ability, as I noted before, to process access requests based on what we call due process rules, a set of templates that can be established and evolve over time, where it's clearly permitted, there's a legitimate interest and legal basis, lawful purpose for disclosing the requested data. So a significant part of our process is the use of these credentials where the requesters are verified and various types of requests and requested data can be disclosed under these due process rules. So under this approach, the requester has their relevant identity and other qualifications verified through an identity service, and one or more credential issuers who may look at particular aspects of that, such as their IP rights if they're and making IP based requests. And then they can use those credentials to submit a request which will be evaluated in either an automated fashion or a manual fashion under these due process rules. And that's something we're going to show you in a moment with the demo.

Another aspect of our approach is—and I highlighted this before because we were considering other concerns of those in the community beyond just access to the data and part of that is getting access to accurate data. So part of what we're also piloting with .music and as part of this larger sandbox is verified credentials for registrants. So under this approach, registrants can be incentivized to verify their registration data. In the case of .music, they're mandating a certain minimum level of verification. But in other cases, it can be built into the policy aspects governing those credentials to incentivize verification of that data that is stored with the identity provider just as with the requester credentials would be.

Another advantage of this is that the same registrant data can actually be used for different credentials across different TLDs, for example, or for other purposes, which promotes standardization and reduces cost. It also reduces friction in the registration process. And from a privacy standpoint, these credentials can be used to pseudonymously register domains where a transaction specific identifier is used for that registration, that information is put into the registry essentially as a

Thin registry and linked back to the verified and trusted data that would be stored with the identity provider.

As I noted before, one of the key features of our approach is the development of these due process templates. I have an example on the screen that we have here in the sandbox. These rules consider various attributes of the requester and their credentials, the nature of the request, and the data that's being requested. In that regard, we do make distinctions for natural persons, for example, legal persons, a category we call protected persons, which could be, for example, a dissident or another person or organization whose release of their data would be subject to a heightened scrutiny. That would of course be established by the policies that would govern their registrations.

We want to vet these rule templates in a live implementation. One of the things that we've found with data protection authorities is that it's very difficult for them to provide actionable guidance in a vacuum. So one of the things we've done both for .music, as well as for this larger sandbox, is built out a live implementation, a complete domain name ecosystem, registrars, registry, and identity providers, etc., to actually test not just the technical aspects of this approach but to actually vet these rules and how they would work in a live environment so that we can get actionable guidance as these rules evolve over time.

The other key aspect of this approach, there's the technical piece with the verified credentials. The due process rules that I mentioned is the overall credential governance model and the legal protections that we built into that. I won't go into all of them here, but things to note is, number one, that the rules in the model can layer in, ICANN consensus policies, as well as particular policies for registry, for example, and data localization and other requirements for local parties, identity providers, registrars, etc., who may be holding that data. So the process is adaptable and flexible enough to incorporate in all of those different policies and requirements into the model. It does include the due process rules, as I mentioned, and a credential code of conduct that governs the use of these credentials by requesters as well as by registrants. And it includes dispute resolution and other legal mechanisms which we'd be glad to go into in more detail.

Now, I'm going to show you a demo of our live sandbox. We're going to tempt the demo gods here to do a live demo. But this is an existing sandbox, as I mentioned, that is a complete domain name ecosystem, which we think will help getting actionable guidance from data protection authorities and other regulators and other interested parties as we evolve the policy and legal aspects of the system as well. In that sandbox, we have a number of use cases. What I'm going to just focus on today, in the interest of the time that we do have, is the registration of a domain name pseudonymously using these credentials, and then on the other side of that processing of an SSAD request based on a request from an accredited requester.

Okay. So on the left side of my screen—hopefully, everyone can see my cell phone here—we've implemented this first in a credential model that can be stored on your mobile device. There is, of course, a desktop version of this as well. It's not particularly limited but we think that using this approach, particularly with verifiable credentials, is very forward looking and satisfies a lot of the needs for the system.

So I'm going to go into my credential manager here. Now, the credential manager, this is our test implementation. But this could be integrated into any particular application like an Apple Wallet, Microsoft Authenticator, or other types of related applications. It provides the mechanism for using these credentials and managing them with the identity provider that the user has. What you see here is my .music registrant credential. And if I go to the details of that, there's obviously some metadata related to this registrant. There's a proxy profile information. I have a placeholder here but that would include various information about the IDP, the level of verification, etc., that proxy profile can be used as the registration data in lieu of the private registrant data. But that information is also linked to the credential as well and stored with the identity provider. So if I want to actually register a domain name on the right-hand side of my screen here is one of our test registrars that we have in the system. And so I'm just going to register icann72.music. I'm going to search first and see if it's available, like you would with typical registration process. Not surprisingly, it's available for us. Put that into my cart and I'm going to go to check out of the system.

Now, because .music requires the use of these verified credentials, I need to provide proof that I am sufficiently verified for .music to register that .music domain name. And so to do that in this implementation, I'm going to scan this QR code. And again, we have other methods of actually providing the credentials but this is our preferred implementation. I'm going to scan that QR code. That's going to connect the registrar to my identity provider and prompt me to provide my proxy information to the registrar as proof of my ability to register that domain name.

So in this step, what happened here was the identity provider provided that credential data to the registrar. It's in the form of a signed token that can actually be validated via the DNS that could be done by the by the registrar or it could also be done at the registry level, which is in fact what we do for .music.

So I'm going to check out to complete that registration. And then what you'll see here is that domain name is now registered. And it's registered using proxy information. So in this example, it's providing information on the identity provider. Part of what we're doing, we're actually submitting five RSEPs to ICANN for .music, which include additional fields that can be added here, such as the level of verification of the individual and other information about them as well, so that this can serve as a form of evaluating that registrant even without unmasking their registrant data.

The other key aspect of this—let me just refresh this page here. Sorry. It prompted me to log back in again. There we go. So you can see here we also maintain a ledger for these credentials that that shows the registration of this domain name using this pseudonymous identifier. And the purpose of this—so when the registrar submitted the registration create request, it also passed the credential data, the registry validated that data, and then registered the domain name, and then prompted this transaction in the ledger. This is a pseudonymous identifier that's unique to this particular registration so it can't be inherently correlated with other registrations from the outside. However, under our trusted credential network and ledger system, when someone submits an appropriate SSAD request, either just to unmask the data or perhaps to request correlated data for different transactions in a pseudonymized form such as for cybersecurity research purposes, that this information [inaudible] the ability for the system the trustee credential network, as well as the IDP who holds the underlying data, to evaluate that request and provide the necessary information.

So now, as I come along and I see that registration, and I am now an IP requester who believes that that registration violates my IP rights, and so now I'm coming to the request gateway. I'm going to submit WHOIS request to unmask, go to request to unmask the registrant data. We also are building a trusted notifier process as well for .music and that is in our sandbox. Here I'm going to submit a request based on intellectual property rights. And just as before, I'm going to now provide my requester credentials. So now I'm not the registrant in this example, I'm now a requester who's seeking to unmask them. And just as with the registrant, though my various qualifications, in this case, I'm a legal professional, I am accredited for trusted notifier, etc., are part of my credential along with my IP rights, and whether I'm the attorney for the owner, the owner, etc., what type of IP it is, all of that can be included in the credential. I'm going to scan this QR code to provide that relevant information to the request gateway. In this case, I'm going to just pick one of these trademarks. And just as before, I'm going to consent and send that information to the request gateway. And this request gateway can be hosted at .music, it could be hosted at an identity provider by ICANN. The approach does not particularly limit where the request gateway or even whether there be a single request gateway.

So you can see that certain information about me as the requester was provided, and that's included that populates this WHOIS request form. I'm now going to provide the legal basis for my request. Of course, these are set by policy and are incorporated into those due process rules that I've mentioned before and, of course, any uploaded information that's needed or any information that's needed to upload can be included as well. The domain name that I'm interested in is icann72.music. And of course, we're showing this to do a single request for a single domain. But the approach and the system are particularly limited. We can do requests for larger number of related domains as well. So I'm just going to request certain data elements. The system can, as I mentioned, differentiate the rules based on the data element requested and the nature of that, whether it's for natural legal person, whether it's business data, or personal data, etc. Of course, I'm attesting that I'm complying with the code of conduct. And now I'm submitting that SSAD request.

Now, as I mentioned, that SSAD request could be processed manually or it can be processed in an automated fashion for certain sets of due process rules that allow for automated processing. But once that request is submitted, the trusted credential network that I showed in the earlier diagram that it contains the ledger, holds the ledger, will evaluate the due process rules that apply to those .music credentials.

And you can see here now I am MyIDP, who is the identity provider, the organization that actually holds that registrant data. So on my dashboard, I have that WHOIS request with all the relevant information that was submitted. So in this case, I'm showing a manual review. But included in that manual review is the due process evaluation, the evaluation of those due process rules. We include a jurisdictional test for cross border transfers. In this case, both parties are credentials. Both the requester and the registrant, they're based in the U.S. In this case, the registrant is designated as a protected entity which requires, in this case, a manual review or whatever the heightened level of review is for a protected party as established by policy.

And then for each of the data elements requested, it applies the various due process rule templates, which you can see here, it runs through several of them. It looks at the legal right, is that sufficient, the lawful purpose, whether there's a pending legal proceeding, whatever criteria are going to be evaluated for determining under those due process rules, whether the requested data can be released. In this case, I'm going to approve the disclosure of that information. And then that information now is delivered to the requester.

So I'm coming back to my credential manager. We have a number of ways to deliver this data. But in this example, I'm just going to come right into the credential manager, pull up the approved request that was sent to me as the requester. Here is obviously everything that I included in the report, as well as the due process rule evaluation, and the requested data, which, as I showed you earlier, was actually the registrant data stored with the IDP, as opposed to the data that was actually stored with the registry, which was the proxy information.

So that's a very, very quick overview of the registration process. The pseudonymous registration, the application of due process rules for evaluating a request from an accredited SSAD requester, and then obviously the disclosure of that information to the requester upon approval of that request.

The next steps for the coalition, we want to integrate various partners into our existing sandbox. I mentioned that Microsoft and DigiCert are participating in the process and particularly with Microsoft as to their solutions for verifiable claims and credentials through Azure AD. And with DigiCert, in regard to request for verification and identity provider solutions, the identity provider credential manager features that I showed you in the demo. And obviously, we'd love to integrate others as they join. We will be announcing additional participants in this coalition shortly. But obviously, we're looking for additional participants. We'd love for any of you folks to participate in any manner with which you feel comfortable. We're also looking outside the ICANN community for related organizations that want to participate as well. Of course, we're open to ICANN Org's formal participation in the process in the future.

So with that, I'll end the formal presentation. Mason, I know we're on a tight schedule. I don't know if we have time for questions, but certainly we'd be glad to answer any questions, whether here or offline, that folks may have.

MASON COLE: Frank, thanks very much for the presentation. Very insightful and comprehensive. There are some questions in the chat. If they haven't been answered, I invite you to raise your hand quickly. We've got time for maybe one or two questions. So would anybody like to ask a question of Frank while we're live with him today? Any hands? Oh, Steve DelBianco, go ahead, please.

STEVE DELBIANCO: All right. Nice job in the presentation. It gets more and more polished every time you give it. Two questions. I wanted to know whether any of the work in the Phase 2A would be of any benefit or obstacle to what you're doing. And in particular, I asked in the chat about the potential for a field that every registrar would hold indicating whether somebody's legal or natural person. And the other question would be, are you sure you want new partners now for a pilot that would really complicate things if you have to implement multiple solutions? As a pilot, usually, you'd like to do a pilot in really controlled circumstances, and once it's proven then expanded. Thank you.

FRANK CONA: Great. Thank you, Steve. Yeah, great questions. Yes, the answer to a question, and even more broadly, is it's not an obstacle. As I mentioned, we have been participating in the EPDP process overall all along and have incorporated, of course, the recommendations into the solution. So it's definitely not an obstacle. A natural/legal distinction and even protected party within that is certainly a part of what we're doing.

To your second question, yes, it's always something to consider. But one of the reasons we want to open up to other participants is we do want to see how this works with existing data, for example, in existing systems, and we proposed an end-to-end model that would work with verified registrant credentials, obviously, and a separate SSAD. But certainly, it can be used for existing data and existing systems. And I think an important thing to do as part of any sandbox and implementation if you're testing is you need to integrate with that. Even other test environments, to try to work out a lot of those bugs and any issues that may come up that need to address, whether that's technical policy or legal.

MASON COLE: Right. Thank you. We have time for one more. Mark Datysgeld, go ahead, please.

MARK DATYSGELD: Thank you very much for your presentation, Frank. My question is centered more around the, let's say, the permanence of this data and how it's operated. Where exactly is all this data being hosted? Where are these ledgers being hosted? Is it on the side of the contracted party and then it's transmitted to a broader database? Is the database integrated at heart and they just feed that database? Where exactly is this data physically in a practical sense?

FRANK CONA: Sure. Great question. Thank you. To break it down into three parts, under this approach, there is the beneficial registrant data, the actual data for the registrant, there's the data that's maintained in the ledger in this trusted credential network and then there's the registry data and, of course, any data that would be at the registrar. The actual beneficial registrant data is maintained with the identity provider, which in our approach is it can do privacy proxy servers but under this accredited model. And that data can be localized. One of the benefits of this approach and particularly the pseudonymization of the data that's in the ledger, and all the data that's in the ledger is just the pseudonymized transaction data that I showed you. All of the identifying and other sensitive data—identifying information of the data is actually maintained with that identity provider. That information can be localized with that identity provider in country. For example, if it's subject to data localization laws or other constraints. The credentials can be used pseudonymously across border and it's that pseudonymous data that's maintained in the ledger. Then of course, the proxy data is what is provided in the registry. Essentially, what's known as a Thin registry type approach, where the identity provider information, maybe the verification information for the registrant is maintained in the registry. But the actual beneficial registrant data under the ideal approach, the full implementation, would be with that identity provider.

MARK DATYSGELD: Thank you very much.

MASON COLE: Thank you for the question, Mark. And thanks for the follow up, Frank. We're at top of the hour. Frank, there are a couple of questions in the chat that I'm not sure we got to. I might invite you if you have time to stay for a bit and maybe answer some of those questions in the chat. If not, we can follow up by e-mail afterward and we can get back to the BC on what you said. But you're welcome to stay, of course, for the rest of the meeting. This is an open meeting. I'm going to cut the queue there. And thanks, Frank, for your presentation. I appreciate you making time for us today. I look forward to the answers to the questions in the chat.

All right, ladies and gentlemen, two minutes past the hour. Let's move on to the next agenda item which is our policy update and then an update from Lawrence. Steve, over to you, please.

STEVE DELBIANCO: Thanks, Mason. I need the ability to share my screen. Can you give that to me, Brenda? I don't see a share. There it is. I got it. Thank you. Fantastic. I'm Steve Delbianco. I serve in the role of the BC's vice chair for policy coordination. In the BC, that's a position where I try to manage the process of recruiting volunteers to work on comments. I usually tee up the issue by looking at things the BC has done in the past. We try to coordinate among different edits, manage the process of drafting and soliciting member approval for our formal comments, and then take care of packaging and submitting it and cataloging it. That's for the public comment process. But we also do the same whenever the BC wants to comment on relevant proceedings, such as advice that's been offered by the GAC or even events that occur outside of ICANN, such as the European Parliament or the Mozilla Foundation. If we believe it's relevant to the BC's mission, the BC will comment on that as well.

For instance, the first thing we do in each of our meetings is to go through previously submitted comments. Since our last call, the BC has submitted two comments. Today, we found comments on the draft Budget and Op plan for the PTI and IANA Fiscal Year '23. Thanks to Tim Smith and Lawrence for drafting the comments. Lawrence, you came in over the weekend with a very substantive and just outstanding set of draft comments. I appreciate getting those in on top of the initial work that Tim had done. Thank you.

Then, on Saturday, we submitted comment on the initial report from the EPDP on Curative Rights for International Governmental Organizations. Jay represents us on that EPDP. And Jay, along with Andy Abrams and Zak Muskovitch, Marie, and Jimson contributed to an excellent five-page comment that we put in. Thank you again.

Now in terms of open public comments, I have nothing that's currently open. The ICANN Public Comment agenda typically throttles back around the meeting but more will be coming. I did want to remind you that the BC continues to develop a publicly displayed position with regard to what we are encouraging the European Parliament and committees to do on the NIS2 amendment process. The BC has gone on record in the EPDP meetings and our comments there to say that NIS2 is likely to create an obligation for registrars to differentiate between legal and natural persons, and to have an obligation of some form of publication and disclosure for legal persons. In addition, there are going to be accuracy requirements that could make their way into NIS2. The BC has tried to be proactive with key committees, the European Parliament, try to provide rationale and suggested language to see if we can move that process to one that will restore to us the ability to discover a registrant who might be responsible for trying to defraud or cause malware distribution to business users and business registrants. That is the BC's mission. We have a number of BC members that are very active on that. Would any BC members wish to ask any questions or make any comments on what we're doing on NIS2?

DREW BENNET: Steve, this is Drew Bennett. Quick comment/update. As folks know, we've been following closely what's happening at the ITRE Committee at the European Parliament, which now has confirmed that for Thursday, there will be a vote on their final report for NIS2. I'm going to just put in the chat a link to the agenda that folks can go to there.

Hopefully, that link will work. There is in there, it's a little hard to decipher. But the report, also known as the compromise amendments is there. You'll be able to see the final language that committee will be voting on on Thursday. You'll see it in bold and italics some of the recent changes that will be of interest. Particularly, I recommend scrolling down to pages 45 to 47. That's all for now. Thanks.

STEVE DELBIANCO: Thanks, Drew. Any other questions from BC members? Drew, the link you provided works perfectly. Thank you for doing that.

All right, let's scroll on to what we call Channel 2, which is the BC's opportunity to discuss the Council meeting that just concluded and the Council meeting that's coming up in Any Other Business that's before Council. We're happy to have Marie Pattullo and Mark Datysgeld as our elected GNSO councilors. We have covered this in previous meetings where we went back and looked at what happened since the 23rd of September. The EPDP Phase 2A, there was a point of order about whether the recommendations were in scope, Council leadership determined that it was in scope, and then all the recommendations would be voted on together. The next Council meeting comes up tomorrow. I've included a link to the agenda and documents. Then I thought I would just allow our councilors to do a high level overview. In previous BC meetings, we already covered what our vote will be on the EPDP Phase 2A so we can skip that and go right to the items five and six, and then we'll turn to you Zak with respect to the Transfer Policy review. Mark and Marie.

MARK DATYSGELD: Marie, would you rather start? Should I briefly comment?

MARIE PATULLO: Whichever you prefer.

MARK DATYSGELD: I will very briefly talk about point five. As I mentioned in our closed meeting, the revised GNSO councilor job description is intended at defining what the role of the NomCom elected councilors should be. In the current consensus, which I'm not entirely sure that I agree with, but this is the way it's going is that it should be somebody who's not currently affiliated with any SO/AC or really have much of a role in the ICANN community, so to say, which in honesty, is what has been done in the past. It's not like this hasn't been the general feeling, but at the same time, it creates this the situation in which we are very reliant on this person existing. I don't know if that's exactly the best path to take. But this is how it is right now.

Apart from that, on yesterday's meeting or day before, I'm not entirely sure, with the Council, as you all know, I have been fighting very hard to instill this notion that the DNS abuse has policy implications. And it's seen together with several other councilors from the CSG. Apparently, people are picking up on this. There is some incipient discussion on the role of DNS abuse in the GNSO Council. Since we're having a bit of a transition right now in terms of elected officials, I believe that it has been pretty much said, "Let's wait for this for this new term to get this going." So possibly expect us to be able to advance a little further on that subject in the coming year. That would be my general take right now. Thank you.

MARIE PATULLO: Okay. I'll jump in and have some more bits on our agenda tomorrow. We will be talking about the UDRP. We talked about this before. As you know, what is happening here is that ICANN staff have decided they are writing a policy status report about UDRP. And the idea is that this will feed into and help us with the drafting of the charter for Phase 2 of the RPMs Working Group. As you know, we, as the BC, had a number of concerns there. The first one being why is ICANN staff writing this because they've never taken the UDRP and had thought that WIPO would have been a far more appropriate offer.

Anyway, a whole bunch of comments went in from us, a whole bunch of comments went in from our colleagues in the IP Constituency. From what we know at the moment, it looks a lot better. We will know more tomorrow. The idea is that this status report is actually going to be published around the end of the year for public comment. Steve, you'll have another public comment on your list.

Another couple of things, if I can mention them, we are actively looking for somebody to take on the role of the Standing Selection Committee rep from the BC because I'm termed out. It's not a heavy lift, it's something we do need to be involved in. If you have any questions, let me know. As of not quite this time tomorrow, but nearly, we're going to have a new Council chair. No, we're not. We're going to have the same Council chair. We're going to have two new Council vice chairs, Tomslin from the NCSG and Sebastien from the CPH.

I'm really conscious of time here, Steve. So the only thing I will say is I'm in a very cold and dark Brussels. I know that Chris Mondini is with us, and he's also in a very cold and our Brussels. And I wish that I was in a very cold and dark Seattle. Back to you, Steve.

STEVE DELBIANCO: Okay, good. I wish we were all in Seattle right now. We'd be sleepless in Seattle since these are long meetings, for sure.

Next up, I wanted to give Zak Muskovitch and Arinola an opportunity to talk about the current happenings in the PDP for the Transfer Policy Working Group. The BC has, for decades, been involved at the Transfer Policy and various elements of it. It's got a new name right now. Zak, we, unfortunately, ran out of time on the last BC call and I know you wanted to share some things with us. So the floor is yours.

ZAK MUSCOVITCH: Thank you so much, Steve. I always hate speaking after Marie because I don't have her jokes or sense of humor, but I'll try to keep this brief. I'm privileged to represent the BC in the Transfer Policy Working Group. It's been meeting for about six months and it's scheduled to meet for another approximately two years. This is the Policy Working Group that deals with the existing Transfer Policy and it concerns when locks are put on domain names, how authentication codes work, how long the codes are, some technical things stuff, as well as some more general policy stuff. The group has participants mainly from the Registrars and the Registries. These are truly experts in the mechanics and operations of how registrars operate when it comes to transfers.

Nevertheless, the BC has an interest, as Steve mentioned, in this issue. For example, business registrants have a twofold interest, a security interest in terms of securing their domain names, making sure that they're not subject to hijack by bad actors and also portability. Business registrants need to transfer domain names as part of acquisitions, as part of sales of businesses, as part of deals concerning domain names and websites. The BC is looking at this generally from that twofold perspective, security balanced with portability.

The working group is at its very early stage. I'm going to put into chat a status update that was shared earlier today in the Transfer Policy Working Group. It's a convenient flipbook. If anybody cares to review it, that will give you in broad strokes the status of where things are at. No decisions have been made, yet. Slowly, but surely, methodically, the working group is looking at various options and recommendations. If anyone in the BC ever has any input, they'd like to provide, any guidance, particularly if you have technical expertise, which I don't, it would always be much appreciated. Thank you very much, Steve.

STEVE DELBIANCO: Thanks, Zak. In the previous iterations, it was known as the IRTP, the Inter-Registrar Transfer Policy. And the BC had several members, Chris

Chaplow, among them, who had been victims of transfers gone wrong or transfers denied that should have been granted. That always helped us to be able to explain some of our root concerns. I think you've captured that. And thanks for sharing the link. Do we have any questions for Arinola and Zak? Not seeing any. So we'll go back to the policy counter. Thanks again.

Let's turn to Channel 3, which is the Business Constituency's work within the Commercial Stakeholders Group. So for the guests that are on the line, the CSG was a label that was given in 2009 when the ICANN Board imposed a new dual house structure on GNSO. When they did that, they took the IPC, the BC, and the ISPs and put us under a label called the Commercial Stakeholders Group. And the non-commercial users are under the Non-Commercial Stakeholders Group. So it's a label but it doesn't have a structure. There aren't officers, there isn't a separate group of policy, each of the three constituencies maintain our own perspectives and policies. But we come together under the label of CSG for purposes that are requested by ICANN Board to deal with certain elements of the GNSO.

With that, I want to turn things over to Waudo Siganga who's our liaison for the BC. Starting next year, Tim Smith will take that role in the BC. Waudo? I can't hear you, Waudo, please. Tim, would you like to take over while we wait for Waudo?

TIM SMITH: Actually, Steve, I don't feel appropriately prepped to be able to give Waudo's report so I would have to defer to you or to Mason, in fact.

STEVE DELBIANCO: No problem. I'm happy to go through it. When we met last Thursday, we already covered what happened on the 18th of October when we met with a GAC Public Safety Working Group and the discussion of that. Then on the 20th of October, I was asked to present for the CSG ALAC session on the ICANN Org Accountability and Reviews and it was particularly focused by the organizers on the holistic review. I shared with you my three-minute remarks, which summarize the BC's perspective. And our hopes that a holistic review would be able to look at the mechanisms by which ACs and SOs interact with each other. And the example I cited, which is in part two, was that the GAC, ALAC, and SSAC worked very hard to participate in the EPDP for over two and a half, three years. And yet they aren't voting members of the GNSO, which goes on to make the policy. I brought that up as an example, that if a holistic review looks at the way that bodies interact, it's true that GAC, ALAC, and SSAC are stakeholders when it comes to things like the EPDP. But as stakeholders, they have no voice or vote in GNSO. And that would be something that a holistic review would want to take a look at.

I also brought up the idea that the non-contracted parties and the contracted parties each have one Board member, but we have approved almost six years ago a request that the contracted parties and non-contracted parties each have two Board members at ICANN. This reflects the fact that the GNSO is over 95% of ICANN's revenue and workload. And the fact is we have to make these awkward compromises to be able to get a single Board member that represents both the Non-Commercial and Commercial Stakeholders. And I know the Registries and Registrars have to take turns. So we are recommending that as something that a holistic review can also look at.

All right. And then we also had on the 24th of October the GNSO—we watched the contracted parties give a DNS Abuse Workgroup Community Update. It was an excellent presentation with slides. They discussed mostly the trusted notifier framework. So I encourage you to look at the slides and listen to that session. The Zoom recording is available and it was quite informative.

We also had yesterday an engagement between the CSG and ICANN Board. As we suggest, there's a link to it there. We talked about ICANN's roll covering what governments do globally with respect to interactions and laws. Then we talked about the implementation of review recommendations. And there's quite a stack, quite a backlog of review recommendations that have not been implemented. Prioritization will end up being key to that because it looks as if there's no way ICANN can do it all. That's it for the CSG update. Mason, if there are no questions, I can turn it back over to you.

MASON COLE: Thanks, Steve. Mark, is that a new hand? I'm sorry.

MARK DATYSGELD: Thank you very much, Steve. Very briefly, I would like to emphasize our colleagues at the CPH gave this really incredible presentation outlining all of their progress in the matter of trust and notifiers. I would like to highlight, since we have a broader meeting today, the importance of this in a minute. Keep me honest on that minute. With an actual trusted notifier framework, this provides us with a way to try to structure better the way that DNS Abuse can be actually worked with. Steve has a face that says, "Let's see." But really, we can really work with this. We can actually start trying to form partnerships and trying to build bridges and working with something that's more tangible than just trying our best to notify into the work on our own. We could establish real partnerships here and to try to get very focused actors that can reliably provide data for the different contracted parties on the types of abuse that concerns us the most.

For example, I together with Tim, we're very involved in matters of health. SIPA that Tim represents here is within the trusted notifier general structure. But it can be deepened. We can keep expanding our reach and creating more inroads to be able to actually work better with the contracted parties. So if you have a subject that is of interest to you, you might as well keep working on that better now. This is pointing towards what I think is a brighter future of cooperation. I haven't been the most eloquent in explaining this. But I think that the general idea can be surmised. Thank you.

STEVE DELBIANCO: Elegant, Mark. Thank you. I would invite you, Mark, if we have time, maybe you and I could go through that slides and presentation. If there's things we can pull out to draw our colleagues' attention to it.

Because with ICANN underway, it's very seldom that somebody will go back and watch a previous session if their calendar is full of new sessions to watch. Okay, Mason, back to you.

MASON COLE: Thank you, Steve. Thank you, Mark. All right. Colleagues, we have a few more minutes before we get to Greg running his presentation. Greg, I see you online. Thank you for joining early. But let's go to Lawrence first for an update on Operations and Finance. Lawrence?

LAWRENCE OLAWALE-ROBERTS: Thank you, Mason. Good day, everyone. My name is Lawrence Olawale-Roberts, the vice chair of Finance and Operations for the BC. It basically covers issues around operations, and of course, managing our finances. Welcome to all guests of the BC at today's meeting.

I'll start off with some open announcements within the community. ICANN73 NextGen application deadline has been extended to the 5th of November. This is a program for those who are still in the university. For ICANN73, which is going to be in San Juan, Puerto Rico in March, there is an opportunity for interested NextGeners, so to say, to join this program. Incidentally, there's been this belief that for the NextGen and Fellowship program, usually don't really serve the kind of members that the BC is looking for. But this has been proven not to be true as we've had current members of the BC even moving up to leadership from the NextGen and also the Fellowship block. I don't know if Mark who wants to say one or two things in just one minute about his NextGen experience.

MARK DATYSGELD: Thank you, Lawrence. So the NextGen program is for mostly academics, young people who are into academia. I first joined ICANN when I was doing my master’s degree in international relations. Through the NextGen program, I managed to get to know community members and eventually find my path within ICANN, and eventually end up here as the BC’s councilor, which has been a great experience both professionally and academically. It has been very opportune and incredibly inspiring.

So if you have young people in your network that are pursuing a specialization, a master’s degree, a PhD, make sure to encourage them. We don’t get enough submissions from people from the private sector who are studying business, who are doing their MBAs. We don’t get enough of those. I’ve been on the Selection Council Committee, and I can tell you, we get so few. If all of our members and/or friends or guests could take the time to maybe think about someone that could fit in this program, I’ll tell you, it’s really great. It really provides interesting opportunities and it’s a bridge to the Fellowship. Eventually, the NextGen can graduate into a Fellow, and this is what we see happening often. Thank you, Lawrence.

LAWRENCE OLAWALE-ROBERTS: Thank you, Mark, for that. For members, we have up until the 5th of November to share this piece of information. We can definitely direct interested candidates to the ICANN Org websites where they will find more information. The Fellowship program has concluded selection for ICANN73.

In November 11th, there will be opening applications for ICANN74. ICANN74 happens to be the policy forum and is going to be at The Hague. That's also another opportunity that we can share with our network.

Moving on, we have the BC outreach plan already on the BC's website, icannbc.org. So if you were to navigate to communications, the Communications tab, right on where you will find Outreach, and you will see the Outreach Plan. Normally the outreach plan is a requirement for BC members who are interested in using CROP to have effective. We might not have face-to-face meetings but we decided to stay compliant with the practice.

Over the last week, I had an opportunity to be in the Middle East for one of the largest technology fairs in the region, GITEX, and used that opportunity to speak to businesses. Quite a number of them they're aware. But those from the region, especially the Arab region, about the BC, and the impact it will have on their businesses, especially in terms of Universal Acceptance [inaudible]. It's a very unique region. This is one region where you have to type from the back towards the front, and Universal Acceptance is definitely a key concern.

A number of trade associations, including the Arab ICT union, we're very excited about what the BC is doing. This happens to not only be a union within the ICT region/sector, I understand, but they cut across about 10 different countries. And so we'll be driving that discussion further. The Moroccan counterparts are also interested in getting more details about the BC, how they could stay engaged and all that. So I will definitely keep that rolling.

One interesting company that I was able to engage with while in the Middle East was also a representative from Zoom, who was excited to know that, to a large extent, the ICANN remote tools that we're using happens to be their platform. They also are taking discussions further with regards their interest in the BC.

I want to continue to encourage members of the BC to talk one on one with businesses with the aim of getting them interested in the Business Constituency and joining them even in our virtual mode.

I'm happy to announce that we have a new member in our fold. We welcome the company Web X.0 Media to the BC. Their key lead representative is Mike Cyger. Web X.0 Media had gone through the process of joining the BC just before the pandemic, but due to the breakout of the pandemic decided to hold off their membership. They are now reengaged and paid off and fully joined the BC. So we welcome Mike and his team to the BC, and we will definitely love to hear you engage. If you're here, please indicate so we might want to give you a few minutes to speak a bit about your interest and your company. But welcome to the BC. So this brings our membership strength to 64. We hope that before the end of the year, we will increase in our membership.

We want to announce that we have the ICANN72 newsletter, BC newsletter now live on the BC website. Thanks, Brenda, for sharing a link to where we can find this current edition. It's a beautiful addition. Please take time to review the materials and to share the information there. Thanks to everyone who sent in an article to make this happen. We're looking forward to a better, a more robust and richer addition for ICANN73.

We have set in motion the process of having our compliance with the IRS, filing our financial reports. And once this is completed, we will revert back with a report on this. Recall that we have a reserve fund of $60,000. We would hopefully grow these by at least $5,000 right after ICANN72 because some funds allocated to ExCom travel and an outreach that were not used for ICANN72 will definitely be pooled into our reserve fund. So rather than going back into our account, we'll just use that to grow the BC's reserve.

We have a few companies who are yet to pay off their dues. We want to encourage you, if you're not sure of your status, please reach out to myself or the invoicing secretariat and we'll be glad to help you with every information you need. By the 1st of November, we will start the process of elections for our committees. This will be the Finance, Credentials, Communications, and Onboarding Committee. Of course, we will be looking to have more members join the BC's DNS Abuse Working Group. For those who are interested, we will be sharing more of this information on the private list. The process starts on the 1st of November and by the 29th of November, we should have results for the elections when to hold.

Finally, I will want to let members know that our next meeting will be on the 18th of November by 16:00 UTC. If you have any questions, I'll be happy to take them. Otherwise, I will yield the floor back to Mason. Thank you.

MASON COLE: Lawrence, thank you very much. I know it's been a couple of meetings since we had a comprehensive report from you. And that's no fault of yours, of course. That was scheduling problems. But thank you for that very comprehensive report. Any questions for Lawrence? Okay. I see no hands. All right. We are four minutes over schedule so let's continue.

We're on to the next agenda item. We have Greg Aaron and Lyman Chapin from Interisle as guests with us today. I see they've already got their presentation queued up. So no further delay. Greg and Lyman, over to you. Thank you, gentlemen.

LYMAN CHAPIN: Thank you, Mason. Hello to all of the folks in the Business Constituency who have turned out for today's meeting. We will, as briefly as we can, present the results of a study that we've done on the prevalence and character of phishing attacks during the period from May 1, 2020 to April 30, 2021. This is the second phishing landscape report that we've published. We also published one for a similar period last year.

We've been collecting data on phishing and other cybercrimes as defined by the Council of Europe's Cybercrime Convention. Since September of 2019 and beginning with the data of May 1, 2020, everything is posted at the Cybercrime Information Center that Interisle has set up, cybercrimeinfocenter.org. Brenda, if you'd move to the next slide.

So we have a year of data. It's collected from four highly reputable sources, APWG, OpenPhish, PhishTank, and Spamhaus. We're deliberately using only high confidence reports and also threat intelligence feeds that have a good chance of remaining in existence. One of the biggest things about what we're doing, including the Cybercrime Info Center, is to have longitudinal comparability across many different time periods. The idea overall, of course, is to replace anecdotal accounts of phishing attacks and the way in which domain names are used in them with actual data about what's happening.

So we collected just under a million and a half phishing reports representing almost 700,000 unique phishing attacks, and we noted in those reports, roughly half a million unique domain names used for phishing. And with that introduction, I'll hand it over to Greg to give you some of the details from what we found in this second phishing landscape report.

GREG AARON: Thank you, Lyman. Let's go to the next slide, please. So over the course of the year, our sources reported basically a 70% increase in the number of attacks. And you can see the red trend line there. So our sources are going out and they're trying to find out about phishing URLs. They're finding those in e-mails which are sent to potential victims and in other fashions, and then they're confirming them. And so the sources were able to find more and more generally over the course of the year.

So one way to characterize this is, yeah, phishing seemed to be really popular, it seemed to increase against the baseline. Phishing goes up and down. Sources generally tend to use consistent methods to find out about phishing. But generally, we saw them finding more and more over the course of the year, and it dipped down. As you can see in January after the holidays, things tend to rise after the holidays. But again, we also saw then a rise in the early part of this year. Next slide, please.

One of the things we look at is whether a domain name, which has a phishing site on it, was maliciously registered or if it was compromised. There's an important difference there. A compromised domain name has been broken into by the phisher. So the phisher got into the hosting and they put a phishing page up on some innocent registrant's site and their domain. You don't want to take down that domain name because you could harm the registrant and their business or whatever they have on their website. But you can go to the hosting provider and they can take down that specific phishing page.

A maliciously registered domain is registered by the phisher so they can victimize people. In our report, we talked about the methodology we use to identify those. Separately, there's a project called the COMAR project, which was put together by researchers at SIDN and AFNIC and some university researchers. And we've both ended up with pretty similar percentages. What we found is that about 65% of the domains that we saw were maliciously registered. So these are phishers going to registrars buying domain names.

Those domains can be safely suspended by the registrar or by the registry operator. The only person you're going to hurt when you suspend those is the phisher, and that's what we want. That kind of activity by registrars and registry operators does happen every day. There are lots and lots of domains suspended for phishing every day by registries and registrars. But this is a place where we see that the phishers are getting access to domain names directly. Next slide, please.

One of the things phishers do because they're registering their domain names, they tend to use them quickly after they register them. One reason is they don't want to get caught. Sometimes they get caught because some registrars use anti-fraud detection to make sure that there aren't any bogus credit card charges and that kind of thing. So they tend to use their domain names quickly. Most domains, 89% of them are reported for phishing within 14 days following registration. And with malicious domain registrations, it's even faster. However, it sometimes takes a few days for them to be used after they're registered and so there is time to find those and maybe even be proactive about suspending them before they're used. Next slide, please.

Now, like a lot of cybercrime, a lot of phishing is concentrated in a few places. And that tells us that concentrating on these places could have a big effect. Now, 69% of the domain names used for phishing were in just 10 TLDs. Now we would expect a fair amount to be in .com. It's big and it's old and it has some domains that get compromised. But phishers also like to register .com names for some reason.

The free non-domains are licensed or repurposed TLDs. They are offered for free. That includes .tk, .ml, .ga, .cf, and .gq. Phishers really, really like free domain names and they go to the free non-TLDs to get enormous quantities of them. .xyz also had a fair number. And you .cn, .top, and .net also in the top 10. Next slide, please.

Now, one of the things we saw on the left side, that's the market share of different kinds of TLDs, .com and .net is 46% of the market and so forth. The lower right shows you the distribution of the phishing domains. One of the things we saw is that the new TLDs are 6% of the market, the 21% of the domain names used for phishing. And virtually, all of those were malicious registrations. So, things are a little unbalanced. Phishers, for whatever reason, are buying and have been buying new TLD domain names out of proportion to the market. Not so much ccTLDs. We count those free non-TLDs in the ccTLD category, and if you don't count those, then that ccTLD category really shrinks. So, phishing does not take place generally in proportion to the market. Next slide, please.

We also see a concentration in phishing, depending on registrar. So there are certain registrars where phishers are getting a lot of domain names. Now, this is maliciously registered and compromised domains. You'll see that the largest registrar in the world, of course, is GoDaddy, much larger than any other registrar. But they're only at number three. Number one is NameCheap, which is a large registrar but much smaller than GoDaddy but has more than twice as many phishing domains. NameSilo is a mid to large registrar but is number two. So for whatever reason, phishers are going to certain places. Some of the large registrars will naturally show up. You see a lot of the listings here are for some of the largest registrars including Tucows and Google and eNom. But we see certain places seem to be more popular according to by size. Next slide.

If we look just at maliciously registered gTLD domains, this is where they were registered. Again, NameCheap and NameSilo seemed to be places where phishers went, and that's what the numbers tell us. Next slide, please.

There's also a concentration of phishing attacks if you look at where they're hosted. These are the places that phishers are generally hosting their stuff. And again, this includes some of those compromised domains as well. The number one is NameCheap. NameCheap also offers hosting. This registrar has phishers that are buying domains there and also hosting them there.

Cloudflare is number two. Cloudflare technically isn't the hosting provider. Cloudflare offers a service where you can use their name servers, and that's basically a proxy service that protects from DDoS attacks. The real hosting location is hidden behind those proxy servers. So we list Cloudflare because they provided the name servers and they provided the resolution service, but nobody can see the actual IPs or hosting locations behind that service. Those were somewhere else. But what we do know is that phishers sometimes like that Cloudflare service because it hides where they're doing their actual hosting.

And then we've got some other very large hosting providers, including Unified Layer and Google and DigitalOcean. These are very large companies, some of them with multiple hosting brands.

Hostinger is a provider at number six and they offer basically free subdomains. That's another free resource that phishers like a lot and they use that to launch sometimes thousands of attacks per month. So again, these are places where some attention by the hosting providers might have a good effect. Next slide, please.

Over to you, Lyman. Thank you.

LYMAN CHAPIN: Thank you, Greg. Mason, I think you can take the gavel back and ask people if there are any questions or any other comments on the report. I will point out that the report is publicly available and is backed up by the data that are at cybercrimeinfocenter.org.

MASON COLE: Okay. Lyman, thank you very much. And, Greg, thank you. Thank you both for running through this report with us. Very informative. Informative as it relates to our issues on DNS abuse as well. Actually, we have a pretty good chunk of time remaining before the top of the hour. So let me open up the floor for questions. Steve?

STEVE DELBIANCO: Thanks, Lyman and Greg. The question would be did you cover both text messages used to phish and e-mail messages used to phish? In other words, what was the method of phishing that your study encompassed? Thank you.

GREG AARON: Okay. These are the URLs of the phishing attacks themselves. How people get there is kind of what you're talking about. We do have a mix of both of those methods. Text is very popular in certain parts of the world. You'll get a text message that leads you to a phishing site. It's popular in places like India. The Bank of India has a big problem with this right now, getting attacked through SMS messages, sometimes also in South America. So we have both. Detection happens in other ways as well besides texts and e-mails.

STEVE DELBIANCO: Right. So the quantity of attacks, it sounds as if the way you report it is you report the quantity of domains that are used in attacks, not the actual quantity of e-mail and communication attempts to drive people to those phishing domains.

GREG AARON: We're looking at the sites themselves, the locations where the people are being led to. Yeah, exactly. It's impossible to know exactly how many e-mails and kinds of things are involved. But it's, of course, a very large number.

STEVE DELBIANCO: And if you had to do an estimate, when somebody goes to the trouble of setting up a domain for phishing purposes, either of the two attempts, did they send on the order of hundreds of attempted communications, on the order of thousands or tens of thousands? What do they typically do to try to attract traffic to a phishing domain once they've established it?

GREG AARON: It's going to depend. But phishers are generally interested in victimizing as many people as possible in a very short time. The average phishing attack is only going to last about 12 hours, and most of the victimization is going to take place in the first about 8 hours. So what I call mass market phishing, yeah, you're sending out as much spam as you can, and hoping that some of it gets through, and that some people then click on it. That's kind of the old, tried-and-true method. But some phishers are more sophisticated and they're going to use targeted lists, which they've compiled in various ways, and maybe they've even purchased from another criminal in the criminal underground. Those can be qualified lists. So instead of just spamming indiscriminately, they may have a list of people that they know who are customers of, say, a particular bank, and the yield on that might be higher. So it can vary, and phishers do use a variety of techniques to get through to people.

STEVE DELBIANCO: Thank you.

MASON COLE: Thank you, Steve, for the question and, Greg, for the follow up. Any other hands? I'm going to put myself in the queue but I want to defer to any other members or guests before I do. Any other hands? All right, Greg, let me ask. Have you had an opportunity to give—you and Lyman—this presentation to anyone at ICANN Org? Or have you interfaced with ICANN Org about your findings? And if so, can you talk about what kind of reception you received?

LYMAN CHAPIN: Mason, we have essentially sent a note to Maarten Botterman as the chair of the ICANN Board to bring the report to their attention. And we've interacted on a less formal basis with other Board members and with some members of ICANN Org. But the point of this was not directly focused on ICANN or, in any sense, an attempt to put in front of ICANN something that we expected them to act on or respond to. It's very much an attempt to make sure that there are reliable and verifiable data available so that people who are looking at different aspects of phishing, for instance, the question and answer thread that

Steve and Greg just participated in, shows the kinds of directions in which people are likely to want to explore. Our goal could make a brief in favor of any particular policy consideration or policy decision, but to ensure that as folks go down those paths and look at different aspects of phishing and what different parts of the community can do about it, obviously, ICANN is just one player in that, that as those investigations were pursued, the people pursuing them had access to reliable data, and in particular data that could be examined over a longitudinally extensive period. So we'll be doing this again next year, we'll be looking at other cybercrimes in addition to phishing. Again, the idea is to start to build up a database of information that can be used to support a variety of arguments or investigations that other folks might want to make in the policy sphere.

MASON COLE: Thanks, Lyman. That's very helpful. It's useful to know what kind of reception you're getting across the entire community. So thank you for that update.

All right, ladies and gentlemen, we have five minutes left. Are there any other questions for Greg and Lyman while they're with us in our meeting today? All right, I don't see any hands. Greg, Lyman, thank you both very much. I appreciate the briefing, and thanks for making time. I know you took some time away from the SSAC today, and the BC is very appreciative for your time.

GREG AARON: It’s our pleasure. Thank you for having us.

MASON COLE: Thank you.

LYMAN CHAPIN: Thank you, Mason, and everyone on the BC.

MASON COLE: Thank you, Lyman. All right, ladies and gentlemen, item number six. Any other business to raise for the BC today? All right. Again, no hands in the queue. All right. Very good. All right, then we can draw this meeting to a close about three minutes early.

So thank you all very much. It was a crowded meeting and we got through it efficiently and with a lot of good information. With special thanks, number one, to Brenda for all the support that she’s given us here for the whole year, but particularly during ICANN72. Thanks to our guests for joining us today. I wish you all good ICANN72 and we’ll see you again at our next BC meeting in November. BC is adjourned.

[END OF TRANSCRIPTION]