ICANN

Moderator: Ozan Sahin
July 26, 2018
11:30 am CT

Coordinator: Your recording have started. You may now proceed.

Man: Good morning, good afternoon, and good evening. This is the Accreditation and Access Model for Non-Public WHOIS Data Call on the 26th of July 2018. In the interest of time, there'll be no roll call. The attendance will be taken by the Adobe Connect room.

On the audio bridge we have Fred Felman, Brian Winterfeldt, Marie Pattullo, Bradley Silver, Fabricio Vayra, David Steele, Renee Fossen, GG Levine, Barbara Wanner, David Maher, Aaron Hickmann, Marc Anderson, Griffin Barnett, Steve DelBianco, Brian Beckham, and myself, Ozan Sahin.

If there's anyone else on the audio bridge, could you please let yourself be known now?

(Mark): Hi. This is (Mark). I just joined.

Ozan Sahin: Thank you. Calling once, calling twice, thank you. Hearing no further names, I would like to remind all participants to please state your name before speaking for transcription purposes and to please keep your phones and microphones on mute if you're not speaking to avoid any background noise. With that, I will turn it over to Steve DelBianco for welcome and format of the event, Steve?

Steve DelBianco: Thank you, Ozan. So, Steve DelBianco here. I'm the President - oh, I'm sorry, the Vice Chair for Policy Coordination at the Business Constituency, President of NetChoice and I'll be joined on the moderation of today's community call by Brian Winterfeldt who's the President of ICANN's Intellectual Property Constituency.

We're simply the bigger heads for a large group of businesses that have worked hard for the past several months in trying to develop a model for the accreditation and access to non-public WHOIS in a post GDPR world so that legitimate users with legitimate purposes can still protect consumers through the use of access to the non-public WHOIS.

Today's event, what we'll try to do is set it up in a way that invites as much interaction, questions and suggestions with the community as we could possibly generate. We are going to try to have a section by section walk through with respect to objectives and aspects of the accreditation model, which version 1.7 is what we're speaking of, and I'll ask someone to make sure they put the link to 1.7 into the Adobe chat, so you'll be able to click on that if any of you need to.

And with respect to that after each section leader walks us through, we then want to allocate eight or ten minutes or questions from the participants on the call. We'll try to adopt a limit of say a minute on questions or comments, opinions that are expressed and, of course, give presenters and others a chance to react. This is version 1.7 so there's been six iterations prior to this and at least four community calls as well as meetings that we've held at the last two ICANN public meetings.

So there's been plenty of opportunity for interaction, but you can never have too much community involvement and that's why we are erring on the side of (doing more). On our mailing list for open public mailing lists for accreditation and access model there is a lot of interaction with individuals expressing preferences for text in a particular session or questions that are raised by others who perhaps haven't been as close to the drafting.

But nothing beats an interactive call like this as an opportunity to ask pointed questions or make suggestions to try to get some of our momentum back, to try to generate something that really brings us into convergence with the accreditation and access framework that ICANN Org publish just before we all convened in Panama, so I think that puts us on the right track. So with that, I'll turn it over to my colleague Brian Winterfeldt.

Brian Winterfeldt: Great, Steve. Thank you so much. I want to echo your thanks to everyone for joining us for the call today to discuss this critical issue and to work together as a community to implement an accreditation and access mechanism that balances the right to privacy with the legitimate need for information. I wanted to take a couple of minutes to basically set some objectives for today and give a little bit of background for folks who might be newer to our dialogue or conversation.

The need for access to critical WHOIS data has been well acknowledged. The temporary specification on gTLD registration data mandates access, but does not provide a central standard mechanism to obtain it. Many internet stakeholders such as the IP cybersecurity and consumer protection communities have confronted issues with access since GDPR went into effect on May 25 of this year.

We are only just starting to wrap our heads around how the lack of easily accessible data has impacted important functions that support ICANN's mission including preserving a safe and secure internet. We do know that enforcement time to address dangerous activity online including fraud, infringement, and other cybercrimes has increased leaving consumers, businesses, and other internet users vulnerable for greater periods of time as threats are now longer lived, unfortunately.

We know that many businesses and brands are confused about how to address GDPR and ask for registrant information in this new space that we're in post GDPR compliance. We also know that some contractor parties have taken an overly strict view of GDPR and refused to evaluate or accommodate any requests for information in violation of GPRS requirements to provide reasonable access for legitimate interests.

So the bottom line really is that without a central accreditation and access mechanism, many parts of the community are struggling with the confusion and chaotic environment and it's allowing for additional time. So, we really feel like there is a strong need for a community driven solution. We feel like it's very important that the entire community work on an access solution so that all stakeholders are appropriately represented and all interests are balanced.

The European Data Protection Board and ICANN Org have encouraged the solution developed by and representative of the ICANN community. The EPDP charter notes that the community will address the question about a centralized access model and the work that we do can and should be easily adopted by the EPDP working group for integration into the community policy development process.

As you know, many organizations and individuals that are part of the ICANN community have weighed in on the accreditation and access model including groups from the contracted parties and the non-commercial stakeholder group as well as members of the IP consumer protection and cybersecurity organizations. Between calls and submissions, over 200 community members participated in developing the accreditation and access mechanism.

The goal of this is to help all of us come to a speedy solution for access. During today's call, we will review the latest version of the accreditation access model, discuss how to integrate the accreditation access model into the unified access model framework elements for discussion that was put out by the ICANN Org several weeks ago. We'll specifically discuss access and accreditation for cybersecurity interests and we'll review next steps in this process.

The objectives of the continued community work on creation access model are a few, one; to further the adoption of the community to develop to access and accreditation model as part of the unified access mechanism. Two; to create a model that mandates a standard framework for access for legitimate purposes for adoption by the contracted parties. And, three; to help ICANN adopt an accreditation model that establishes legitimacy for IP security and other interests with legitimate purposes.

So with that kind of brief background and kind of setting some goals for our talk today, I will turn it back over to Steve DelBianco to introduce the status of accreditation and access model and kick off the next section of our call today.

Steve DelBianco: Thank you, Brian. I want to thank Fred Felman who posted into the chat a link to that latest model and I want to invite anybody who wants to pull that up. And we're next going to turn to Fabricio Vayra, a partner at Perkins Coie Law Firm who's helping many of the (BC) and (IPC) members through this issue. And, we're going to turn to Fab to help us understand what have been the changes to version 1.7 relative to version 1.6 and other significant milestones in there of which we should be aware. So, Fab, would you please take over?

Fabricio Vayra: Thanks, Steve, Brian, I appreciates the intro. Yes, so the latest accreditation access model as, you know, is in its seventh version. I think the major additions in changes since the last iteration, version 1.6, are as follow, and I think there are four significant changes.

The first being that during the ICANN meeting we had been asked by the community if we would be willing to reorganize the document from version 1.6 to 1.7 in a way that more easily mapped with ICANN's just recently released unified access model and the questions therein. So, we added a new section, section two which is framing of the model according to ICANN's Q&A and you'll be able to go through there and see in that sections the questions that ICANN pose and how the model itself addresses those questions.

The second major change is that members of the cybersecurity sector have provided input into the model. Version 1.6 had a placeholder for accreditation approach for Cybersecurity and OpSec Investigators. That Annex C has now been updated and fleshed out by members of the cybersecurity sector. So look to Section C accreditation approach for Cybersecurity and OpSec Investigators.

The third would be that there's now a populated section where previously there was a placeholder for use of registration data by private parties for verification and compliance functions. That section can be found in Annex F entitled accreditation approach for verification and compliance by private parties.

And last but not least, we've updated the section on oversight and types of accreditation to reflect distributed model where ICANN approved authority would oversee accreditations, but would distribute the accreditation vetting to the subject matter experts in various categories reflecting a little bit of, for example, the accreditation and access approach in the cybersecurity model or any of the other annexes that are split up by expertise. That new section is Annex G entitled oversight and types of accreditation.

Now, before I go to the next milestone, I just wanted to point out we've mentioned this is 1.7 of the model, the draft. It's - we've now held six community consultations on the models, four-virtual like this, and two in person in Panama where we went through the different sections and discussed it.

This latest version of the model represents at least 84 distinct comments from the community and at least 130 distinct edits, and that obviously doesn't account for the reformulation of the model and things of that nature. It now totals to 62 pages, so it's pretty fulsome. And, I would suggest to read through it, because, you know, we've noted here some of the major changes, substantive changes, but there have been some changes to the model with regard to where previously we had a background section to account for the community discussion up to this point, say, in Annex A, we've recast that section as a rationale and more of a rationale behind the development of this model, accounting for some of the history that's gone on since first publishing of the version 1.0 back in ICANN Puerto Rico.

And then, Steve you'd ask me about the next milestone and I'm happy to report that in quick secession to adding the cybersecurity section, we have had community members reach out to us, and agreed to put in, and fill out the Annex E which will be the accreditation approach for public safety and health organization. Again, that was a placeholder and the next version, 1.8, will have that filled out.

And, of course, we've already received some comments to version 1.7, which we're speaking to the folks who made the comment and working through this so that we can account for those comments and changes (edits) et cetera in version 1.8. And, I believe that pretty much summarizes what you'd asked for, Steve. I'm happy to pitch it back to you.

Steve DelBianco: Thanks, Fab. We thought the next element of this discussion is to sort of understand how this latest version fits within the framework, the framework that was proposed by ICANN or just before we convened in Panama in June. And for that we're going to turn it to Brad Silver, who's another member of the drafting team.

And, Brad, I think you've got some slides that will help to map that through, but I did want to point out to everybody that - well, the document itself is quite long, there's only 15 pages in the accreditation and access model other than the annexes that follow, the annexes are three-quarters of the document. And I know that the team did a lot of work over the past couple of weeks to fit those first 15 pages to the framework that ICANN suggest for moving forward. So, Brad silver, I'll turn it over to you.

Bradley Silver: Thanks, Steve. Just to check, I guess, folks will be able to scroll through the slides themselves or do I need to do that from where I am? We can - okay, all right so let's go. So, a few general comments first about the complementarity of the AAM and UAM. So I think that ICANN's proposed framework elements really do share the same goal as the access and accreditation model which is a unified approach to allow continued access to full WHOIS data for authenticated users that have a legitimate interest.

Another shared characteristic is the attempt to respond to various inputs from a variety of parties, including the GAC, SSAC, European Commission, and in particular the Data Protection Board which stated that it expects ICANN to develop an implementer WHOIS model to enable legitimate users by relevant stakeholders like law enforcement of personal data concerning registrants in compliance with the GDPR.

And, as a collection of framework elements, the UAM really looks at access from a 10,000 foot level while the AAM takes a much more granular approach incorporating proposals for both access as well as accreditation. So, one could say that the UAM, ICANN's UAM is a model for a possible forthcoming model while the AAM comes closer to a more fully realized and fleshed-out version of what that model would look like.

And, at a conceptual level I think that it's safe to say that the UAM has in fact bolstered the earlier ongoing work being done by the community through the AAM, because both of those frameworks start from the premise of a uniform approach which revolves around a number of basic elements, being firstly the identification of a set of eligibility criteria for specific categories of users that require access for certain defined legitimate purposes, a process to authenticate such users which envisages an authenticating body or a mechanism to provide credentials to enable access, a uniform approach to the technical means of such access, and then, of course, very importantly safeguards for ensuring compliance with the GDPR and legal responsibility.

So, those principles are, in fact, drawn from the list of questions that ICANN have set forth in the UAM. And so, what I want to do over the course of the next few slides is just run through each of those questions showing how that maps to areas that have been addressed in the AAM.

Steve DelBianco: Hey, Brad. It's Steve DelBianco. I said this in the chat, for those that have dialed in, please try to indicate your interest, either raising your Adobe hand or those of you who dialed in, you might want to try to speak during a break, because we wanted to allow the asking of questions or making of comments as we go through. Thank you, Brad. Back to you.

Bradley Silver: Sure. Thanks, Steve. So, under the question of eligibility, the AAM tackles that in a few ways. Firstly, it prescribes the particular categories of users that are regarded to have demonstrated a rationale for requiring access. It determines eligibility in accordance with a set of criteria emanating from that particular stakeholder community that maps to the underlying legitimate purposes that justify access to the data. And then, of course, compliance with those criteria would have to be determined by an accreditation authority which the AAM envisages would be approved by ICANN.

I think one of the areas where there may be a little bit of difference which may turn out to be not much of a difference at all in fact is that the UAM is - as I'm sure those who've read it will recall places quite a fair amount of emphasis on the role of the GAC in the accreditation process, at least as a first resort and certainly with regard to the accreditation of law enforcement agencies.

The AAM takes a more flexible approach to authentication and that may be because it focuses not on law enforcement but rather on a private stakeholder groups and has also taken account of the fact that the GAC may not be the best place to identify an authenticating body in the context of those groups, but neither does it preclude participation by the GAC to the extent that the GAC would like to participate, and provide inputs.

Be that as it may, we know that the GAC has stated previously that it doesn't envisage an operational role for itself in this process, but certainly the GAC is welcome and invited too and has in fact provided input into this or individual members have. So, the UAM acknowledges that where the GAC isn't able to assist and when ICANN could then work for the Board of communities to identify relevant stakeholder group.

So, really, it's a distinction I think without much of a difference and in that sense I think the UAM and the AAM are pretty complimentary of each other, and I think it makes the most sense with regard to authentication of private third parties that the AAM is the best starting point for that discussion with input available, of course, if possible encouraged from whomever would like to make it.

So let's - moving on to the next slide, the question of process. So, who provides access? The identifiers registries and registrar's as being required to provide access with the accrediting bodies being responsible for accreditation and accredited bodies having access to the full record required for their query. At the moment, the AAM does only specifically refer to registrars but, you know, I think that there is certainly no great difference or objection to aligning with the UAM in that regard to the extent that that's feasible.

The AAM also goes into a fair amount of detail on what requesting parties would need to provide tests to and accept as part of the terms of their accreditation. And both the UAM and the AAM contemplated an obligation by registrars to provide access to authenticated users. Of course, in each case being subject to local laws, you know, throughout this whole process, the WHOIS conflicts procedure has remained on the books at ICANN and, you know, it is applicable not just to the GDPR but certainly any other process - any other law that may raise a potential conflict.

And so, there is always underlying all of this, an acknowledgement that to the extent there is a conflict, there is a procedure in place, and then an understanding that adjustments may need to be made in certain circumstances.

On transparency, the UAM envisages authentication bodies, keeping a list of accredited parties, logging all requests would be - which would be available to ICANN for auditing, and also envisages logging of access requests in the AAM of - and allowing periodic audits to ensure compliance with authentications criteria. So, I think the two are fairly in lockstep on their fronts. On the question of fees, the AAM also envisages fees to be potentially recovered on a cost recovery basis, and both models contemplate regular reviews to study the effectiveness of the mechanism.

Moving to technical details, neither the UAM or the AAM contemplates essential repository of data as per current WHOIS requirements, and both envisage the use of RDAP. The AAM does address the possibility of using Port 43 and whitelisted IP addresses as a means to streamline access while the UAM is - does not specifically address Port 43 and relies solely on RDAP, so the AAM actually does provide several technical solutions for access to address short and long-term scenarios.

On the question of what technical method might be used for authentication, I think that's really open to further evolution and inputs. Currently, the AAM provides two alternatives which are fully explained in the model in which I encourage folks to look at and those are the RDAP open ID connect profile as well as a centralized accreditation authority issuing public key certificates and those are set out in quite a bit of detail in Annex I and J of the most recent model.

And then, finally, with regard to the question of a code of conduct. Now, the UAM envisages codes of conduct tailored for each user group developed in consultation with the GAC and the European Data Protection Board, incorporating safeguards relevant to those user groups. With authenticated parties needing to adhere to the code binding on them and enforceable by the relevant authenticating body.

So, the AAM does not directly propose or outline specific codes of conduct but what it does do is it contains a variety of elements in fact, I think, most everything that is contained in there could become part of a future code of conduct. And so, I think it does contain most, if not all, of the ingredients for that approach if that was determined to be the right way to go.

You know, as overlaying all of this, compliance with the GDPR is naturally an obligation. They would have to be respected by all who are operating within the ecosystem whether they are requesters or processors. So, any such safeguards, any such codes or binding rules need to take both of those activities into account and be applicable horizontally as well.

So, those are really the - that's really the lay of the land. I'd say - I think it's safe to say that the AAM has anticipated many if not all of the questions that have been posed in the UAM to a large extent and reflects a great deal of ongoing thoughts and input into these challenges. So, the hope is that the UAM is a great development to spur further discussion and encourage inputs on next steps using the AAM as a great platform for that, so thank you. Back to you, Steve.

Steve DelBianco: Thank you, Brad. I'll pause now to see if anyone on the dial-in has any questions or comments before we turn to Rod Rasmussen on the cybersecurity aspect. I'm looking in the Adobe to see if any hands are up as well. I did mention in the chat that with respect to RDAP, ICANN Org and (Akram) in particular promised us in Panama that by the end of July we'd see a pilot profile for RDAP or tiered access.

Of course, it doesn't contain all of the rules or how one gets accredited, but it would say that we ought to be able to articulate how it is one would present a query through RDAP and the query could contain an encrypted token of accreditation, it would also need to contain the reason that the query is being requested even from an accredited entity. So that's one of the points of arrival that we have in mind and one of the reasons that we'd like to see the are gap converge with the development of these accreditation models.

Another point of arrival is with respect to the AAM or the UAM, in both cases the objective is to have one or more accreditation models and schemes worked out that would be sufficiently compliant with GDPR that the data protection board and potentially other regulators could give some sort of assurance that those - following those accreditation models and the, you know, the robust codes of conduct that are involved would not run significant risks, so violating GDPR.

No one ever wants to suggest that we would need legal certainty or formal approval, but you can see that the degree to which we can require contract parties to respond is party a function of how we can significantly reduce risk that responding to an accredited query will not run off our GDPR. All right, so with that, I'd like to ask Rod Rasmussen of the Anti-Phishing Working Group and Chair of ICANN's Security and Stability Advisory Committee to talk about cybersecurity interests, because cybersecurity interests are just one of the potential entities that would pursue an accreditation model.

So cybersecurity interests, Rod, and let me ask staff to load the actual (V1.7). I think Rod is going to speak to that, he doesn't have slide. Thank you. So, Rod, cybersecurity interest you've long been seen at the trusted protectors of security stability and resiliency of the internet and you in fact are a respected member of the community, APWG in particular. Could you please tell us your perspective on accreditation and access with respect to cybersecurity community and as you're managing that through the Anti-Phishing Working Group, Rod?

Rod Rasmussen: Thanks, Steve. This is Rod and I'm not wearing any kind of SSAC hat today just to be clear, this is - (I will be talking) - focused in the APWG and the submission that I am, mainly, and Greg Aaron put together to add to this model. It's been incorporated into 1.7 in various sections. I believe Greg is on the call right now, so if I get anything wrong I'll let Greg jump in with the correction.

Brian Winterfeldt: Hey, Rod. I'm sorry. This is Brian Winterfeldt. Before you jump in, I think Lori Schulman had a quick question and I think her hands was up in the room.

Rod Rasmussen: Okay, go ahead.

Lori Schulman: Yes. Hi. This is Lori Schulman for the record. I want to thank the organizers today and the drafting team. I think we've come such a long way in a very positive direction. I do have a question regarding the process slide and the statement about providing access to full data once you are accredited. Well, I believe that it's the right direction for IP and security interests.

I am interested in seeing how we are going to approach that as a community in terms of justifying the full data set against what has been the European Data Protection Boards or formally Article 29's advice about making a good case for each data point versus an entire deal. And I think this is something we need to give some serious thought to as we begin to socialize this. Thank you.

Steve DelBianco: Thank you, Lori. I appreciate that. Yes. I did - I do think that as a particular group of entities pursue accreditation, the part of that accreditation could inform which fields in the non-public WHOIS or appropriate for the kind of queries that they would conduct for legitimate purposes and it may be that an accredited entity would map a certain fields or it could be that in a credit entity for a given purpose might have a limited number of fields that could be returned for the purpose that's indicated. I do think that we mentioned that to (Akram) when we were in Panama, that the tiered access could potentially pass along not only the accreditation token of the individual, but more importantly the purpose that's given, since that could inform which fields come back. Thank you, Lori. I think we'll go back to you, Rod.

Rod Rasmussen: Great and to that point as well before I dive into the rest, the - we actually talked to that in our own discussion around access to data set and that - I think there's an important distinction of access to the full data per se as in - there would be no restrictions on things you could ask for. However, your particular ask in a particular situation may only garner you a limited set of data.

So in other words, the full library, if you were, an analogy is open but you can only check out books of certain kinds when you come in and make a request. So I think it would be good to - for the (doc) to be clear on that, so that there isn't confusion that any requests should get the full data set back. It's - on the contrary, it's - the full data could be - should be - there should be a restriction on data that you can ask for, it's what you are actually able to get per query and during the - based on the purposes and the (unintelligible) and all of that, that it determines the data you're actually able to obtain for any individual query.

So, that is one of the point I was going to make, so I'm going to take away from the time. So APWG has submitted some input into this. Part of that, a big part of that went into the rationale, which is in Appendix K and - that was weaved into other rationale - legal basis rationale outside of - and those are fairly straightforward to look through, because I won't dig into that.

The interesting section that, you know, speaks towards cybersecurity that's in - appearing Appendix C or Annex C, I mean, and this talks about the accreditation process for access. First thing I want to point out is that this is based on APWG's own accreditation model that we have for a separate set of data around cybersecurity and - that we previously developed for different purpose. So, it's already been field tested as it were. It's been adapted and modified for this application around RDS data.

And it is an example, it's all - it's also important to note that this is not a proposition at the APWG to be the sole and only arbiter who may provide or who may be - get access for cybersecurity purposes. In fact, we would encourage other organizations to develop similar processes and codes that may take a different approach particularly around things like how the accreditation is done and if there any ongoing things like fees or processes or annual audits or anything like that that many people may want to take a different approach to how those are done.

The net-net of the way the APWG has worked this and proposes to handle accrediting and monitoring, the use of that accreditation to access data is that there would be an application by a member of the APWG, a good standing, that a member have - would have to provide a wide - quite a bit of a variety of information around who they are and what the purposes of them - that organization, the access in data are, who the primary players within the organization are, and who would be using that data.

And that would go to a panel within the APWG. That would make a determination as to the appropriateness of authorizing that entity to make queries, you can - getting an accreditation via the APWG. Those queries need to be logged with purposes attached to them as they come in that does not preclude, of course, doing things in a nominated fashion.

It does, however, require you to, you know, as a result ensure that your systems and processes are put in place to the things you are asking for or what you are truly using them for. Then, it makes the organization that is getting that data subject to terms of service, code of conduct, and of course transfer of - transfer through its responsibilities, your privacy laws, in particular, GDPR right now, but that would apply to any other privacy regimes that will be involved.

There would be an audit process to ensure that things are lining up as far as requests versus reaction. And that - if they're - then, there would be an abuse or a complaint handling mechanism where if there were some issues going on with overuse or misuse of data to be reviewed, access to be revoked, and any -

and the organization would be - that we'll have - having such issues would be liable under whatever their particular privacy laws they'd had problems with.

And this is - obviously, I'm talking about GDPR on this case, but they would be subject to any of the penalties that would come down thereof, so that would be a bit of both beginning with, you know, future access and any transgressions happen. So, it's - and then there's an annual review process built-in, so that any new types of requirements and things can be brought up to speed or any new requirements for information about the entity can be added, and I'm hoping it rolls over on an annual basis.

That's the, you know, the gist of it there's a lot more details there in the report that you can or - of the modeler 1.7 that you can take a look at to dig into further details. And, I'll throw it back to Steve for any other questions.

Steve DelBianco: Rod, it's Steve. I do have a couple of questions for you, but my general one is I want to understand how those of us in the call could be most supportive of the cybersecurity community at moving ahead on the aspirations that you're showing to be one of the first groups to become accredited?

And one potential way we can be helpful is that if some of the things you're describing would be required of any accreditation body, well, then we should try to move those to the more general part of the model and not be something that APWG has to take off. Let me show you a couple of examples.

You've described how there could be publication or compilation of lists of the accredited entities and if that's going to be the same requirement for intellectual property for law enforcement, consumer protection authorities, well then we ought to try to generalize the function of keeping a database of accredited entities, for example, with the accreditation date, the date of which that review is due next.

Another example is logging of the queries themselves, Rod. You mentioned that one of the requirements that when accredited cybersecurity professional is making a query that that query would be logged. Well, I - my guess is that it's not APWG doing a logging, but rather it's the registrees/registrars who would log that as part of their responsibility. And in that regard, logging isn't something that you need to take on as part of your proposal. You need to explain that anybody seeking accreditation and queries would need to have their queries logged, but it's not something that you need to write the specifications for how logging actually would be done.

So, this is just two examples, Rod, but I would invite other ways that - more at the community level that we can articulate support so that you can focus more exclusively on creating this code of conduct, the credentials review, and eligibility requirements for those who are seeking cybersecurity accreditation and leave the rest to the broader community since it's going to be used by multiple accreditation entities.

I'm interested to see a response to that, Rod.

Rod Rasmussen: Yes. No. I think you've hit on some things that are important. When you said we've developed this from our own separate program while we are actually having to take on some of that functionality ourselves, but yes it makes complete sense. And, in fact, it makes it probably a better solution if you have accredited - accrediting agencies telling people who want to get accreditation to them, what the rules are, and how they have to comply, but without necessarily having to do all of that work itself, otherwise you end up with a huge duplication of effort, and potentially methodologies that don't -

are difficult to then go in and cross examine as it were as to how people are accessing things.

So, I would certainly envision that something like logging would be done, obviously, the registrees/registrars who are providing the data better be logging them, I think they're required to. And then, let the - on the flip side, you know, some - you can either envision a model where the querying organization manages the log of themselves that's subject to audit or you can have a model where there is some sort of third party that manages that for them.

And, I don't think those are necessarily mutually exclusive either. I think that there is - that becomes a matter of efficiency, business use case, those kinds of things has determined how the actuality is done. What is important is to write down the fact that they need to be doing it and they need to be subject to certain auditing and other requirements to make sure there's a mechanism for accountability. So, yes, not get too perspective.

I think that some of the things that we're - we've covered and we're incorporating into a more generic model, but there's definitely more work that can be done and take what was put in the cyber section as it were, and genericize too.

Steve DelBianco: Thank you, Rod and Fabricio and others who worked on these details of the document, if you could indicate in the chat where in our document general purpose of the logging is done from registrees and registrars. And, Rod, while we're waiting for another question, I did want to suggest that if an accredited anti-phishing working group member did a query of a registree or registrar, it's possible that we may have a model whereby the accreditation credentials are simply checked in an automated way, and they might be checked with APWG if you have the ability to validate that certificate is still current.

It's entirely possible, Rod, that you as the certificate validator would log the fact that GoDaddy, for instance, requested verification of an APWG credential at 9:00 this morning and that you've granted and certified or authenticated that credential. You wouldn't, at that point, have any idea what the query was about doing it by name, you might not even know the response that GoDaddy provided but at least you would log authentication of credentials on your end.

So, logging could happen at two - a couple of different levels, the query itself and the authentication of credentials if that makes any sense.

Rod Rasmussen: Yes, it does. And I think that would be a model fairly straightforward to implement as well due to the technology is pretty readily available. In fact, there's a variety of methods. You can even envision - I'm getting vision having some sort of publication where, you know, using (PKI) you would have the requesting entity publish something that can then be authenticated against with just a standard set of public key information to validate that they are in fact currently a valid entry.

In which case you may not even have the accrediting body any sort of record of that particularly for it.

Steve DelBianco: That's right and it might be different for law enforcement. I could well imagine Interpol having a different way of wanting to validate the credentials that - in this issue, that might be different than what the IP or cybersecurity committee would do. Fabricio, has put into the chat that Section 4 on procedures is where 4B and 4E, pages 10 and 12, discussed this notion of how the registrars would log request that they've received.

And we just brought up this other notion of obligations to log that might be assumed by the accredited entity. Now, Michael Palage, I do hope you'll speak up, but I did notice your first question which was, "Can anyone point out the existing contractual requirement?" But, Michael, you, of course, you know this better than everybody here, there is no contractual requirement about logging today.

The whole point of ICANN saying, "We want a unified model and then if we create a model that fit that framework and those models achieve a legal acceptance necessary, well then there would become a contractual requirement that contracted parties would respond at the mandatory unified." That means that we eventually get to the point where contract parties are required to respond to queries from accredited entities that provide valid credentials and valid reasons for the queries that they make.

And then - when that is together, then the contractual requirements for those contract parties would have to be baked into ICANN's language that might be done by a temp spec which is exactly what was done earlier this year with respect to GDPR. It might be done by a policy development process as well.

So, Michael, you knew the answer to that and so I invite you to speak up and tell us what you're thinking.

Michael Palage: So, can you hear me, Steve?

Steve DelBianco: We do. Go ahead.

Michael Palage: Excellent. Well, my point in raising that was that under this current model the only fees out to be collected are in connection with the accreditation body for the people seeking access. There is nothing in this model that allows the contracting parties any cost recovery mechanism for this. And one things is if you look in the registry contract, specifically, there is provisions where registrees are able to raise their price.

In fact, this is one of the only exceptions in the Verisign.com contract where there is an imposed consensus policy that they are able to, if you will, raise their prices to cover that. So, I guess that's my concern here, the logging and the - not only the logging of the queries coming in, but also what the underlying nature of what that query - who it's associated with, that's not an insignificant cost, and I'm just wondering financially how that is going to be accounted for in the current model or is it simply just do it for free. That's what I'm trying to understand.

Steve DelBianco: Thanks, Michael. Well, we're waiting for others to answer on that I wanted to indicate that today and Elliot Noss told us all about this in Panama, but today even under the temp spec, registrars and registrees get queries for non-public WHOIS data and they are spending serious dollars and personal time to try to determine whether those queries need to be replied to, whether they can be replied to, and how they have to be replied to.

So, Michael, there are costs incurred today in a completely non-unified, a completely disparate disorganized fashion. One hopes that if we do a unified model for the standardized RDAP, standardized logging, that those costs after implementation will be far lower. So, I think you'd agree with that as a guy who has some systems in his background. And, so I don't believe that was...

Michael Palage: Well (unintelligible)...

Steve DelBianco: ...supposed to be incremental cost.

Michael Palage: Yes, and I could...

Steve DelBianco: It could be lower cost than that which is incurred today and if in fact the costs are still very significant, then you're right again. The community would need to evaluate whether the actual registration fees would be sufficient to cover that or should there be some other cost recovery mechanism for the contract parties to respond. I think you make a valid point.

Michael Palage: Yes. And, again, that's all I'm trying to do, is to make sure that we don't undertake this discussion in a vacuum and look at the actual economics, use metrics to go about whether this will save money. Because if in fact it does save money, I'm sure the contracting parties would more than welcome that opportunity to recognize those savings. Again, I just want to look at metrics to make sure that we're not doing this in a vacuum. Thank you.

Steve DelBianco: Michael, that's a very good point. We're going to call on Rod next. But, Michael, I did want to indicate that if a registrar today were simply ignoring legitimate queries from non-public WHOIS, then they're not incurring any dollar costs today. So, they might not see a savings if they suddenly started to honor the temp spec obligations for them to do a reasonable reply.

So, I think, you'll want to look at registrars or registrees who are attempting to give a reasonable response and examine whether we can come up with a way to do it that cost a lot less than the cost that they're actually incurring today. Okay, Rod, a question over to you.

Rod Rasmussen: Yes. I was actually going to speak to the same point. There are requirements currently for the contracted parties to log WHOIS request, but those are more of a generic level as to sheer volume, right? There's actually report of that monthly on WHOIS access queries.

I'm talking about a far more sophisticated system that would be required in order to make, you know, really this is to be compliance to GDPR, right? I don't - because I don't know think that the - whatever the access model is that you may use to get to non-public data regardless there is still any obligation or any entity that provides data out to know who is using it and what purpose they're claiming to be using it.

So this is an interesting question around how do we both - who's everybody complying with this in a way to make sure that they're meeting the obligations of GDPR and other privacy regimes as well as, you know, the practical application of we need to know who is messing around with systems and not following the rules, so we can do something about that.

So, it's a really interesting part of this. I think we should be careful not to be over prescriptive at this point, because I think there's a lot of different ways to work this out. But those - all of these issues need to be on the table so that - or at least a policy directional set that can be then looked at from various methods of implementation. Thanks.

Steve DelBianco: Thank you, Rod.

Michael Palage: And I don't...

Steve DelBianco: Rod...

Michael Palage: Yes, and if I can just - if I can follow up on that. I don't disagree with that right, Rod - (Ron). I guess my point is if the APWG is potentially going to be this first pioneer for the model to sort of set the stage for other accreditation bodies for other sectors, I think it's really important that we get it right so that it scales in those other sector. I guess, that was the only thing I'm raising, so thanks again. I appreciate it.

Rod Rasmussen: Yes, (unintelligible).

Steve DelBianco: Hey, Michael, it's Steve DelBianco. You're right and some of that scale for other sectors is achieved if we ask the accrediting drivers whether it's (CP) - APWG, law enforcement, Interpol, (Europol) or IP. That whenever possible we try to ask how can we support with general requirements, logging is a general requirement, how can we support with general requirements so that we limit the amount of complexity, and pioneering that a group like APWG has to do?

So, that would indicate Rod that on your next set of edits to this section on - that it includes whenever possible, you're identifying some function that is attributable to other accrediting sectors that flag it that way, so we can move it to a more general section of the document and that's done not to be prescriptive but to be supportive.

We want to be supportive of APWG like we want to be supportive of Interpol, (Europol) intellectual property community and turn around and say to the contract parties that, "Don't worry about it, the RDAP you've implemented works for all of these accredited queries."

Second thing, don't worry about validating credentials, we come up with a standard way to validate the credential logging in accredited query, and potentially we come up with a validated way to do centralized logging in someplace that minimizes the amount of implementation cost that would have to be incurred.

So, let's try to find efficiencies where we can locate them, but not be overly prescriptive, because nobody on this call is probably going to tell Interpol or the Federal Bureau of Investigation how it is they have to do their accreditation. We might offer them methods of logging the validation request. We might offer them assistance in a technical way that reduces the complexity that leads to a more unified model, but we can't require them to follow it.

Rod, your hand is up still.

Rod Rasmussen: Oh, I'm sorry, I just forgot to take it down.

Steve DelBianco: Okay. For those who are on the phone or in Adobe, this would be a great time to ask a more general questions, because our next agenda item is to move to what are the next steps. And, before I turn it over to Brian, last call on questions or comments here. Fabricio, would you like to speak to what you have in the chat?

Fabricio Vayra: Sure. So, I just wanted to point out on the logging section, there are nine references to logging within the document. So, we can, you know, obviously go through those sections but definitely the concept of logging is there. It's to serve multiple purposes which we've discussed a bit here.

The other being just basically, I think, the notion of transparency is throughout, so you can see I put in the last section here in the chat just the concept of logging matches up to one of the questions actually that ICANN asked and it's UAM model regarding transparency and logging is one of the big components of that, so it's referenced throughout several sections, some of which I noted here.

Steve DelBianco: Thank you, Fab. All right, last call for other general questions. Okay, fantastic. I want to turn things over to Brian Winterfeldt to talk about where we go with next steps. Wait a minute, I'm sorry, I'm sorry, (Katie Ann Smith) asks a question. "The GDPR precludes imposing a requirement on all contracted parties that as a precursor to a domain registration you must have consent." (Katie), your - let me see if I can understand that question correctly.

You would suggest that under GDPR consent of the data subject is required, but I understand, and I'm not a lawyer, but GDPR does balance against other forms of law so that if a party that had collected your information shares the information under some legitimate purpose, under applicable law that that can be done without consent, and I'll ask someone on the call who knows the law better than I to respond. John Levine, for instance, go ahead.

John Levine: Yes. I mean, I don't want to go into this in detail, but the GDPR has a whole bunch of - (consent) is one criteria under legitimate use and there's a couple of others. We've been through this a whole lot of times and as you said we get - it's a balancing issue and even the - and the letters, the Article 29 is then sent to ICANN and (unintelligible) that they need to hear a story that they can believe about balancing the, you know, the privacy of goods of the subjects versus legitimate security and all of the other interests of people.

So, I don't want to (rat hole) on this now, but it's something we know about and it's something that I think we're all taking into account.

Steve DelBianco: Yes. Thank you, John, and (Juan) wants to say that if we struck the balance we have to demonstrate that we accredited the entity and that the entity provide a legitimate purpose for the query. And, if all that is done and it is properly logged and documented, you have at least a chance of showing data protection board that we have achieved that balance for that query by that individual at that time. (Katie) does that cover it? Thank you. All right, I'll turn it over to Brian Winterfeldt, please. Next steps.

Brian Winterfeldt: Great. Thanks so much, Steve, and thanks so much everyone for giving us such a lively discussion today. I think this is really productive and helpful. Before we let everyone get on with their day, I thought it would be helpful to highlight some of our next steps as a community to continue this work on accreditation and access.

I think one of our first goals is going to be developing an accreditation access model for health and safety organizations. Second goal, we'll be working closely with the ICANN Org to help flesh out the unified access mechanism framework elements for discussion to really tie the (3AM) work to the org's work in the access model. Essentially, they put out an outline and we have a lot of meat to really put on those bones so to speak.

Third effort, we'll be supporting the community efforts in the EPDP and fourth goal we'll be working on answering additional procedural and operational questions such as what is reasonable access and how RDAP can accommodate tiered access. So, we continue to welcome everyone to join the community discussion by joining the accreditation model lister.

You can email admin-accred-model@ICANN.org to be added to the lister. We welcome any additional comments, feedback, and work on these efforts through the community group. Please also watch the accreditation model lister for additional details about further community calls and calls for input.

Steve DelBianco: Thank you, Brian. I'll pause there to see if there are any other hands up, if there are any comments that people would like to make. Brian, you did mention this notion of a temporary specification. We abbreviate that as temp spec, we're all in the ICANN world are familiar with the temp spec being the tool that the registree and registrar contracts allow through ICANN work and Board to approve the requirements that are meant to be temporary, requirements that make their way into contractual obligations for registrees and registrars.

And in fact the temp spec was the tool that was used when ICANN Org proposed, "Here's how we would change the contracts to be compliant with GDPR and the collection and processing of information and the publication of non-public WHOIS in the redaction. But that temporary spec also included an obligation for registrees and registrars to do a reasonable response to our request for access to non-public data.

So you can well imagine over the remaining nine months of that temp spec's year that there could be modifications to the temp spec if the EPDP for instance was able to identify specific ways that reasonable access has to be delivered. And then, completely apart from that if we are successful, if Interpol or health and safety and cybersecurity is someone is successful at obtaining the kind of legal clearance from the Data Protection Board for an accreditation scheme, then you can well imagine a temp spec that would require contract parties to respond to requests if they are done by a properly accredited entity with that kind of legal assurance in a way that logs the particular purpose of each and every query.

So, we throw around the word temp spec as if it is a point of arrival and it is not, it is a path, a tactic towards getting policies implemented through the contractual process prior to the actual adoption of consensus policies that fit within ICANN's contractual framework. So, I hope that helps a little bit.

Michael Palage, your hand is up.

Michael Palage: Yes. Thanks, Steve. One comment to Brian and this goes to the point - to your point, Steve, about looking for efficiencies and scale across the accreditation model. One of the things I did in the Philly special was I actually came up with an access contract, which I tried to model after other bulk access agreements both within (ARIN) and as well as some of the contracting parties, while I understand that this group may not disagree with aspects of the (Philly) model.

Perhaps, what they could do is look at that contract, because hopefully the contract by which accredited members will be accessing this will be a unified contract. So, I think that that is an area where this group could perhaps move and create some efficiencies and economy of scales by coming up with a model access agreement that would work for all parties.

And, again, I - (and do) some work in the (Philly) special, you could take a look at that or you could start from scratch. But that would be the one area where I think it would be helpful, because I don't think Rod or Greg really wants to be working on a legal contract for access to registree and registrar systems.

Steve DelBianco: Thank you, Michael. I would invite if possible if you could pull the access contract aspects from Philly special. I believe that you would do a better job of that than I would to pull the parts that you seek to include and send it to our list for inclusion in V 1.8, potential language surrounding an access agreement that would be required, and that would be really constructive as was your suggestion that we drive towards efficiency and standardization.

And if, in fact, everybody does it the same way, then we also achieve the goal of being unified, because that's really what the word unified means in the ICANN context, it's the all contract parties will do it the same. Thank you, Michael, for that suggestion. I appreciate that. Are there any other questions? any hands raised at this point?

Dave Piscitello asked a question on reasonable access. Dave, I'm sure you understand that in the temp spec that's already enforced today reasonable is the word that's in there and no one has a clue what that means. Each registrar and registree is inventing it on their own and they - people that are requesting non-public WHOIS are trying to figure out what they think is reasonable. I do hope that we address that, but that's not part of an accredited access model that might be well part of the EPDP, and I believe it's in the scope of the EPDP.

Now, with respect to query volume in 24 hours, I believe we need to address whether an accredited entity should be permitted all if it is a fully accredited and making legitimate log request of information. I don't think you're going to tell law enforcement and Interpol that they've hit the limit for today. "Sorry, no more queries allowed." That's just not going to be doable, especially, if one has cleared all of the hurdles necessary to become accredited and achieve enough legal clearance to say that you are a legitimate entity who's making queries for legitimate purposes.

Michael, your hand is still up. Don't - that might be an old hand. And, Michael, I guess I could say you are an old hand when it comes to ICANN. All right, with that, Brian, unless you have any other closing remarks, I think we can thank staff, and thank all of the participants who came onboard, and especially, thank the authors of this document, and Rod Rasmussen, and others who are contributing to it.

So, I look forward to our next call which we'll give adequate notice and please watch your email list, join the accred model email list if you haven't already. Earlier I put into the chat a link to those archives, but we need to move ahead on this and I do hope we'll show a lot of progress between now and Barcelona. Anything else, Brian?

Brian Winterfeldt: No, that's great. Thank you so much, everyone. Thank you Steve and I appreciate everyone's contributions today and I look forward to continuing our work together.

Steve DelBianco: All right, thanks all. Staff, you can conclude the call.

Ozan Sahin: (Roxanne), can you please stop the recording and disconnect all lines. Thank you.

END