ICANN72 | Virtual Annual General Meeting – SSAD ODP Project Update
Thursday, October 28, 2021 – 12:30 to 14:00 PDT

ANDREA GLANDON: Hello, and welcome to the ICANN72 Standardized System for Access and Disclosure (SSAD) Operational Design Phase Project Update #3 and community discussion. My name is Andrea Glandon and I am the remote participation manager for this session. Please note that this session is being recorded and follows the ICANN expected standards of behavior.

During this session, questions or comments will only be read aloud if submitted within the Q&A pod. They will be read aloud during the time set by the chair or the moderator of this session. Interpretation for this session will include English, French, Spanish, Russian, Arabic, and Chinese. Click on the Interpretation icon in Zoom and select the language you will listen to during this session.

All participants in this session may make comments in the chat. Please use the dropdown menu in the chat pod and select Everyone. This will allow all participants to view your comment. Please note that private chats are only possible among panelists in the Zoom webinar format. And message sent by a panelist or a standard attendee to another standard attendee will also be seen by the session host, co-host, and other panelists.

To view the real-time transcription, click on the Closed Caption button in the Zoom toolbar.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

With that, I will hand the floor over to Eliza Agopian. Please begin.

ELEEZA AGOPIAN: Thank you, Andrea. And thank you to all of you for joining us today. We're glad you could all be here for our third update on the progress made in our first Operational Design Phase (or ODP, as you've heard probably all week long). My name is Eliza Agopian and I am the Senior Director of the Strategic Initiatives team that sits within the Global Domains and Strategy function here at ICANN Org.

The Strategic Initiatives team is responsible for leading the first operational design phase for the EPDP Phase 2 team's consensus policy recommendations for an SSAD (or System for Standardized Access Disclosure). The EPDP Phase 2 team made 22 recommendations, 18 of which we're regarding SSAD. The remaining four, some of you may recall, were associated with EPDP's Phase 1 policy recommendations. And those have been adopted by the Board on a separate track and are now with the EPDP Phase 1 IRT to include as part of their policy implementation work.

Since our last webinar in September, the team has made substantial progress on our analysis, and today we'll be sharing with you our design recommendations in two important categories: contractual compliance and identity verification. The team is also going to be sharing with you an update on our survey of the GAC members regarding the governmental accreditation recommendation piece.

As we noted in our last webinar update with you all, while we've been hard at work on a design, many questions have arisen for us regarding the design choices we're posing. And today we're going to describe for you some of those choices and ask for your feedback.

As a reminder, the ODP is not meant to reopen discussions about the policy recommendations themselves. Rather, we want to hear from you on our proposed approach for implementing those recommendations. We know this is new and detailed information to digest, which we're going to be presenting to you here today, so we're really keen to hear your thoughts, and not just during this webinar but also afterward via our dedicated public inbox at odp-ssad@icann.org. We're really looking forward to hearing your comments and questions.

I also wanted to take this opportunity to remind all of us why the Board has requested this ODP of the Org. The Org team is developing this draft design to help inform the Board's consideration of the SSAD-related recommendations. The recommendations for the design that we're sharing with you today—eventually that will form part of the operational design assessment, which is our final deliverable for this effort—are really the starting point for implementation should the Board adopt the recommendations. In other words, what you see today is not the end of the discussion on how we may tackle some of these complex design choices but really the beginning of a longer conversation if and when ICANN Org begins the implementation of an SSAD.

So with that, I'd like to hand the microphone over to Yuko Yokoyama, our Program Director, who is the project owner for the SSAD ODP. And she will go over today's agenda. Thank you.

YUKO YOKOYAMA: Thank you, Eleeza. Good morning, good afternoon, and good evening. Thank you all for joining us today. My name is Yuko Yokoyama, and I'm the project owner of the SSAD ODP.

You see here an agenda in front of you. I'd like to note that. We will have questions posed at the end of each topic and take a moment to hear your thoughts or feedback before moving on to the next topic. As Eleeza mentioned, this is not the only opportunity for you to provide your feedback, so please bear that in mind. We will also have a general Q&A at the end of this session if there are any other questions unrelated to today's topic.

So let us know begin. First up is the timeline. So I will hand it over to Diana Middleton, who assumes the role of Project Manager for the SSAD ODP. Diana, please?

DIANA MIDDLETON: Thank you, Yuko. Next slide, please. As you may know, the SSAD ODP project delivery date has been extended past the initial six months the ICANN Board originally requested the ODA to be completed. Some of the causes of the delay include the fact that the SSAD is a brand-new concept in a first-of-its-kind system that affects people globally. Various data collection activities have taken longer than expected. This includes extending the deadlines on all three surveys. Also, the data we received has raised more questions for the team to explore as it assembles the ODA. This will require further discussion with the community in the coming months.

Next slide, please. Thank you. The SSAD ODP project team went back to see if we could tighten the delivery date but also allow time for the community to engage in our work. As you can see, on top of the community webinar we've already conducted, plus this month's ICANN session, we have additional webinars planned for November and December. With this new timeline, we are expecting to complete the bulk of our work by the end of November, at which point we'll be able to deliver a final draft to the technical writer in early December.

I want to highlight that, by December, you will have already seen key topics via community webinars I've just mentioned. For example, today we'll be discussing contractual compliance and identity verification. Next month, we'll be discussing the business process design and system design, followed by the cost discussion in December. Shortly upon our return from the holiday break, we'll begin the formal review cycle. Once those reviews are completed, we plan on presenting to the Board by early February. We have planned for a formal publication of the ODA by the end of February, but that could take place sooner depending on the feedback we receive. Please note that community feedback on various key topics could affect this timeline.

I will now hand it off to my colleague, Jonathan Denison, Director of Contractual Compliance. Thank you.

JONATHAN DENISON: Thanks, Diana. Yeah, we're going to go over the compliance portion of the SSAD. It's pretty straightforward. We're going to leave all the fun stuff for Aaron at the end here. But if you go through the recommendations, there are two areas that involve ICANN contractual compliance. The first one would be for mechanisms where complainants can basically file complaints with ICANN Compliance about contracted parties' violation of procedural requirements.

And basically there's a couple examples there that we pulled from the recommendations. For instance, if the contracted party going to deny a request for data, they have to include a rationale sufficient for the requester to understand the reasons to deny. That's one example. Another example would be once a contracted party takes a first look at the request and is inclined to deny. The recommendations state that they first have to reach out to the requester and seek further information about the request for proceeding with the denial. So that's one way that Compliance can become involved in investigating those types of complaints.

Another one is the contracted party SLA requirements. For instance, with each request, there's a priority level assigned. In this example here, that comes from the recommendations. For instance, with Priority 1 urgent request, if the contracted party fails to meet the response time that comes from the policy, then potentially Compliance could become involved with that as well.

And if we go to the next slide, we just go over the general approach. The good thing is that these two areas fit really well into existing mechanisms that Compliance has for handling complaints—for instance, the issues where a requester might imply that a contracted party is not following procedural requirements. Those would fit well into our mechanisms where we have public-facing complaint forms. So they could fill out the complaints, and those feed directly into Compliance's NSP systems. And then, potentially for something like the SLA issues, since we already deal with contracted party SLA issues in other areas, there's potential there for even implementing some type of automation to those types of complaints, since those are generally technical-based type issues. However, as always, the implementation phase will be important when we further develop our methodology and approach because in Compliance we deal with the end language, pretty much. So that's going to help inform how we build everything and approach these types of issues.

And if we go to the next [slide], we do have our questions fairly open. It's kind of a catch-all question. Not everyone, probably, has all the recommendations memorized. So if there are things that occur to you and you come back to us, you can always e-mail us. But the main question is, do these two areas in which we identified Compliance intervention … Are those all the intended areas in which we can enforce from the policy? So that's the main one here.

We also asked the GNSO Council liaison about out approach regarding development of potential complaint forms and automated notifications where possible if that fills the intentions of the recommendations as well.

And from there, we got the impression that we're on the right page. But again, we're open to any feedback and questions you might have.

So that was it. Pretty quick. Again, we can address any questions. Otherwise, we can pass it off.

You got something, Jane?

JANE SEXTON: Hi. My is Jane Sexton and I work in the ICANN Communications department. If you have any questions related to the compliance section, please submit them via the Q&A pod at the bottom of your Zoom screen, and I will read them aloud. We don't have any open questions at the moment, but maybe we'll give it a minute.

Just as an FYI, other SSAD-related questions will be answered at the end of this session.

I don't see anything, so I think we can move forward. Back to Yuko.

YUKO YOKOYAMA: Thank you, JD, and thank you, Jane.

Next [slide]. Thank you. Now we promised that we will be providing the update and results of the GAC survey during the last webinar in September. We have actually received an extension request from [Jacques], given the complex nature of our questions within the survey.

So as a result, we have extended the deadline to the end of the month, the 31st of October. As such, we do not have anything to update on this topic today. We of course wanted to share the results in our future webinar instead.

Next slide, please. Now we're going to switch gears and talk about identity verification methodology that ICANN Org has come up with. I'm going to pass it on to Aaron Hickmann, Senior Director of Operations, Service Delivery, and Support. Aaron, please?

AARON HICKMANN: Thank you, Yuko. All right. So we're going to go through about dozen slides on identity verification. And the intent here is to review background information first on why accreditation and identification is required and then cover some of the concepts that provided a foundation for developing our proposed methodology. Finally, we'll get a little bit into the specifics and review the process for various scenarios for identification verification. And then at the end, just as we did with the compliance section, we'll open the floor for questions and discussion.

So to go back a little bit here, the EPDP Phase 2 recommendations established the requirements for the SSAD system, as Eleeza mention in the introduction. One of the requirements is that any user that gets added to this system has to be accredited. Accreditation can occur in two different ways, and that's based on Recommendation 1 and 2.

So here we've broken down this into two categories. We've got non-governmental, which is really Recommendation 1, and then governmental (Recommendation 2). So here, when we talk about Recommendation 1, this is where ICANN has been established as the Accreditation Authority (or AA, as we've abbreviated and as was mentioned in the chat). We're calling it the central AA to set it apart from other governmental AAs that may be designated or created by governments and territories. And I want to make sure it's clear that, when we talk about accreditation authority, that is not referencing any term in any sort of legislation, like GDPR. This is using the term as defined in the final report for the EPDP Phase 2.

So let's go through the two sections then. In the central AA, accreditation is really primarily determined by verifying identity. Verification methods can be applied to either legal or natural persons, and there'll be some scenarios that we'll go through later in which both can be required. Maintaining accreditation will require renewal periodically, of course, and then abiding by the terms and conditions of the system: can't do anything abusive or anything like that. So to be clear, this first category is where our proposed identification methods will apply.

In the governmental accreditation, countries and territories are allowed to determine whatever method they'd like to follow. Presumably, in many cases, governments would already know which users should have access because they're involved in public policy tasks. So further identification may not be required. But if a government would want to follow the methods being proposed for their accreditation authority, they're of course free to do so. It's really up to them.

Could I get the next slide, please? Okay. So here in this slide, we've broken it down just to reinforce the differentiation between the two categories. Again, in the center column, we're talking about the ICANN accreditation authority, which is the central accreditation authority of central AA. This is really for non-governmental users and will deal with natural persons and legal persons that are non-governmental in nature.

On the righthand column, you'll also see the breakdown for governmental accreditation authorities for countries or territories. That is where they would identify and add users to the system from their governmental entities and deal with that. And then they would also add intergovernmental organizations as well.

Next slide, please. Okay. All right. So here is one of those foundational pieces I mentioned earlier. Identity verification is not just a single term. It could be a range of effort/cost—that kind of thing—complexity. And so what we really had to look at was, well, what is high, what is low, what is limited, what is moderate, what is substantial? Things like that. And we wanted to make sure it's clear that there's no such thing as a perfect system that would be able to identity and verify identity without any mistakes. Every sort of system that you might design has a potential to be compromised.

So what we looked at, though, was, what's reasonable? What would an appropriate level of cost and effort be for identity verification? We wanted to balance the effort that someone would need to make to become accredited as well as the fees that they might need to pay but also balance that against the needs of the system to make sure we have an acceptable level of risk, also called assurance, which is why we have assurance level on this slide.

So as part of this, we really looked a number of different models that were in use around the world and noted that there are these different levels. And so we've laid out here the various levels as defined in a particular model. And we probably wouldn't want to go either very limited or very high but end up somewhere in the middle because we want to balance, again, that verification against risk, cost, and burden. We don't want the cost to become so high that people can't use the SSAD or that it's prohibitively expensive.

Next slide. So with that in mind, we really are proposing a moderate level. I'll get into how we define moderate in just a moment. But, again, we're trying to balance that cost and value. We want to make sure we still can offer a level of comfort for those who are being asked to make the decisions to disclose or not disclose that an individual has been identified. And in the policy requirements, there certainly was a concern about someone being able to game the system or abuse. So we wanted to be sure that we could make any sort of penalties that need to be enforced to be effectively done. So as long as we know who someone is, we should be able to enforce those well.

And at this point, I also want to mention that, when we talk about accreditation, just a reminder: accredited users do not automatically receive data. They are merely able to log into the system and can request it. And then their requests are going to be reviewed and balanced as appropriate.

Could I get the next slide, please? All right. So there are really three sorts of types of verification that we contemplated as we designed the system. We've got verification of natural person (so that's people), verification of legal person (so any sort of legally formed entity), and then there's also a scenario that was noted in the recommendations where you may have a third party that's being represented by a user in the system. So we're going to go through all of these different variations here and drill down into them.

Can I get the next slide, please? Okay. So we're going to start with natural person verification. So when it comes to people, here are the proposed methods that we're presenting here today. We've got the first, which is we'd like to propose accepting what we would call a qualifying electronic ID (or EID). And that may be available in certain jurisdictions. So a qualifying EID, as listed on the slide here, is really a system which is significant. So it's used for things like financial or legal transactions, healthcare transactions—things like that. It also would need to be subject to regulation or has a certain level of transparency so that there's levels of trust using that EID. And then, of course, it would need to be available to the private sector because we need to be able to use it in this implementation.

So if that's not available, then we have a couple of other methods that we would look at. And so there's two flavors which are pretty similar. We've got an individual who has some sort of government ID with a photo, and then we've got a government ID that's enhanced with electronic capabilities. As you may know, there's certain IDs that come with a chip. They're both fairly similar. We would look for a vendor to perform verification of the document. So they would look to make sure that the document features meet that which is known and then compare that to the photo ID with a remote interaction with the applicant—for example, a video interaction—to make sure that the person is real, live human being. And then on the electronic chip level, if we do have an ID with a chip, we'd love to be able to leverage the capabilities of that chip. So we'd still identify the document but then use the electronic methods to further check to make sure it's a valid document.

Okay. Next slide, please. Okay. So let me just walk through the process quickly to take those levels and apply it to how it would flow through. So we've got an applicant. We've got a natural person. If they don't have that EID already, they would need to provide that government-issued ID. The accreditation authority would then verify that ID against the person. They may have to leverage an identity provider. That might be a local entity to check if there's certain things that are specific from local level. And then, once that is done, assuming we're able to get through it, that person then becomes verified and then they're added to the system and are essentially accredited. So, again, this is where there's no automatic disclosure. They're just in the system and then can request access to the data.

Next slide, please. Okay. So a little bit more information about this process. We're proposing a two-year renewal period or potentially upon expiration of the identification document that was provided. So, for example, if you provided a driver's license or something and it expired in six months, the renewal may occur upon six months.

In terms of cost, what we found in the marketplace, based on some of the information we received in the RFI, it's about a $10-20 U.S range for the identification. And I want to make it clear here: we're not talking about that being the accreditation fee. That is simply the transactional fee that a vendor might need to charge for the verification. So actual accreditation fees, as we mentioned, will be talked about in the December timeframe and would be comprised of all the costs for identity verification, system operation, etc., because the system is meant to be self-sustaining from usage.

I think we can go to the next slide. Okay. So then this is another one of the scenarios that I mentioned earlier. We have a situation in which the user may be affiliated. So as we noted, [Göran] works for ICANN, so if we does that, the requirements say you're disclosed that and then verify that that's a possibility. So in that case, we'd have to start with a verified natural person. You'd have to be already verified to be in the system. And then we're going to request certain information about the legal person from that individual—ask for a certification of good standing or a local equivalent. Again, the accreditation authority would review this documentation and make sure they could verify that that legal person exists and that there is an affiliation there. And then, if it's able to get through that process, that legal person would be established in the SSAD and that individual would be linked to it. And then there would need to be some sort of mechanism within the system that would allow for that affiliation to be managed over time because obviously that would change as people and enter and leave an organization.

Next slide, please. Here we're looking at reverification of the legal person for about every five years. This was similar to the renewal period that's already in place for registrars. And I wanted to note here that one of the reasons for affiliation is to ensure that any abusive behavior that would occur by an affiliated user would, could, and should affect all users that are affiliated to that entity. So if one person goes rogue, it could affect everyone affiliated with that.

Okay. Next side, please. Here's the third scenario. This is where have a representation scenario. So this is not, "I work for ICANN." This is maybe a brand protection firm or perhaps a legal entity that's providing this sort of service for someone and is going to be using the system. And so it's a similar flow to what we talked about with affiliation. We've got a verified natural person starting the process again. That individual would need to provide information about who they are representing (that legal person) and provide a point of contact for that legal person so that we can also verify that that individual exists and can be verified. So, again, it goes through an accreditation authority and, once representation is verified, then that entity and individuals can get added, and then representation, again, could be managed within the system.

Next slide, please. Okay. Similar here. Again, reverification of that legal entity at every five years. It is important to note that all parties involved need to be involved in verifying that representation. So it may involve even a person who is not in the system, meaning if you're representing some third party, they're doing that for a reason and they may not be in the system, but we need to verify that we know who they are. And then, again, here, any abusive behavior by someone who's representing an entity could impact anyone who represents that entity or can also be aggregate in the sense that, if you were moving and had a number of representatives and are cycling through them, you won't be able to abuse the system because those abusive behaviors would be noted against that entity that's being represented.

Next slide, please. Okay. I went through a lot of things here. So I want to make it clear that this is not the only questions that we're looking to get answers for here but anything also that people wanted to get clarification on. I think there's a number of questions in the chat pod that we'll start going through. But these are the sorts of thing we're looking for in general from everyone here, including those who are watching the recording. We'll have the e-mail address on the last slide to gather feedback. So if you don't feel comfortable providing information now or just aren't ready, please make sure to send that in. That e-mail address is available 24/7. So we're really just trying to get a feel for if this feels like an appropriate level of verification. Is it a reasonable level of effort for users who want to use the system? And, again, when we're talking about users in the system, there's no automatic distribution of data. It's merely a request as the start.

So I'll pause here and we can go to questions. Jane?

JANE SEXTON: Great. Thank you, Aaron. We first have a question from Brian King. He asks, “What penalties are being completed for abuse?” Aaron?

AARON HICKMANN: Sure. So the penalties in general … In one of the recommendations—I believe it’s 1.5—it contemplates temporary suspension and then all the way up to revocation. They didn’t really limit all the potential ways that we might look at having [counties]. Other suggestions included rate limiting. So for example, you might only be able to do one a day, one a week, one a month, or something like that. And those would be obviously worked out as we get further into the system.

JANE SEXTON: Great. Next up we have a question from Dietmar Lenden. “If you are using a moderately safe system, how are you ensuring very sensitive, like the EID or photo ID, from being compromised?”

AARON HICKMANN: Okay, good question. Well, we haven’t obviously signed any contracts with vendors for this at this point. We would be leveraging vendors. And when I mentioned “moderate,” I didn’t mean to imply that security levels would be moderate in the system. We would expect any vendor who would be doing this work to be using all due care with that kind of information and when they’re processing personally identifiable things and IDs and such like that. It’s more that we’re going to apply a moderate level of verification.

So let me give an example of what might be more extreme. So if we said, "We don't have enough confidence in the methods that have been proposed. We want someone to show up in person to some sort of vendor and verify with their ID right in front of them," that would be more of an extreme level of verification.

So hopefully that separates those two issues.

JANE SEXTON: All right, great. Thank you. Next, we're going to move to a question from Jan Janssen. "Are authorization and identification entangled? Do you need to be identified before you're authorized?" I believe we're going to go Francisco to answer this question.

FRANCISCO CORREA: So a requester has to be first be accredited, as Aaron described. As part of that process, they get the opportunity to set up their credentials—so, for example, username and password. And with that, they later can access the system if they want to submit a request—for example, they need to enter the username and password in the system before they can submit a request. Once a request has been submitted by a user that has been authenticated, then the request is considered by the correct party—the registry or the registrar, as the case may be. And if they approve the request, the authorization for such a request is issued in a technical way that are … I don't know the details. We intend to cover more of that in the next webinar in November. But the point is there will be an authorization that is issued, and that would allow the requester to access the registration data directly from the correct party. Thank you.

JANE SEXTON: Thanks, Francisco. I believe we have a follow-up from Dietmar as well. “When someone is verified/accredited, do they get a simple ID number? Or how does the registrar or registry know who they are?” Francisco, back to you.

FRANCISCO CORREA: Thank you, Jane. So as part of the process, it is expected that details of the identity of the requester are to be shared with the correct parties so that they can consider that information as part of the—I believe the term is the balancing test—that need to make in order to decide if it’s appropriate to disclose the data or not so they will get some data points about the requester—for example, the requester name, the organization name, jurisdiction or country where they are established, if, for example, they are an organization, etc. So those are examples of the data points that are intended to be shared with the correct party as part of the [requester submission.] And, again, more of those details on the design are intended to be shared in the next webinar. Thank you.

JANE SEXTON: Thanks, Franscisco. Next, we have a question for Chris Disspain. “Why do you think the ID needs to be renewed every two years?” I’m going to throw this one to Aaron.

AARON HICKMAN: Sure. So, again, this is a proposal, so we wanted to get some feedback on it. I will note that many of the folks that responded to the RFI actually were proposing an annual renewal, but we felt that identity doesn't really change. You are who you are. So once it's identified and verified [, then] a two-year period could be reasonable. If the community feels strongly, we'd certainly love to hear what would a better one be. I'll note that, with identification, it's really an art, not a science. So we're doing the best to make sure we're adapting everything that's available out there to the needs of the community. So two years just felt like a reasonable accommodation.

JANE SEXTON: Thank you, Aaron. Next, we have a question from Sivasubramanian. "Whie accrediting users, organizations, and NGOs, would the accreditation authority also define the data domain that the class of user could request? A simple example is that of an NGO working on agriculture in a certain geography requesting data related to an IT industry domain (business [inaudible])—for example, that of data related to a portal of high-tech professionals. Would a [traffic] police department in one geography be eligible to request data otherwise considered relevant for a drug enforcement authority? Would a government from a certain geography be considered eligible to request data related to a sensitive organization in another geography or would it all be global, any accredited person or entity accredited globally across domains?" I believe we're going to go to Göran for this answer.

GÖRAN MARBY: Hello. Thank you very much. So when it comes to, for instance, the local drug enforcement authority or government user, I think that's up to the government who should be able to make that request. Remember that the policy says that we should identify the organization someone works for and the individual. Also think that not all requesters might actually be associated with an organization.

And the whole point with this is that we are building a global system, which is one of the things that Aaron talked about. That makes it a little bit complicated because we are actually talking about many different jurisdictions. One law enforcement agency might have access to information with some laws and then in other ones. I know, for instance, in Europe, one law enforcement agency told me, if they just make a query into a system without notifying or having a court order, they actually have to notify the person they're asking about. If they do it through a court order—sorry—they don't have to notify the person.

So there is a lot of different things to take into this. So your question is really hard to answer in that sense. But when it comes to governments, I think it's up to the governments itself. Thank you.

JANE SEXTON: Thank you, Göran. We are going to go to another question from Dietmar Lenden. "How many verifications are you expecting to have? It will be difficult to find someone who can verify in all regions of the world." I believe we're going to go to Aaron.

AARON HICKMANN: Yeah, I could take that one. Thanks, Dietmar. So in the RFI and then also in some research that we did as we were working through this, we have vendors who have said that they could do around 195/196 countries around the world. So obviously that's not necessary every jurisdiction, but we believe we can get pretty substantial coverage through one or more identity providers that would work with the accreditation authority.

JANE SEXTON: Thank you, Aaron. It looks like we have one last question from Reg Levy at Tucows. "This might be a reasonable way to verify corporate searchers, but I can't imagine the average Internet user providing their government ID to ICANN in order to submit an SSAD request. Does ICANN expect that this system will be used by primarily corporate users, as our data has shown is quite likely? And is ICANN comfortable with the chilling effect this request will have on single-use requesters?" I'm going to go to Göran.

GÖRAN MARBY: Thank you, Reg. I think it's an excellent question, as always when you ask questions. First of all, just as a reminder—I wrote it in the chat—we are actually trying to figure out how to operationalize and implement the review [inaudible] PDP recommendation. And the PDP recommendation says that we should build a system like this in this way. So the intention of the system is to fulfill the things from the PDP.

I do think that you're raising an interesting question. The effect of a PDP might be the effect you're looking at. At the same time, we're also doing surveys about the volume of requests. We started doing that inside the ICANN community and I thank you very much, especially to the contracted parties and the registrars who've been helping us with that. But we're also seeking to see if we can have a possibility to actually go outside ICANN to see if there's some potential for us to seek more about the extra volumes because the volumes will of course have an effect on price.

I want to add too that, in the PDP as well, it says that cost of the system should be carried by the one who uses it, which means that the requester will have a cost for actually using the system.

But I think it's a fair question. I would come back to that later. I think that the ODP shows how important it is to have an OPD so we can raise those questions before we start actually building something because I think it's a fair question. Thank you.

JANE SEXTON: Sorry. Just looking to see if there's more questions in the Q&A pod. One second.

GÖRAN MARBY: I got one additional question from Becky Burr, one of the [inaudible] members of the ICANN community, who asks, "How much will this cost per [authentication?] And will the cost vary from jurisdiction to jurisdiction?" Who would like to take that one?

AARON HICKMANN: I could take that, Göran. So this is where, for natural person, we believe the range is around $10-20 U.S. the vendors we've seen actually don't really have much of a difference between jurisdictions. Really, they have a standard approach, and all they need to really do is add each individual country's ID, and they sort of do the same process repeatedly. So the range should hold at that.

I just want to note that, while that's the transactional cost, again, that doesn't represent the full cost for accreditation, as there may be other costs that need to be bundled into that. And we're going to be discussing more about costs in the December webinar as well.

GÖRAN MARBY: To give a little bit more insight to what Aaron said, you can divide the cost for any system like this into development costs of the system and then the running cost for the system and then the [moveable] cost for the system. If the system costs $10 million to implement and then it costs usually $2 million to run it—that's sort of a benchmark—and on top of that you also have the cost that we have to pay to other vendors for doing that … Of course, you go into [excellent] discussions about depreciation and all of that. But what Aaron said was that the transactional cost is not the only cost. That will be borne by users of the system. Thank you.

JANE SEXTON: It looks like we have a hand up from Leon. Before we go to him, just a reminder that, if you have any comments or questions, please use the Q&A pod at the bottom of your Zoom screen. Can we unmute Leon, please?

Andrea, are we able to unmute Leon? I can't hear anyone.

Oh, accidental hand. Okay. Thank you again for … Looks like we have an additional question from Chris Disspain. I'm going to read it out loud now. "I'm slightly confused. Are you saying that this ODP will not consider the benefits of this whole thing but simply will structure and cost it? If so, then who gets to assess the cost/benefit, and when do they do that?"

GÖRAN MARBY: Chris, excellent question. And I know why you're asking it: because you [know we're aware]. So thank you for giving me the opportunity.

So there is really many points to this one. One of them is actually the discussion like this with the ICANN community to hear your thoughts about it. The Board has of course the full responsibility for making that decision in the end. And if the Board disagrees with the PDP in some shape or form, the Board has to go back to the GNSO. But the GNSO, when they accepted the PDP, they added a notion that the Board has to come back to the GNSO and actually discuss the cost benefits of the whole system.

So I think there are several built-in [layers] of this. The ODP is not the decision maker. The ODP prepares the material or the Board and also for the GNSO. And that's why the outcome of the OPD is one thing but we are doing the work to figure it out. But remember, the ODP is to make sure that the Board has sufficient detail to make the decision. So it's the Board who makes the decision. So I'm happy that you helped me to clear that up.

JANE SEXTON: Thank you, Göran. Doesn't look like we have any additional questions in the Q&A pod, but if you do have one related to identify verification methodology, please use the Q&A pod at the bottom of your Zoom screen to submit any questions.

All right. If you don't have any more questions, then let's move on to the next slide. I believe it goes back to Yuko.

YUKO YOKOYAMA: Yes. Thank you, Jane, and thank you, Aaron.

JANE SEXTON: Oops. Sorry. We got one question in the last second.

YUKO YOKOYAMA: Okay.

JANE SEXTON: We have one from Becky Burr. Her question is, “Of course, don’t we also need to know how much users would be willing to spend for authentication and on a per-query basis? And how will we know that?”

GÖRAN MARBY: So I think that’s also a very fair question. Remember, as I said before, we are trying to operationalize the actual PDP recommendations. And as we said, we are coming back in December with a more full discussion about the cost of the system and how that relates … And potentially to come back to the GNSO about if there are things that we can improve from the review recommendation that might take down the cost because I think that’s a fair question. And I don’t know the answer to the question of how much people want to pay for it because that question has never been asked before. And we couldn’t have asked it before because we didn’t actually know what it was going to cost. So I’m looking forward to continuing that conversation.

JANE SEXTON: Thank you, Göran. All right, back to you, Yuko.

YUKO YOKOYAMA: Okay. Thank you for all the very good questions.

All right. So we’re going to go back to, now, what’s next. First and foremost, we need your feedback. We shared a lot of information today, including Org’s assumptions and questions to the GNSO Council. If you can think of any feedback or input after today’s webinar, we encourage you to submit it through our publicly archived mailing list. You see the e-mail address here on the screen. We plan to analyze the feedback submitted and utilize the information to further the ODP work.

We will also be posting a [inaudible] summarizing today's session.

I also want to reiterate that the SSAD ODP project team is committed to keeping the community informed and involved throughout the ODP process. As such, we are planning to have several more webinars, as Diana has mentioned during the timeline discussion. We currently have plans for November and December webinars, where the format will be similar to today's session, meaning that we'll be sharing these substantive methodologies and design that we came up with during the ODP process.

For the November webinar, we plan to share business process and system design and our assumptions and questions related to them. It will be held on 18 November at 16:00 UTC, and the announcement will be made soon with the registration link. At the December webinar, will be focusing on the cost estimate and fee structure of the SSAD as well as sharing the results of the GAC survey. As soon as we determine a day and time, we will make sure to post an announcement to you.

So this concludes our presentation portion of our webinar.

Next slide, please. So we've already taken some questions on contractual compliance and identity verification methodology, but I'm going to open up the floor to see if there are any other questions unrelated to those two topics. Or if you think of more questions than those two topics, you are welcome to ask in the Q&A pod. Also, I want to reiterate that this webinar is not the only time you can share your thoughts on what we presented today. So we welcome any written feedback which can be submitted via e-mail to opd-ssad@icann.org.

Back to you, Jane.

JANE SEXTON: Thank you, Yuko. Looks like we have one question in the pod from Sivasubramanian. "Does the process define limitations [specificity]? For example, could an accredited entity give us all non-public data from the .com domain or give us all non-public data related to the registrants from South Africa?" I believe we're going to go to Francisco for this answer.

FRANCISCO CORREA: Thank you, Jane. So part of the policy recommendation … I cannot remember immediately the specific policy recommendation, but there is one that says that the requester has to specify the domain name or domain names for which they are interested in discovering the registration data or a subset of the registration data, which is also an option. But they cannot, for example, request the non-public registration data under a [inaudible] TLD or of a certain region or registrant. They have to provide the specific domain name or domain names they are interested in. Thank you.

JANE SEXTON: Thanks, Francisco. We have another question from Jan Janssen. "Will costs be limited to identity verification, or will there be extra costs on a per-request basis?"

GÖRAN MARBY: Marketing the event we're going to do in December, there will be three types of cost. One of them will be the cost of the individual … When you become a member of the system, the requester has to pay a cost. The second part is if there is a cost every time you use those credentials. So that's a [moveable] cost. But the second cost … Basically, there are two different parts. One of them is the initial investment of the system plus the running cost of the system. So you might say that's going be three different costs that all go into the cost for the requester. I hope that answers your question.

JANE SEXTON: Looks like we have a follow-up from Jan. "Will the registrar be paid as well?"

GÖRAN MARBY: In the current model, in my understanding, in the recommendation that is not the case, in our understanding. And I don't think we thought about it in that sense—that the contracted parties are receiving a request. And I haven't heard that they asked for additional funding if they are to build a system. And I think that's something that we therefore have to think about. I don't think that's in the plans today. That will of course only increase the cost.

Chris asked a question in the chat as well. Or a flag. Would you like to expand on that one, Chris?

Can we give Chris the floor, maybe? Or the mic or whatever it's called in Zoom? I've only done this for one-and-a-half years.

ANDREA GLANDON: Yes. One moment.

GÖRAN MARBY: Don't ask me, Chris.

ANDREA GLANDON: We'll open your line, Chris. It'll be just a moment.

Okay, Chris, your line is open now.

CHRIS DISSPAIN: Thanks, Göran, and thank you for opening the line up. It's hard to type. There's so much information. What I'm trying to say is that I think the GNSO have said, when they sent this up to the Board, that what they would like to have done is a cost benefit analysis so that the usefulness of the SSAD can be considered. Now, I make not judgement about whether it'd be useful or it won't be, but it seems to me that, if what the Board is going to be faced with us a perfectly legitimate ODP which looks at the costs, etc., and the Board is the group that's going to be doing the benefits analysis, having looked at the system and the costs, given the preamble that GNSO put in place that said there should be a cost benefit analysis, then I think the GNSO itself or the community generally should be able to contribute to that cost benefit analysis. And there is no process in place to do that, as far as I'm aware.

So my suggestion is that we have the time, if we choose to do so, to put this process in place while this OPD is going on, so that, when the results come to the Board, there is something that enables the community to be involved significantly in the discussions about the cost benefit analysis.

And thanks, Göran, for giving me the floor.

GÖRAN MARBY: Thank you. I don't disagree with you, Chris, at all. I always think it's possible [and good] with the community interaction. One small flag is that the intention is to have the discussion with the GNSO Council about the cost benefit before the Board actually makes its decision. So maybe we can calm you on that point. And I'd love to engage in a conversation with the GNSO if they would further open up some of the discussions based on the cost. I have no problem with that at all and agree with you to maybe have an interactive discussion about the cost benefits.

What we are tasked with also is to make that the ODP in itself doesn't open the full policy question because that is actually decided by the GNSO Council. But we can always sort it out with the dialogue.

JANE SEXTON: Thanks, Göran. If anyone has any other additional questions related to the SSAD, please submit then via the Q&A pod at the bottom of your Zoom screen.

Not seeing any questions at the moment. Unless we get anything at the last second, I'm going to throw it back to Yuko to end this session. Thank you.

YUKO YOKOYAMA: Thank you, Jane. Seems like, since there's no questions at this point, we will be ending this session with a reminder that any questions you can submit to odp-ssad@icann.org. Thank you all for joining us today. Have a good morning, afternoon, or evening. We can stop the recording now.

[END OF TRANSCRIPTION]