ICANN86 Seville | PF – GNSO: SSAD Supplemental Recommendations Session (1 of 3)
Monday, June 08, 2026 – 10:00 to 11:15 CEST

ANDREW CHEN

Hello and welcome to the SSAD Supplemental Recommendation Session 1 of 3. Please note this session is being recorded and is governed by the ICANN Expected Standards of Behavior, the ICANN Community Anti-Harassment Policy, and the ICANN Community Participant Code of Conduct Concerning Statements of Interest.

Please observe the following guidelines to participate in this session. I will post them in the chat for your reference. Only questions posted in the Zoom chat identified as a question will be read aloud during the session as time permits and when directed by the chair of this session. If you wish to speak, please raise your hand in Zoom or otherwise as directed. When speaking, please state your name for the record and speak clearly at a moderate pace. I will now hand the floor over to Marc Anderson.

MARC ANDERSON

Thank you, Andrew. This is Marc Anderson, lead of the SSAD SRT team. Hopefully that's not me, a little bit of an echo here. So, welcome, everybody. This is a working meeting of the SSAD Supplemental Recommendations Team. I am the lead of the team and will be shepherding us through our discussions today.

I see we have a good number of guests in the room. Welcome, everybody. I thought I'd start off with a little bit of an intro for those of you that might not be familiar with what we're doing since we do have a good number of guests observing today.

So, the SSAD recommendations, the System for Standardized Access and Disclosure, have been published for quite a few years now, but there were a lot of questions as to their viability and feasibility. So, ICANN has been running an RDRS pilot to flush out the feasibility of the SSAD system. There was a standing committee that evaluated the results of that pilot, ably chaired by our own Sebastien, who's in the room today. Thank you, Sebastien.

And that standing committee produced a set of recommendations that formed the basis of our purpose here today, which is to review the SSAD recommendations. And based on the findings and recommendations from the RDRS standing committee, produced supplemental recommendations that are in the best interest of a broader ICANN community.

So, like I said, this is a working session. I see most of the people around the table are members of the supplemental recommendations team. Guests are obviously welcome, but I'd like to ask that we reserve participation for members of the team only. We have a light agenda for today. If we could go to the next slide here.

We're going to focus on recommendations one and two today, which deal with authentication and authentication of government

entities. Andrew sent an email yesterday to the team teeing this up, but I'll just sort of introduce it.

Based on our conversations from yesterday, there was some question around Section 1.4 of the proposed straw man policy recommendations. They're currently sitting in the implementation guidance section, and there was some discussion yesterday about whether they should be in implementation guidance or whether they should be moved to policy recommendations.

So, we're going to start off the conversation today looking at that. We'll take a look. We'll pull up the straw man document itself and look at it in there, and I'd like to encourage the group to have a conversation about that. Discuss what aspects that are currently in implementation guidance we want to see in actual policy recommendation language. And as a reminder, let's focus on making sure we have implementable policy recommendation language. What is the desired policy that we want to see from the language we're moving into policy recommendations?

From there, we want to cover a new topic and this came out of some of the conversations we've had so far. What is the minimum information a contracted party needs from an authenticated user? The conversation started, I guess, a couple of meetings ago when somebody asked the question, as an authenticated user, what do you get? And I thought that was a pretty fair question.

But what you get out of being an authenticated user is you get additional information that's passed to the controller, the

disclosing entity. And that additional information can help inform a disclosure decision. But nowhere have we defined what is the minimum amount of information that would make that authenticated user useful to the disclosing entity. So, what I'd like to do, and I know this is just teeing up the conversation today, I don't expect us to have a final answer on this. But what I'd like to do is start the conversation. What do we as a supplemental recommendations team see as the minimum viable information that is necessary?

And I think we know that different user groups are going to have different information that they'll pass along so we're not looking for a solution that fits every single use case. What we're looking for is, what is the minimum amount of information that would make this useful to the disclosing entity?

And then lastly, we've had a conversation, and I know some people have raised their thoughts on this. There's been some discussion in chat. Thank you for that. But we want to have a conversation about whether we can combine RECs 1 and 2 or not. And if we do end up combining them, what is all the information that currently exists in REC 2 that we would want to see moved into REC 1 on authentication? So, I know some people have already weighed in on this one so I look forward to that discussion, but that's the agenda we're looking for.

If we get through these, we'll move into recommendation eight, which is authorization, but if we don't get that today, that's okay.

We'll save that for our next meeting. Any questions on the agenda before we get started? All right. I don't think I'm missing any hands. Why don't we dive right into it? Okay, this is good.

So, Andrew's pulled up for us section 1.4 and this is the language that's currently -- In the straw person document, this is the first language that follows the implementation guidance section. So, I'd just like to just start things out, just throw it out to the group. And Sarah, I don't know if I can put you on the spot. I know you put some thoughts into email, but what here do we think needs to move from implementation guidance into policy language and why? And I'd really like to get to like, what is our desired policy outcome from this language? So, Sarah, please kick us off.

SARAH WYLD Thank you. This is Sarah Wyld and with the Registrar Stakeholder Group. So, we looked at 1.4 and noted that it's in the implementation guidance, but we think it should be in the policy language because the specifics of it are so important. With implementation guidance, it's guidance. It's not quite mandatory. There can be adjustment and we felt that we want to make sure that these specific elements really do become required for this process.

So, already included, it is up on screen, 1.4.4, those are all really important. We especially think about the credential management and the security properties, but as well as circumstances for revocation because that's something that we noted in the RDRS

that we didn't really have. So, all of this is important and should be kept and on top of that, I had a series of questions. I had a series of questions from like two public comment periods ago about authentication. And so, I compared those to what we already have, and then resulted in a few other questions that I think we should answer, which I then presented more in statement format.

But the questions I'm thinking of are like, who has ability to view and manage the users? And if the responding party can't see a list of users, then how does the responding party know that a given requester is authenticated? So, there needs to be some level, something like a token or a confirmation of some sort. And then that feeds into the third question that Marc presented that we'll get into later.

Then the other questions I had tie to other aspects of our recommendations, but are important here. So, we have, does the system track data about how the authentication is used in relation to disclosure requests, and who has access to that data?

So, that should be thought about in this recommendation, but it's related to reporting. And on that note, also, what public reporting is done about authentication, and what private reporting is done? Are they different? Who audits the system operator to ensure that there's adherence to requirements by that operator? If we don't have the accreditation authority that was envisioned in the first place, then we would have something more lightweight, but there needs to be some level of oversight, so that should be considered.

And then finally, what happens if the system operator itself isn't adhering to those requirements? So, if we set out a standard of what the designated user group needs to do, and then they're not doing it, how do we deal with that? So, that was what I presented in the email and I hope that's a helpful starting point. Thank you.

MARC ANDERSON Thank you, Sarah. I appreciate you letting me put you on the spot there to start things off. And I see staff has put the bullet points that Sarah just went over up on the screen. So, thank you for that. Any other thoughts on this one? Anne, please go ahead.

ANNE AIKMAN-SCALESE Thanks. It's Anne, a NomCom non-voting councilor. And I feel very supportive of all of these points that Sarah has made. It does strike me that there's a lot about it that actually happens in the implementation phase. And that it might differ from one authenticated user group to another.

And so, how do we account for the fact that much of what's described here, and it does say must for implementation -- I don't object to moving it into policy, but somehow, we have to understand that it's not more of the broad general policy that we usually use. A lot of it is about implementation and the questions that we want to ask of each group could be different and different criteria developed along the way for authentication. So, I'm not sure how to split the policy side from the implementation side.

MARC ANDERSON

Yeah, thanks, Anne. I think that's a great question. I wish I had a great answer for that one because I think that's what we have to solve for is, what's the language we need in policy and what is more appropriately left for implementation? But I'll go to the queue. Sam, please go ahead.

SAMANTHA DEMETRIOU

Thanks, Marc. This is Sam with the Registry Stakeholder Group. You asked a question at the beginning of this, which is, what is it that we're trying to achieve with this revised policy recommendation? And I think this very much gets to the question you raised, Anne.

I think what we have agreed to, based on our conversation yesterday is that, this recommendation should say that there should be an ability for authenticating bodies to authenticate users that then access the future system. And so, I think our task under this particular item is to come up with the minimum set of criteria that those authenticating bodies must engage in, or they must have in place in the process of their accreditation.

It's not our job to come up with the details of each, because like you said, they're going to be different based on different user groups, but it is our job to set kind of minimum standards that then those accrediting bodies would meet per their own specific, you know, the unique circumstances that their user group embodies. So, I

think that's the task here. And I think that maybe also gets to the question of like what becomes policy versus what is a matter of implementation that we don't need to work on as a group.

MARC ANDERSON Thanks, Sam. David, you're next.

DAVID BEDARD Thanks. Thanks, and good morning, everybody. It's David Bedard, GAC Canada, just for the record. I think Sam probably more eloquently said what I was about to say. It's good. These questions that are initially there, and thank you, Sarah, for posing some additional considerations, I think they're really helpful for the discussion.

But I just want to make sure that we don't get bogged down in too many prescriptive elements in terms of how folks must respond. So, it's good to sort of set the floor, set what guidance or what we should have in policy. But I just don't want to get us too prescriptive in terms of what identity providers need to provide in terms of that it should all look the same. I just want to make sure that that's considered. Thanks.

MARC ANDERSON Thanks, David. Hadia.

HADIA ELMINIAWI

Okay, so I did raise my hand to basically the same thing, that recommendation 1.4 needs to be rewarded in order to fit the policy section. Implementation details need to be left out. So, as an example, when we say must, this could apply to establish general technical standards and administrative criteria for user groups seeking authentication.

However, the part that says the supplemental recommendations team expects that an interested group would reach out to ICANN, this is too prescriptive, and that kind of text needs to be omitted from the policy part. Also, at the very beginning when we say ICANN org or its designee, we assume it's a designee, but we don't know. It might end up to be one or more. We just know maybe this is also an implementation thing, so maybe we can say also designee or designees. So, let's avoid being too prescriptive and put it at a policy level. Thank you.

SEBASTIEN DUCOS

I am Sebastien Ducos for the record. First of all, they made a point of saying it yesterday, NCSG is not in the room, so golden opportunity to agree with Winston. Oh, you are. Sorry, I missed you. Got a spy. I wanted to chime a bit differently here.

I agree with everything that has been said. We shouldn't get too prescriptive, except, and I'm going to contradict what I was saying yesterday, except about law enforcement, except about law

enforcement and that authentication, if it's the first thing that we're going to look at.

Because of the weight a badge carries, because of that, I don't know if it needs to be in this policy or in another policy, but I would suggest that we have in policy the clarity that we need to have as responders of who we are talking to. Not just the individual, but the jurisdiction, the mandate that that individual, that authority may have in their own jurisdiction. It makes a difference for me to understand that I'm talking to --

In my jurisdiction I understand, in France, I know exactly what a cop is allowed to do and not, roughly. I know what other authorities, governmental authorities are allowed to do about, you know, whatever, searching my car and things like that, that the police is not allowed to do just like that. I don't know that in other jurisdictions. I can't know that in other jurisdictions and it makes a difference to me to get a request from a police officer, to get a request from a police officer that is backed by a judge, a court order. All these things make a difference to me when I make that judgment. So, because of the weight of the badge, I would suggest that we should have that in policy.

MARC ANDERSON Can you hear me on this one? All right. Sorry about that. Can I put you on the spot? What you say it makes sense, but I would think jurisdiction would be needed in all cases. If you don't have an

answer right now, that's fine, but maybe think about like, how would I turn that into policy language what you just described?

SEBASTIEN DUCOS

Can you hear me? Oh yeah, here, this one works. So, jurisdiction is not a question, and by the way, it's already in the forms, in the RDRS form. But the fact that I understand I'm talking to French authorities is not in itself, for me, enough of a guarantee that the person I'm talking to is allowed to ask me the information that they want. And there is no way for me to know that.

The local authority has to be able to say, this is a person that could present a court order. This is a person that is entitled to their data. To have that sort of level of granularity in the jurisdiction that is presented to me. And again, I keep on saying and repeating the same thing, because otherwise, authorities that come from too far from my knowledge outside of my perimeter, maybe complete valid law enforcement, but I will deny it because I don't know who I'm giving that data, if they're allowed to have it, if they can be trusted with it, and et cetera. And, I'm not going to put it on the record, but I have examples of jurisdictions where I've had to say, "No, I just don't know that I can give you that."

MARC ANDERSON

Hello. Okay. For those of you online, we're having a little bit of challenges with the microphones in the room so apologies if the sound's a little scattered. I want to add, you know, Sebastien, it

sounds like you're getting to authorization within authentication, right? And I think we had a long conversation about that yesterday. I don't think that we can ask accrediting entities to authorize access.

We can ask them to authenticate who their users are, but we can't ask them to authorize access to data at the authentication time. That's ultimately a decision of the data controller. I know we have a long queue, but maybe we can come back to that one. John.

JOHN MCELWAINE

Thanks; John McElwaine, for the record. So, I don't think I'm going to be particularly helpful. I did do my homework, but I'm a little bit lost where we are because I think this is diving into some new issues that weren't part of the original reading. So, if I'm hearing right, maybe from Sebastien, is that we want to make sure that the rules we developed for 1.4.5 aren't so restrictive that it would read out law enforcement. Can I get a nod? Was that your concern, that if we make too many details on 1.4.5 then law enforcement wouldn't be able to get accredited, wouldn't neatly fit that? No. Okay. So, I am really lost.

Secondly, I'm not sure where Sarah is, but Sarah seemed to basically be summarizing the six or seven pages of policy that was in the EPDP like auditing and public reporting. So, I could use a little bit of background. Why was that in the EPDP? And are we

really just looking to add back in everything then that had been previously? So, maybe if Sarah could talk a little bit about that.

It seems to me like we're just taking the system that had been developed. Maybe we want to tweak it a little bit and that's what I'm not prepared to talk about because that was a lot of new text, but we're just making it optional, right? You don't have to be accredited, but now we have all these rules and we think we need to add some of them back. So, again, forgive me for asking questions, but I'm just trying to get up to speed as to where we are this morning.

THOMAS RICKERT

Thank you so much. Thomas Rickert for the record. So, I think that we're making it extremely difficult for us to discuss this because we have the text in front of us, but I think we haven't agreed on this conceptually. And maybe we would do ourselves a favor trying to get aligned on how we want to structure this.

I think what we are looking at is different types of user groups of the SSAD. So, we have individuals that might want to find out who is behind the website, let's say, where unauthorized pictures of them are published. Then we may have companies that have been exposed to cyber-attacks that want to find out who's behind that. And then we have other groups that are for likely under the definition of DUM, as we discussed yesterday. Lawyers, law enforcement, consumer protection agencies and others.

And I think that we can define rough parameters for each of those or some common parameters, but I think we can't discuss everything for everyone. I think we can come up with a set of requirements for these individual users, and then there should be a possibility for ICANN to enter into arrangements with these DUMs, and then the criteria for different DUMs may be different. So, there needs to be an opportunity for ICANN to accredit those Designated User Groups that what we came up with, I think Sarah used the word DUMs.

And they -- DUGs, okay, DUGs, okay, it's too early, Designated User Groups. And Sebastien's part comes in there because the Designated User Group administrator, if you wish, let's say the person in charge with a law enforcement authority, needs to make sure that they only allow people into the system that are actually authorized to issue requests so that it's not the person cleaning the office or something that might also be on their payroll.

And then we need a mechanism to revoke that accreditation, if we may call it accreditation, if we find out that one of the DAGs is rogue, that they're using this for the wrong purposes. And I think maybe we can visualize that, that we're looking at this federated system where we have direct users and then sort of indirect users that come through a DUG. And what we need for everyone is, you know, to start with who are we talking to, email address, and name, and role.

Also, the jurisdiction that they come from, the legal basis based on which they ask for the information. Or if they can't specify that, the reason as to why they need the information that they're requesting and the set of information that they're asking for. For some, the registered name holder is good enough. Others might want an email address or the phone number or whatever might be on file in addition.

And then for the DUGs, we might ask for the registration number with the Bar Association to find out that somebody is a lawyer. Not to say that they're going to get the disclosure granted, but just to find out that we are talking to someone who is in the legal profession. And then for law enforcement, there might still be a different set of requirements. Does that sound fair? I don't want to take your role, but I think it would be good to get some agreement on this general structure and then go from one part of that concept to the next.

MARC ANDERSON Can everybody hear me? All right. I think our microphones in the room should be working now so hopefully that continues. Thomas, thank you for that. I think we maybe got a little bit in the weeds there and I think that helps bring us up a level.

I think maybe more specifically, what we're looking at in Section 1.4 is, what are the minimum requirements that we need from a Designated User Group? So, I think maybe I'll take it up even another level from where you left us, you know, I think we don't

want to get too prescriptive because we know we're going to have different types of user groups. So, we want to make sure we have flexibility for different types of user groups, but what are the minimum requirements we need to have for all of these Designated User Groups?

And I think to your point, what are we trying to solve for? I think that's what the language in 1.4 gets to. In order to be a Designated User Group, what are the things you need to bring to the table? And previously, that was all in implementation guidance. What needs to be moved to policy and what can be left to implementation? I think we have Hadia, but you're coming off of an alternate now.

HADIA ELMINIAWI

Leah did not join the room yet, so I'll log out. I will just say this one question and I'll log out and she'll log in. So, she's not logged in yet. So, I just raised my hand to say that yesterday there was this suggestion of putting Recommendation 2 along with Recommendation 1. And I guess with this discussion that we're having today, it will be very difficult to do this.

So, Recommendation 1 is better off without any specific group in it because we are saying it needs to be at a policy level. It doesn't need to be too prospective. And if we are going to be talking about non-authenticated users and authenticated users who belong to Designated User Groups then it doesn't make much sense to

identify a specific Designated User Group in this recommendation. Thank you. I'll log out now.

MARC ANDERSON: Thank you, Hadia, and welcome, Leah. Anne, you're up.

ANNE AIKMAN-SCALESE: Thank you. By the way, I agree with not merging Recommendation 2 into Recommendation 1. I'll just say preliminarily, though, that I think the staff has proposed some great language on Recommendation 2 that maybe just might need to be modified to say, but guess what, in Recommendation 2, all those who have these public policy concerns do need to be authenticated so it refers back to an authentication process.

But I think going back to what Seb said, that he's actually asking or identifying a little bit different question. You know, Thomas said, okay, you're going to have the law enforcement Designated User Group and then you'll have law enforcement coming in that may not be part of the Designated User Group. And I think that what Seb is saying is, let me see your badge.

In other words, if I was driving down the highway and I'm speeding, okay, and the lights go on behind me and I get stopped for speeding. And a guy comes up and he's wearing a uniform and I say, "Well, you know, let me see your badge. Are you really a police officer? Are you really an authorized police officer?" In a Designated User Group, you might have all of that pre-screened by

the -- Almost the Designated User Group having procedures that we can trust.

When an individual law enforcement officer comes in and may not be part of a Designated User Group, there needs to be a process that I will call, let me see your badge. And, you know, how we actually do that, again, may come back to implementation because we're going to need a whole lot more input from PSWG on elements beyond the email addresses, guys, because email addresses don't make it. That really constitute, you know, yes, I do know who I'm talking to. So, let me see your badge, I don't know how we establish it, but I think that's what Seb is talking about.

MARC ANDERSON

Thank you, Anne. Maybe just a reminder, in the original asset recommendations, there was assumption that everybody would be authenticated all the time and that proved to be cost prohibitive. That is not the case with the current proposal, where anybody can submit a request and the data controller will ultimately have to, based on the information they have, or are able to exchange with the requester, make a determination.

And that what the proposal on the table from the RDRS recommendations is that there will be ability to have Designated User Groups that will have an additional level of authentication. But that doesn't mean there'll be an offline process to authenticate everybody, right? If you're outside of that Designated User Group,

then it's the same disclosure process that exists in the RDRS pilot today. Does that help, Anne?

ANNE AIKMAN-SCALESE: No. I'm saying that law enforcement will come in through Designated User Group and law enforcement will come in outside of Designated User Group and authentication has to exist for both of those. For example, Lawrence raised the issue of global south, these people are not necessarily, you know in Interpol, in Europol in F, obviously not FBI -- There's Lawrence. Hi, Lawrence. He even mentioned yesterday that they may be coming in individually and may even have some strange looking email addresses that, you know, might be not be.gov or, you know. So, those people have to be able to access the system as well and there has to be a way to say, “Let me see your badge.”

MARC ANDERSON: So, do I understand correctly that you're proposing that the system must provide a mechanism to authenticate any and all law enforcement users?

ANNE AIKMAN-SCALESE: I believe that's true and I think that Lawrence raised this issue about Global South, perhaps he can speak to, that they aren't necessarily going to be part of a Designated User Group. Sorry, Lawrence, to call you out, but we did have a discussion.

MARC ANDERSON Lawrence, do you want to jump the queue there and respond to that?

LAWRENCE OLAWALE-ROBERTS Yes. Sorry for coming into the room late, but definitely I believe that there needs to be access provided for law enforcement that isn't organized or recognized by global bodies like Interpol or Europol. The discussions we've been having with PSWG, you know, suggests that there are global bodies in terms of law enforcement that are networked together. And we're not too sure if law enforcement from the global south, basically around Africa and all that, are integrated into that global network.

But definitely there will be instances where there will be need to assess SSAD and for such a need, there should be provisions for law enforcement in our local regions to be able to assess the portal or the system and get the relevant information needed to do their jobs.

Taking this a step further, you know, talking about Designated User Groups yesterday, there are also other user groups that are not law enforcement, business-minded groups that would also need access to SSAD. And the form or the mode of them being authenticated and allowed to assess the system also has to be adequately looked into to ensure that they're also not left out of the system. Thank you.

MARC ANDERSON

Thank you, Lawrence, and we've spent a little bit of time on this one, but I want to make sure we're on the same page because the proposed system that we're talking about allows access to anybody, period. Hard stop. All right. Is there anybody that's not clear on that? Okay.

We're proposing a system that does not require authentication for everybody because we know that that's prohibitively expensive. Is that also understood? All right. I'm getting nods in the room. Okay. We're proposing a system that supports third parties working with ICANN to establish an authenticating body, what we coined the term Designated User Groups, who can work with ICANN to establish authentication systems where they can authenticate their members, provide an additional data point to data controllers when making their disclosure decisions. Okay? That's open to anybody.

I think we all understand that there's an existing effort underway with the PSWG that Lawrence alluded to, that's not an exclusive club. Anybody is open to join that and our proposal is that anybody can work with ICANN to establish their own Designated User Groups. Okay? We're all on the same page on that? It sounds like we're getting a little off track on that one. Okay, I've got some people that have been in the queue for a while, so I'm going to get to, Steve Crocker. Steve, please go ahead.

STEVE CROCKER

Thank you. I would say, I'm not quite on the same page. Let me pose the following. What you just said has two parts to it. There's Designated User Groups and there's people who are not part of a Designated User Group that want to present themselves and ask questions. That's fine. But with respect to these Designated User Groups, who decides when a Designated User Group is approved for making requests and for having their requests treated with authenticated users? Or to focus attention from the data holder side, what happens if a data holder says, "We don't really trust the level of authentication that's provided by this data holder group," who said that we have to accept them in that process?

MARC ANDERSON

So, Steve, as I understand your question, you're getting to what level of trust must the data controller provide to requesters that come via a Designated User Group? And as I understand the question, or as I understand the answer, that's ultimately up to the data controller.

STEVE CROCKER

No, it's the reverse, in a sense. What level of trust is required of the Designated User Group? These Designated User Groups, what admits them to be able to participate as a Designated User Group And is there an obligation by a data holder to accept their authentications?

MARC ANDERSON

So, I think there's two parts to that question, right? I think as you look through the recommendations in the straw man for REC 1, we're tasking ICANN with the job of working with Designated User Groups to establish minimum criteria for them to integrate with the SSAD system as an authenticator, right?

And we're leaving the decision on whether to trust the assertions made by the authenticating entity to the data controller. It's ultimately up to them what level of trust that they place in part based on the information we have in 1.4, right? I think this is all information that a data controller would take into account when they're making the disclosure decision. Correct me if I'm wrong there.

STEVE CROCKER

So, here's the point. ICANN gives approval for the creation for a given -- The group presents itself, says, “We want to be an accredited Designated User Group.” And ICANN says, “Fine, you now exist as a Designated User Group.” And then the request goes over to a data holder and the data holder says, “Okay, this is a request coming from a user within the Designated User Group and the Designated User Group has authenticated them.” But how do we know as a data holder that that's adequate for the risks that we understand?

And that question is related to, if you're going to set a minimum standard, what's the purpose of that minimum standard? Is it actually sufficient to meet the needs of the data holders, or is it simply sufficient for ICANN to say that they do, but nonetheless the data holders are still in the position of having to separately probe what the processes are, what the rules are, and what the credibility is of that Designated User Group. In which case, the establishment of the minimum criteria becomes less meaningful, I'll say, generally.

MARC ANDERSON So, Steve, I think you're getting to the heart of what our discussion is about today, which is establishing, you know, 1.4 is, what are the requirements for a Designated User Group? And the other part of our assignment today is, what is the minimum information that a data controller needs about an authenticated user for that information to be useful, right? So, I think what we're trying to do today is establish policy language that answers that question.

STEVE CROCKER So, let me put a particular example. If I'm a data controller, if I'm a data holder, and I have to trust this. One of the things that I want to know about any requests coming from anybody is, are they accountable for misuse? And how do I have that level of confidence that if there is a problem, there is recourse for dealing with that?

Otherwise, I'm taking an unbounded risk in dealing with somebody.

Just the fact that they're coming in from, you know, hacker group two in some country that says, “We are experts in computer security. We need access to all this information and we have our own authentication mechanisms,” and we present ourselves as a Designated User Group, surely that should give us access to any data holder, and we simply present our credentials. You're happy with that, right?

MARC ANDERSON I'm going to go to a data controller next. So, Sarah, can you --

SARAH WYLD Thank you. This is Sarah. I will speak to that, but I had my hand up a moment ago for a different point. So, I'm going to go back to the earlier point and then come back to this one. So, with regards to combining the two recommendations, which I know was later on our agenda, but has already come up in the conversation so I will speak to that point. I think we need one set of criteria for authentication, which would be the minimum applicable to anyone. And because of that, it makes sense to me to have one recommendation to hold that one set of criteria.

And then if we determine that we need specific requirements for one type of user group that maybe doesn't apply to another, that can be here as a recommendation, but there's no need to break it

up into two. And indeed, if we do determine that we would need separate requirements for separate types of requester groups, then we might need a big number of different recommendations, which gets really confusing and unwieldy.

So, if there's any text in the original Recommendation 2 that we need, then we should certainly bring that up into the combined recommendation. But having two would mean that there's duplication in some parts, risk of missing requirements in one or the other, and confusion as to where a requester falls. So, I think that's not necessarily the best path to go down.

And sort of more broadly, we should just think about, I don't think that we are obligated to maintain the existing structure of the recommendations, which is maybe a big statement, but we should think about that. I hear the concern that there's varying tech in different places around the world. I see no reason why the requirements that we lay out cannot accommodate for that.

Okay. So, then to the most recent point, I sort of think that any group of people can decide that they want to become a Designated User Group. So, if the American Dentist Association wants to get together and work out how to meet our criteria that we lay out, then they can spin up their own DUG and they can accredit dentists and then those dentists can submit disclosure requests. And we know that they really are American dentists and that can be useful information for the responding party.

So, if they meet the requirements that we are laying out here, then we would accept the authentication which we all agree does not necessarily mean we would disclose the data. And we need some type of ongoing review to make sure that the group itself maintains adherence to those requirements, which goes back to Steve's point just now about knowing that they will be accountable. So, we're setting up the system that permits and requires that.

MARC ANDERSON Thank you, Sarah. Ashley.

ASHLEY HEINEMAN Thank you. Sorry, trying to figure out which button to unmute myself with. Yes, Ashley representing registrars. And I apologize, I feel like the conversation is bouncing around a bit and I might be stating the obvious, but I kind of feel we're still at a point where we're not speaking from the same page. So, please indulge me if we're all saying the same thing and I've misunderstood.

But in terms of authentication, what we're doing is just giving registrars like mine a better idea of who you are so I don't have to take the time to find that out on my own. So, that's what we're doing. We're saving us time. We're not giving them any other special treatment other than that. So, I think looking at what, at a high level, requirements are necessary for authentication, you need to think of it in those terms.

So, for example, knowing that the party is capable of securing the data properly, that will be helpful information for us to know. And I think depending on the group will also depend on what requirements will be helpful. Personally, from my own perspective, authenticating law enforcement, that is very clear cut and I understand what we need. It's not so clear for the other groups, quite frankly, at this stage, beyond knowing that there is a capability of being able to handle the data properly.

So, I just wanted to kind of set that tone. Hopefully, we're all at that same level of understanding of what authentication actually gets you. When it comes to LEA, I see it as you can be authenticated, but you don't have to be authenticated. But if you're not authenticated, it's probably going to take a lot longer for us to respond to your request because we will have to, as a registrar, go and find out and make sure you are who you say you are. So, anyway, sorry if I'm stating the obvious, I'll be Captain Obvious today, but just wanted to make sure we were all kind of thinking on the same wavelength. Thanks.

MARC ANDERSON Thank you, Ashley. Lawrence, is that an old hand or? Okay. Sam, please go ahead.

SAMANTHA DEMETRIOU Thanks. This is Sam again. And Ashley, thank you for being Captain Obvious. I think it bears stating. The other point I wanted to make

in regards to that is, a lot of the other questions that have come up, I think are better addressed when we talk about what information needs to go into a request that a requester makes. So, that's going to deal with a lot of the things like the legal basis for making that request. So, I think we want to just keep really focused on the fact that authentication is a pretty minor point and I think we maybe need to start moving forward on this.

MARC ANDERSON Thanks, Sam, and thanks for bringing it up a level. Yeah, we do need to focus. Ultimately, what we're trying to do is produce recommendations that get to that point and I think we've heard that there are sort of two things. What is the information we need to know about the accrediting body? Ashley gave a nice example of, do they have the capability of controlling or securing the data, for example.

And then the other question I want to get to today is, what is the information that needs to pass to the disclosing entity that would make that authentication useful? You know, I think the example we heard earlier was, what jurisdiction are you from, right? So, we ultimately need to get this to, what is the language we need to put in the policy to accomplish these things?

And I think we've been circling a little bit around what we're trying to accomplish. And what I really wanted to get to today is, not so much what we're trying to accomplish, although I guess that's an important discussion to have, but what is the policy language that

we need to develop in order to accomplish that? So, Anne, with that, over to you.

ANNE AIKMAN-SCALESE Thanks, Marc. I want to go back. Appreciate very much what Ashley said about, you know, user groups and those who are not part of user groups. I want to go back to something you said about, hey, this system is accessible to everyone, but you seem to imply that when people come in individually, including like law enforcement, that there's not an applicable authentication procedure that's governed by any of these things. And that surprises me a bit.

In other words, what Ashley said is quite true. She said, look, if you're part of this Designated User Group and there are procedures for authentication, your requests are going to be processed more easily, analyzed more easily, analyzed faster. So, if I go back, however, to the example of individual law enforcement from the global south not part of a Designated User Group, I see still a need for authentication so that those requests are not somehow slowed down.

You know, the fact that a particular law enforcement from a particular country is not part of Interpol or Europol doesn't mean that they should not be able to be authenticated. They should have an authentication [CROSSTALK].

MARC ANDERSON: Can I jump in this? As I understand it, that's way off, way out of scope. Right? Because what I'm hearing you saying is that we need to have an authentication mechanism in place for all law enforcement.

ANNE AIKMAN-SCALESE: Yes.

MARC ANDERSON: And my understanding is that that is absolutely not what we're doing and that what came out of all of our learnings so far is that that is cost prohibitive. Who would build that? Who would pay for it? We have the ODA that showed that it's cost prohibitive to go out and establish an authentication regime for everybody everywhere. Okay? So, what I understand --

ANNE AIKMAN-SCALESE: [CROSSTALK] it's not an accreditation. It's just show us your badge. That's all it is. We've talked about an NPSWG about what would be needed in addition to the email address, don't make it bigger than it is. It's not a mountain. It's, you know, are there one or two additional elements besides the email address that show that you really are law enforcement? That's all. Otherwise, you're putting all those at a disadvantage vis-a-vis how it works in the system.

MARC ANDERSON Okay. I'll just say, again, my understanding is that that is not what we've been tasked to do and my understanding is that's specifically not what we're tasked to do. So, if other people want to jump in and correct me or go in in a different direction, I'm open to that, but my understanding is that that is outside of our scope.

ANNE AIKMAN-SCALESE So, you're saying that law enforcement has to be part of a Designated User Group in order to benefit from authentication? Is that what you're saying? As a policy, that's a policy.

MARC ANDERSON Yes, that's how I understand our mandate and I'll just throw that out, does anybody understand differently? I think we're pretty clear on that one.

ANNE AIKMAN-SCALESE Okay, thanks. You know, if everybody feels that way, that's not really what's been discussed in PSWG authentication, but [CROSSTALK].

MARC ANDERSON This isn't PSWG authentication, Anne. This is SSAD system. The SSAD --

ANNE AIKMAN-SCALESE: But it asks us to work together with PSWG. So, okay, if everybody agrees on that at this table, that's fine. You know, but -- Seb, you're --

SEBASTIEN DUCOS: No, I agree with you, man because otherwise, that effort that the board asked us to work on is completely out of policy. PSWG comes with whatever they want to the table and we accept it as is. It's completely out of policy. So, maybe it's not our task, but then it would be our task to raise a finger and say, "Hey, that needs to exist in some body of policy." Right now, it's not and the board has asked us -- Sorry, I'm designating you [CROSSTALK].

MARC ANDERSON: Sorry. What's the 'that' in your statement? What is that that has to exist in policy?

SEBASTIEN DUCOS: The minimum amount of information we need to have from law enforcement in order for us to take them seriously. I'm happy to recognize that by myself in my jurisdiction, but if I am unable to recognize what I'm looking at for every other jurisdiction, and to Lawrence's point, it is absolutely going to be, well, then you're just like anybody. Then let's not even worry about authentication or anything like that. I don't need it. There aren't just a pedestrian.

MARC ANDERSON Okay. I know there's a lot of thoughts and feelings on this one. I'm going to get back to the queue and Lisa?

LISA CARTER Yes, I just wanted to go back a little bit to what Sarah was bringing up earlier regarding having a minimum requirement for all authenticated users, I just wanted to get a little clarification. Would that include law enforcement or is the thought that there'd be a minimum standard and then law enforcement has a higher standard that needs to be indicated in the policy?

SARAH WYLD I was thinking a minimum standard for anybody and then a Designated User Group could determine their own additional criteria on top of that if they want to which might be very useful for the responding party, but I was not thinking of dividing it up on our side. Minimum criteria is just minimum. Yeah.

MARC ANDERSON Does that answer your question, Lisa?

LISA CARTER I think so for now. Thank you.

MARC ANDERSON Okay. Thank you. Lawrence, you're next.

LAWRENCE OLAWALE-ROBERTS: Thank you. This is Lawrence for the records. So, my understanding of the discussion so far, first of all, to this process, urgent requests exist for law enforcement to get a fast-track attention from their side. So, that's why I think the timelines are different from urgent requests and for all other requests.

Now to the point we've been discussing over the last couple of minutes, it appears that for law enforcement from certain regions that might not be already integrated into the big security network that we are familiar with, if they are going to go through the part of any other user, they will definitely have the timelines for those users applying to them and not urgent requests. And from what we've been seeing so far, it appears that for law enforcement, for my region, for instance, they will need to kind of get integrated with the decisional user that is law enforcement. Is that understanding of mine correct?

MARC ANDERSON: So, I want to correct a couple things. The first, in our SLA discussions, we did not propose separate SLAs for authenticated users versus not authenticated users. There's a timeline for urgent requests and standard requests. So, what we have on the table is not a different timeline for authenticated users. Caitlin's reminded me that you do need to be authenticated to qualify for the urgent request timeline, though, which might be getting to your point.

To your other point, there's sort of two paths to authentication, I guess. You can join an existing group, and we know that there's a PSWG effort underway, or you could form your own group. So, I think your question was, did you understand that you have to join that effort underway in the PSWG? And I think that you do not. I think you could have your own Designated User Group and work with ICANN to establish that authentication system. I think that's the proposal that we have on the table and I'm seeing some nods around the table, so I think I'm getting that right. Does that help, Lawrence?

LAWRENCE OLAWALE-ROBERTS: Yeah, that helps clarify my understanding. Thank you.

MARC ANDERSON: Thanks. Back to the queue. Sam, please go ahead.

SAMANTHA DEMETRIOU: Thanks. This is Sam. I'm wondering if there isn't a fairly simple solution staring us in the face here of needing to incorporate the work that is being done by the PSWG. And I think maybe we can just harmonize these minimum requirements to make sure that they cover what's being done there. Not putting it at risk, those minimum requirements for other user groups, certainly, but I think we can just harmonize these two things and fold it all into one recommendation here.

MARC ANDERSON Thanks, Sam. Justine.

JUSTINE CHEW Thanks Marc, Justine speaking. I don't have any serious opposition to what's being discussed at the moment and I kind of agree with what you said. My question is, if a DUG submits whatever minimum requirements that we are talking about right now to presumably ICANN, is it ICANN's responsibility to then check whether all these submissions are valid?

MARC ANDERSON So, I maybe throw that back at you. What do you think? What language should we be putting in the policy? What minimum criteria should we be establishing there? So, I think our task is to answer that question in part.

JUSTINE CHEW Sure. We can add to the minimum requirements. That's not actually my question, right? My question is, whatever you have as your minimum requirements that needs to go to somebody so to be evaluated and determined as being proper, and then that DUG would be an accredited entity, right? My question is, who does that evaluation? Is it ICANN?

MARC ANDERSON Correct me if I'm wrong. I think the straw man language is ICANN or its designee, but again, I think that's open for discussion, right? I think where we're starting is ICANN or its designee, but if we think the answer should be different, we can propose changes. John, over to you.

JOHN MCELWAINE Thanks Marc. John McElwaine for the record. So, I agree with what Sam had to say and I think we might be at a point because of excellent work that Sarah's done and which I think is based off of a lot of, what is in the straw man proposal we have? It's just not a straw man. I might ask that we have a straw man proposal to help us wordsmith from and look at based off of what Sarah has.

And I think once we see it in writing, because that's the way we've been working, that'll probably be a much more productive discussion. And to Sam's point, we should probably also take into account that it needs to be at a high enough level that we're not going to be excluding work that's already being done on LEA access. Thanks.

MARC ANDERSON Thanks, John. Great points and I think that's a practical path forward. I know we have around 10 minutes left in the session. Well, to be honest, I've been hoping to get more to the policy language itself. I think this was an important discussion to have because it's clear that we're not all on the same page, at least at the

start of this conversation. I hope that we're closer to being on the same page now at the end of the discussion. And I think John makes a very practical suggestion that we need to have language in front of us to say yes, does this hit the mark or no. So, that's probably a very practical next step. So, thank you for that suggestion.

Lisa, your hand's up again? Yeah, sorry, just a reminder, this discussion is for members of the SRT only. So, if we're not getting to you, it's because you're not a member of the group.

We've reached the end of the queue at this point and given the time remaining, it's maybe difficult to have a full conversation about any of the other topics we want to have. So, maybe I'll just throw the floor open. Does anybody have any closing thoughts that they want to share on the discussion we've had? And in particular, since the next task will be for staff to update the straw man with proposed language that we can consider and thank you, John.

Does anybody have any thoughts on specific language that they would like to see incorporated into that straw man? So, maybe last call to get that on the record here. Anne, over to you.

ANNE AIKMAN-SCALESE Thank you. It's Anne. I appreciate what Sam said about merging the work of PSWG with this work. But I also note, I'm not sure why Manju didn't raise her hand, but she put in chat something that needs to be considered here. It says, "Probably we just need

authentication of law enforcement and we don't necessarily need Designated User Group," is the comment. I don't know if she wants to speak to that or not.

MARC ANDERSON

Thanks, Anne. And first off, apologies, I have not kept up on chat at all so I'll have to read up on that later, but Manju does have her hand up. So, over to you.

MANJU CHEN

Thank you very much. It could be part of my comments. So, yes, I've had this thought for a long time that we maybe don't need DUGs because all of the credentials you need, you provide in Recommendation 3, and then, you know, counterparties make their own decisions. But after that comment, Sarah and Ashley have very eloquently explained why DUGs can be useful for contrary parties when they're making evaluation and determination. So, I was convinced but still.

I raised my hand originally because I think we were supposed to kind of consider whether we still want to merge Recommendation 1 and 2. And because you were asking for any final thoughts for this session, so my final thoughts is probably not because I think again law enforcement agency has their special status in a way that they have the privilege to -- Well, I don't know if it's a privilege, but they have this urgent request that they, you know, are privileged too.

So, I think it is quite important that we kind of keep Recommendation 1 for just ordinary users and requirements for DUGs and second still for -- Personally, I think it's not just any government users. I will prefer it just be law enforcement because they are the only eligible to order requests, but I'm not holding a very hard line to that. So, that will be my final thoughts. I think we keep separate Recommendation 1 and 2, and 2 will specifically for, you know, government users.

Oh, and one final point is that, I really hear Anne and Lawrence's concerns about, you know, global styles. Their law enforcement may not be able to be integrated to whatever existing, Interpol or whatsoever. I mean, I think PSWG will have the capability to think of a system that is not only Interpol.

You know, law enforcement in Global South can have their own law enforcement user group, law enforcement DUG, which will enjoy the same rights or privilege or access or whatsoever as Interpol and they have the same kind of level of authentication. So, I think it can be easily resolved as that, but I mean, I welcome any criticism or feedback. Thank you.

MARC ANDERSON Thank you. Lisa, go ahead.

LISA CARTER Yes, I was just going to say, to the point, if you're going to consider keeping it separate, to have the two separate recommendations, it

might be good to define law enforcement in that case, have an official definition of that or some implementation guidance on that if it's going to be separate or even if you decide to combine it as one.

MARC ANDERSON Thank you, Lisa. We're at about the five-minute mark here and so I'll throw it open to the floor. Any other thoughts? We can have five minutes back. All right. So, just to wrap things up -- Justine.

JUSTINE CHEW Sorry, you did throw out a final invitation so I'm going to take it.

MARC ANDERSON I did. Sorry, I missed your hand. Please go ahead.

JUSTINE CHEW I'm going to take it. So, this is Justine. So, I posted something in the chat, but I just want to vocalize it here. I think 1.4.5 or whatever the next number is going to be should also have some indications about whoever who is in charge of the DUGs to declare that they are going to accept responsibility for maintaining whatever they're maintaining. So, I don't know whether that goes under terms and conditions, but I think that should be explicit somewhere.

MARC ANDERSON

Thank you, Justine. All right. So, like I said a little while ago, this maybe wasn't quite the conversation I was hoping to have, but I do hope this was a useful conversation in getting us all moving in the same direction. Because my sort of takeaway is that we did not start on the same page and as far as next steps go, you know, I told you I'd try to summarize what we agreed on.

I think what we agreed on is that our next step is to have a new straw person language that we would be able to review and see if that reflects the discussions and views of this group. So, we'll work on that, try and have new language for you to review as soon as possible. And our next steps will be to review that and consider if we need to adjust that language at all.

So, thank you, everybody, for a very lively discussion today. I was worried at the get-go that I'd have to drag comments out of people, but obviously that was not the case. So, thank you, everybody. We have two more sessions at ICANN this week, so I look forward to seeing more exciting conversations from everybody. With that, I think we can end the recording and adjourn.

[END OF TRANSCRIPTION]