ICANN83 | PF – GNSO: Registration Data Policy IRT Work Session
Tuesday, June 10, 2025 – 15:30 to 17:00 CEST

ELISA BUSETTO: Hello and welcome to meeting number three of the Registration Data Policy Implementation Review Team Urgent Request. My name is Elisa and I'm the Participation Manager for this session. Please note that this session is being recorded and is governed by the ICANN Expected Standards of Behavior and the ICANN Community Anti-Harassment Policy. If you would like to speak during this session, please raise your hand in Zoom. When called upon, virtual participants will be given the permission to unmute. On-site participants will use a physical mic to speak. Please be close to the mic. Please state your name for the record and speak at a reasonable pace. And with that, I will hand the floor over to Isabelle.

ISABELLE COLAS: Thank you, Elisa. Hi, everyone. Welcome to the Registration Data Policy Implementation Review on Urgent Requests meeting three. I hope you all are enjoying the beautiful city of Prague and get to have some time to enjoy some more later on today in this afternoon. So here's the agenda that we're going to start off today. We have a couple of new faces that were here at ICANN 83. So I want to briefly go over the role of the IRT and what we do and then the background of the Urgent Requests and the IRT scope, which is why

we're here today. And then after that, I'll go over what we discussed and what we've heard so far in our last meeting. I believe that was about a couple of weeks ago during the second meeting. And then I have a bit of a diagram to show and talk about where we stand right now as a group after we've had our two discussions around areas of alignment and divergence. And then I want to hand off the discussion to this group to talk more about considerations and I have a couple of questions for this group to move forward on that. And then if we have time, we'll have an AOB. There was a bit of a conflict, it seems like, in terms of or confusion in terms of the agenda scheduling. So some of you may have that we are here until 5:00, while some of you may have that we are here until 4:30. So we will aim for an hour, but we have this room for an additional 30 minutes if we need to have that. Next slide, please.

So as a general reminder of the role of the IRT and based on the two consensus policy implementation framework, as well as the IRT principle and guidelines, the IRT is here to serve ICANN Org as a resource and staff in terms of the background and rationale of the policy recommendations and how to implement the recommendations and help us make sure that we're implementing the recommendations in alignment with the policy recommendations. And then a general reminder that the IRT principles and guidelines that the IRT is not a form to reopen or relitigate policy discussions. There are times when there may be divergence in views, which is okay. But if we have a moment where there is no consensus in this group or there seems a large area of

divergence, then the ICANN staff and the IRT as well as the GNSO Council liaison can escalate those measures as appropriate to the GNSO Council if required, if additional guidance is needed on how we can address the divergence within the group. Next slide, please.

Now a bit more about why we're here. So we've been talking about this a lot, and I believe a few of you, this should not be new news, but as a general reminder, you know, we have, as ICANN, have been tasked with the assignment to reconvene the registration data IRT with the very limited scope of identifying appropriate timelines to request to respond to an urgent request for lawful disclosure. And this is right now in particular circumstances when the requester, particularly law enforcement, has already been authenticated. So we've received several guidance and correspondence where here we have the ICANN board shared concerns to the GNSO Council regarding the policy implementation draft language that provided in terms of the original timeline. The GNSO Council here also acknowledged the board's concerns and agreed that the policy recommendation itself should be revisited. And after a series of trilateral discussions, the GNSO Council and the ICANN board as well as GAC members have agreed that these discussions should be sent back to the IRT for defining what the timeline is within the limited scope and ideally as quickly as possible.

So there are two paths that are currently taking place. We have what we're doing here today, which is discussing the timeline of urgent requests, and then we also have an alternate path that is taking place within the PSWG, which is leading on the

authentication mechanism within itself. So we're not here to discuss what the authentication mechanism is and how it works, but specifically just the timeline within itself. We understand that in general this is a very difficult assignment trying to separate the two paths and understanding how mechanisms should be authenticated as well as how they should be received. But based on what has been shared by the board as well as direction from the GNSO Council, we're obviously only focusing on the timeline itself.

And then just a general reminder in terms of the proposal that ICANN Org has shared previously, which was an acknowledgment of the request within two hours and a response within 24 hours, we wanted to clarify that this was only a proposal and we had shared it with the IRT for consideration and continued discussion. The response itself may not necessarily contain the requested data, but just ensure that there is a response within 24 hours, which is what we shared.

So here's what we've heard so far in terms of meeting two. We have some IRT members who shared the concern that in general the authentication mechanism and the timelines is, you know, they're linked. And it's difficult for them to be artificially separated, which we fully understand and acknowledge. The authentication mechanism should be designed to expedite the support of these requests. And when I say request, I mean urgent requests. And then the mechanism on how urgent requests are submitted must also be defined prior to identifying a timeline for urgent requests and made nonpublic due to the possibility of abuse. There were some

concerns that were raised in terms of right now the registration data policy currently requires the disclosure of how you can request for this data. And if we did that with urgent requests, then, you know, that can potentially be abused. Therefore, trying to have a meaningful discussion moving forward to define the urgent request timeline and the submission of the authentication of such requests must also be considered prior to creating a timeline.

We also heard that based on some IRT feedback that there was an ask in general of the general understanding of the frequency of when we get these urgent requests, how often do they come in, and then what are the outcome of those requests? Whether they're actually urgent, do they fall under the four criteria of which we've discussed, or do they require additional background, and how are they responded to? Do registrars ask for more information, or are they able to achieve and respond to those really urgent requests as efficiently as possible? We've also heard shared concerns within the contracted parties that there's a concern in terms of liability of releasing data without proper review, so especially under certain time-sensitive circumstances. So they want to make sure that they have the opportunity to review the request to make sure that they release it properly rather than releasing it improperly. Next slide. Thank you.

Further on, we also heard more concerns, like I mentioned previously, publishing emergency contact data would lead to channel abuse and mislabeling of requests. So we acknowledge that everyone thinks that their request for data is urgent. So if we

were to require registrars to publish that contact data within the registration data policy, then more than likely it will get abused, and everyone will try to send out requests without identifying whether they're LEA or not. Authenticated urgent requests additionally do not necessarily shield registrars from legal liability. So there has been some shared ideas that because the request that is being received is authenticated, that means that legal liability should automatically be removed, which there has been disagreement with that as well. And then including a response time without considering other issues creates a resource restraint for small registrars. So there's been consideration in terms of like the differences in terms of business models, how that works out for smaller registrars versus the larger ones, how quickly can they respond to a request that is being received.

Then we heard from others that, you know, reopening fundamental questions about why we're here, why are we doing this, and, you know, do we really need this type of work is essentially counterproductive and is misaligned with the prior agreement and assignment that has been sent to the GAC and GNSO council and ICANN board to the IRT. You know, there was recognition that currently registrar practices are sufficient. Registrars, they shared that when they receive urgent requests that are really urgent, they take care of it. They respond to the request and then they also respond as swiftly as possible, oftentimes exceeding those timelines. So acknowledging that these practices are often sufficient in response time, it would be helpful if we had that in a

consensus policy. But also further acknowledging that a response time within four or five business days would render useless for actual emergency purposes, especially for issues that deal with child endangerment or life threats. So before I move on, are there any questions? Okay. Thanks. Next slide.

So lastly, I thought it would be helpful to have this diagram to kind of show I swiftly went through a bunch of slides, but to show where this group stands right now based off of discussions and where there have been areas of alignment, where there are areas of divergence. We've all agreed that urgent requests are important. And while they're rare, they are important. And they're the ones that are truly urgent for them to be addressed. Everyone here or everyone within this group and during these discussions agreed that they want to support the law enforcement agencies during life-threatening and time-sensitive situations. But in the process of doing that, we should avoid policy abuse as much as possible and then develop a secure and abuse-resistant process, but that is also practical for everyone. While these were some areas of alignment, we also had several areas of divergence with this group, which is, you know, the divergence between the response time. Some members in the IRT felt that the response time should be within seconds or minutes, while others felt that it should be within 24 hours or longer. Some members felt that we need additional data to codify a policy or a consensus policy language with an urgent request, that there's not enough data to prove that there is an actual issue in the current landscape. While there have been

discussions of ICANN Org being the central manager in terms of urgent requests before they are sent to registrars, again, I've mentioned this before, but the authenticated requests should remove the legal liability for registrars. That was also not an agreement. And then registrar authentication and urgent request submission mechanisms should be defined prior to defining a timeline, which goes against the board ask as well as direction from the GNSO Council. But there have been raised concerns in terms of the scope of the urgent request IRT discussions that continue to remain unclear. And then we've heard the idea of using the existing 24/7 contact obligations within the ICANN RRA Section 3.18.3. Since this already applies for illegal activity reports, you know, why can't that be repurposed? But we've also heard a bit of pushback, and that was unnecessary. Much traction was gained during the IRT as well.

So based on the discussion that we had in the previous IRT, in light of that I had circulated these four questions for this group to consider and to have the discussion here today. You know, we thought it would be helpful to have these discussions which aim to address the concerns and the examples raised. And then further in consideration of these concerns, a few registrar representatives as well as GAC and law enforcement representatives met to do a sort of deep dive on what the pain points are that exist within the current urgent request landscape. And I think we can definitely touch more on this as we go through these questions. But starting off with the discussion, it would be good to hear from this group

what are the average turnaround times and the factors that influence this timeframe. We've heard several times within the last IRT meeting that when we receive really urgent requests, right, or exigent requests, they are actually received and responded to and handled swiftly, sometimes exceeding the timeline. So it would be good to hear more about this and what factors actually help accelerate these response rates. Oh, go ahead, Owen.

OWEN SMIGELSKI

Hi, everyone. Excuse me. Oren Smigelski for the transcript. So I mean, I think there's a – it's going to be tough to do an average turnaround time because, first of all, I don't think that's something that we as a registrar are tracking and I don't know if others do. And also, this isn't just one central place where these types of requests come in. They can come in through the RDRS. They can come in through our abuse queue. It can come in from them calling our privacy council's mobile number directly. So the ones that go through a proper channel that we can do, we respond to very quickly. Our RDRS disclosure time is within one business day. So that's just in general requests, not even urgent ones. But I think there's going to be a wide variety of things of how registrars approach that, what their staffing levels are, what their sizes are, and you won't have like a one-size-fits-all there. Obviously, if there's something that's really urgent, generally the law enforcement, they know how to get in touch with the people who

can either make that decision or coordinate that decision and get that data to them as soon as possible.

ISABELLE COLAS Thank you, Owen. Anyone else? Sorry. Are there particular factors that influence that besides what you said?

OWEN SMIGELSKI Obviously, which law enforcement are we talking about? Can we confirm that they're law enforcement? There was actually a RDRS request we had within the past year where it was law enforcement. Again, it wasn't an urgent request, but we didn't realize it was law— Some people claim to be law enforcement, but a lot of people claim to be law enforcement in that system. But they were using an Org address, nothing against Org, as Beth is sitting next to me here, but my team didn't realize that that was actually a county or a city in the state of California. Their Org address was for all of the city government, including the police department. So that was just one thing we maybe needed some additional information. That's why I think having that type of authentication in there would really make it a lot easier, because that way you know that this is a verified law enforcement. There's also jurisdictional concerns and things like that as well, too. But having that ability to have that gating just so that we confirm, yes, there's law enforcement, and I discovered this when I was going back and looking at the RDRS request. I'm like, oh, law enforcement. And I looked and was able to figure out that actually was a legitimate law enforcement request. And it would be

much better that we don't have to waste time on those kind of things as opposed to knowing upfront that, yes, this is a legitimate request.

ISABELLE COLAS: Great. Thank you. Making sure there's no more hands raised. Okay. Great. Then, oh, go ahead, Roger.

ROGER CARNEY: Thank you. This is Roger. Yeah, I think, you know, looking at all these, one of the things I actually have our disclosure team researching, the number of urgent requests that they've received. And they have been spending weeks now looking to see how many. So, and again, we do track quite a few types of requests that come in. But with urgent requests being so limited and over a year's time not receiving them, we don't track that because the metrics doesn't really matter a lot when you get one every four years or so. So, I think that, and again, they're still looking and they're going to pull examples of when they did get it. So, hopefully we can supply that back to this group. But I think, you know, one of the things on this slide maybe we need to be careful on is to respond to. I think we have to be more precise there because, as we discussed in the IRT, the current contractual obligations are to respond. It's to acknowledge. But we're not looking for that here. We're looking for it to respond with a decision. So I think that we have to be careful when we say respond, because everybody has responders set up that will respond and say, yes, we received it. But what we're

talking about here for urgent is something that's actionable, either a disclosure or a denial. So thanks.

ISABELLE COLAS: Yeah, that was good points. Thank you for that, Roger. Always. Yeah. Reg and then Beth.

REG LEVY: Thank you. Reg Levy from Tucows. I want to echo a bit of what both Roger and Owen said. We don't track this, so I can't answer the top one. And it happens very rarely. That said, typically we work directly with the provider with regard to exactly their situation. So there was an issue during the Christchurch massacre where a New Zealand, which is not any of my jurisdictions, law enforcement officer contacted me to get a video taken offline. The registration data is not what he wanted. He thought that was what he wanted, and that's what he was asking for. But I worked with him to get him the information that he needed to be able to take that stuff offline. So because it's rare and because we can work in such a bespoke manner, it's not really a question that makes sense in this context. We've received a couple things through RDRS that said that they were from law enforcement and said that they were urgent. And to the extent that we were able, like, we didn't ask, right, if it's that urgent, we're not going to be like, show me the money. We assumed that those were urgent. But my assumption is that they weren't, because, again, we've received probably twice the number through that mechanism in the last six months than we have in the

last eight years that I've worked for Tucows. So it is vanishingly rare, and we always work with the law enforcement officer directly, which is why I'm not certain. I know that previously it said we're not supposed to ask why we're here, but I'm not certain why we're here. I'm not certain what we're trying to solve for and where the gap is so that we can, and knowing where that gap is, is going to help us better define the timeline. Because if there are instances where local law enforcement investigating CSAM, investigating I had a child abduction issue that I dealt with, are not able to contact the registrar, then sure, great, let's hear about them. But again, even in those cases where I've worked with law enforcement, it was never the registration data that they wanted. That's what they asked for, but when we worked with them, we got them the information that they actually needed.

ISABELLE COLAS Thanks, Reg. That was really helpful. Beth, go ahead.

BETH BACON Thank you. I got in the Zoom room. I followed the rules. I'm sorry. I finally nailed it. I'll start with my intervention with an apology that I am catching back up. I had conflicts and I wasn't able to join this group for a little bit. Maybe just for my context, and again, I apologize, my understanding is that this question is to establish kind of just a shared scope of the volume of this issue and what we would be seeing coming in, not necessarily using this for anything that's going to be a big issue. Anyone like to respond? another, you

know, what we would, whoever is looking this up, would be, am I looking for responses that would fit the definition of an urgent request as we have established in the draft language? Because that doesn't exist right now. If you say, like, how many urgent requests have you had? I don't have those. I get, I have frantic ones. So if that's how, I just, clarifying for that so that we can, I can provide you, perhaps a little late with, like, something more constructive, but it's helpful.

ISABELLE COLAS

Yeah, good questions. And yes, I know we removed the criteria for urgent requests with, because it was combined with the timeline, but yes, we're looking for requests that fit within those four bullet points in terms of what an urgent request is and what we agreed in as an IRT. Owen, go ahead.

OWEN SMIGELSKI

As we were sitting here talking and mentioned RDRS, I realized that we actually, Namecheap did a pretty good tracker for our RDRS requests, and I was able to check while on this call, and we have received since the beginning 814 RDRS requests. 23 were self-identified as urgent requests. That's 2.8%. Of all of those, one was an urgent request. All the others we downgraded, and that was one where there was a ransomware, the 24-hour turnaround, or they're, you know, they pay $5 million or whatever. All the other stuff is, most people think their problem is urgent, and so they selected that. And so I think one of the things we need to make sure is that

it's just whatever solution we do going forward is not something that's open subject to abuse, because if you've got registrars that need to respond to, you know, one of them was, I want to contact the domain name in order to buy the domain name. That is not an urgent request. And just make sure that we have a good gating process to make sure that the urgent requests really are urgent requests, because when everything is urgent, then nothing is urgent.

ISABELLE COLAS Perfect. Thank you. Thank you. Those were really good points. Anyone else before I go on to question two?

OWEN FLETCHER Hi. This is Owen Fletcher from NTIA. Actually, I guess we're going through the questions in order. I'll wait.

ISABELLE COLAS Did you want to add to question number two? We can go into it if that's what you want. Not yet. Anyone else? Okay. In that case, then I'll go ahead and go into question two. So for our law enforcement friends and GAC members here, it would be interesting to know, I know just in general, what are the problems and gaps that currently exist with the current landscape? We've heard from our registrar friends that it would also be helpful just to have a general understanding. So go ahead, Gabe.

GABRIEL ANDREWS Hi. Gabriel Andrews, for the record, and co-chair of the Public Safety Working Group. When I was preparing for this question, I guess I could have clarified and failed to, but when you say the current approach, do you mean just sort of like the status quo of today versus the current approach as suggested by ICANN with the 24-2?

ISABELLE COLAS Yes. Current approach and sort of, I mean, like status quo.

GABRIEL ANDREWS So, all right. So the registrars have accurately said that oftentimes law enforcement do know the right points to reach out to at registrars, but often is not all. And so one of the points I've raised is there's a desire to sort of create a systemic mechanism that involves more than already knowing and, or maybe using John Crain's cell phone to figure out if you don't know, right? Because John Crain's cell phone doesn't scale, or at least he's told me. It's worked so far. But the thought being that even if, you know, there's a handful of law enforcement officers that even know what ICANN is and know those folks, but it'd be great if we had a mechanism by which any law enforcement officer could make the request in a reasonable amount of time and solve all of that decision-making process before it needs to happen in real time, like at the actual bad urgent event. And so that's sort of the goal there. There's a number

of gaps that exist right now in terms, I guess, I'm sort of moving on to the other topic of like, you know, the proposal of the 24 plus 2. I think that we have gaps in sort of understanding the degree to which we are already agreed upon some of the issues in this room. But I, since I have the mic, I'm going to kind of jump topics to that, but Owen was just talking, Owen S. of Namecheap, was just talking about clarifying when urgent requests actually are urgent. And I think that we sort of have clarity that when law enforcement, in an authenticated fashion where you know you're talking to law enforcement, is attesting to which of the four categories of urgent requests that they're making, that we sort of have agreement that that justifies urgent requests, regardless of whether or not they're actually in your jurisdiction, though we do note that you might choose to incorporate their location and their jurisdiction in your disclosure determination, right? But I think we have agreement that as long as the officer is known to you to be an officer or investigator, etc., employee of a public safety agency, and that they are telling you which of those four categories, then that is sufficient to call it that, right?

ISABELLE COLAS Thanks, Gabe. I have Roger and then Sarah in the queue.

ROGER CARNEY Thank you. Maybe back to Gabe a little here. I know that this group has talked about potential contact list for registrars. Do you think, and I know this group has been reluctant to go down that path too

far, but do you think, Gabe, this could be included in the LEA authentication project?

GABRIEL ANDREWS

Oh gosh, that's hard to answer at present. So to give a little bit of background, so just to make clear what the law enforcement authentication is trying to do right now, we're trying to identify existing mechanisms that law enforcement already has available to it to authenticate their employees, their officers, their investigators, etc. We're envisioning that we could use portals that either exist now or soon we hope will exist at large entities like Interpol and FBI in the states for approximately 18,000 state, local, federal, tribal agencies that are already connected to us, and then pass that authentication to ICANN. The issue I think that we're going to run up into is that that is a good mechanism, it's far better than what we have now, but I don't want to presuppose, given the status of the RDS right now and the uncertain future of the asset, I don't want the policy to presuppose that RDS will exist exactly as it is now in the future, and so I would suggest that when we talk about the state of authenticated, we sort of be a little bit agnostic in terms of how they're authenticated. For example, I might be authenticated to Sarah over to my right or over to my left because they know me, and that's probably sufficient too.

ROGER CARNEY

Just to follow up, I think that in one of our LEA authentication meetings, I brought that simple fact up as well, that I think the

process that comes out of that doesn't have to be associated with honestly any current policy and definitely not any current system, so I think that we can use that no matter where it goes or however these things go, but I also think that we can come up with this contact list in the same vein and keep it that way as well, so thanks.

ISABELLE COLAS Perfect, thank you. Sarah.

SARAH WYLD Thank you. Hi, this is Sarah. I heard something from Gabriel that concerned me a little bit, and so I need to say I don't think that it's appropriate, as was suggested, to ignore jurisdiction when one of these cases comes. I do think it really still depends on the specific situation at hand. For example, the consideration of what constitutes threat to life can be different. The law enforcement request for disclosure of data relating to a domain that is an LGBT website, they might say it's a threat to life, and the actual threat might be to the domain owner after their data is disclosed, right? So we cannot assume or expect or require registrars to ignore jurisdiction, just as we also must not allow or expect the registrar to ignore due process where due process is appropriate. Thank you.

GABRIEL ANDREWS Yeah, I appreciate the comment Sarah made, and I just want to clarify because I think maybe something was lost in

communication, but what I was suggesting is that the jurisdiction, the location of law enforcement absolutely can be part of the registrar's balancing test and consideration as to whether or not to disclose data, but what we're not anticipating is that a request is any more or less urgent when it's made, and as long as it's attested to by law enforcement that you know it is, you know, it doesn't matter whether it's from the U.S. or from Canada in terms of whether or not it is an urgent request, although you might take into account that when you choose to say no to me or yes to Canada. Is that clarifying?

SARAH WYLD Thank you, this is Sarah. So I'm hearing jurisdiction as part of the balancing test or the review, but not particularly part of the definition of urgent itself

ISABELLE COLAS Thank you, Sarah and Gabe. Go ahead, Reg.

REG LEVY Thanks. Gabe, I don't want you to feel piled on, but you were the one who answered this question. The question says what are the problems that you're seeing, and the answers that I heard were you don't know who to contact, which is not a timing issue, and the extension of jurisdiction, which is also not a timing issue. So are there gaps that we're trying to solve for you in terms of timing?

GABRIEL ANDREWS

Well, me personally, unfortunately I'm not gonna be able to speak for all law enforcement globally ever. Yeah, PSWG, there are instances where we've made requests and it's taken significantly longer to get answers than we had hoped. It's hard to speak with, for the same reasons that I think other registrars have mentioned before, it's hard to speak with any sort of real certainty in terms of statistics on this. There's only anecdotes that I'm familiar with. I think there is absolutely an awareness that when there is a threat to life, for example, or ransomware and critical infrastructure potentially impacted by ransomware, there's recognition that there has to be essentially response without undue delay, right? And so that's the issue that I think we want to just see enshrined. I don't want to say that my anecdotal experiences, however, are the sum of all law enforcement experiences. I'm just not in a position where I'm capable of saying that.

GEMMA CAROLILLO

Thank you. This is Gemma from the European Commission. No, no, but please, if you want to respond, go ahead and then I will intervene.

REG LEVY

Well, I was just gonna say if there are other people from PSWG who do have an answer, that would be great to hear.

LUC SEUFER

Just, yeah, I'm really sorry. Luke from EuroDNS. And just to ask, Gabe, you were talking about disclosure here or action, because we already have that in the RAA, that we need to take action, like mitigate, suspend, when, and in an urgent manner when we are talking about LAA, because it was not clear to me.

GABRIEL ANDREWS

Yeah, I'll give you an example. Just disclosure, but yes. So on the topic of ransomware, because it was brought up, I was recently speaking with David Stern, who heads the Pre-Ransomware Notification Initiative at CISA. CISA is a sister agency in the United States that covers critical infrastructure protection. They run an initiative whereby they're sometimes notified that a bad guy is just now getting pinged by a new victim, and they know that what's going to follow that, based off historical precedent, is that victim in the next 24 hours, 48 hours maybe, is going to have ransomware dropped on their networks, and they're gonna have a very bad, no good day. And what we need there, frankly, is an ability to convert internet identifiers into conversations in order to prevent harm, right? These are very much examples of where this sort of disclosure of data absolutely can and will enable conversations to occur to prevent harm. I'm not sure how many of those times it's going to be ransomware that's actively targeting critical infrastructure versus not, but he has told me that during his ongoing initiative, they have made notifications across all 16

categories of critical infrastructure as categorized in the U.S. I couldn't name them off the top of my head for you, but it occurs. So that's just one anecdote that I'm able to bring to mind right now, but I'll tell you there is need for this to be responded to swiftly. I just, again, I don't want to suggest that I am capable of providing all the needs that exist in the world, because I don't believe that any officer has that full and complete visibility, and I am all the time being surprised by new circumstances.

GEMMA CAROLILLO

Now, I just wanted to comment on what is the issue regarding the timing. I think it's been identified a policy gap, so the lack of an existing policy regarding the timing to handle urgent requests. So considering the categories of requests that are defined under these urgent request labels, so which qualify as especially critical circumstances, the lack of a policy itself is a problem, and I think it's very reassuring both to hear that there are currently a lot of good practices that can be leveraged in order to address these urgent requests, and also I want to recall what was recapped by the chair at the beginning of the meeting, that there is, I think, broad consensus, including from the GAC, that we definitely want to avoid abuse of this tool. And one of the means is that these requests have been really narrowly defined, and it cannot be, I heard in previous IRT meetings, weaponized. I mean, this we need to avoid at all costs. But the fact that there is a policy gap, this is the reason why we're here again.

THOMAS RICKERT

Thank you so much. As far as question two is concerned, for LEAs submitting urgent requests, I mean, nothing prevents them from submitting requests and taking them urgent. The real question is, how can we ensure disclosure? Or what does it take to allow for disclosure? And I guess what we do need is a more nuanced approach. And I'm not sure whether that's something that we can actually write into the policy, because it might be overwhelming for the policy. But if you have law enforcement asking for data from domestic contracted parties, that's a totally different thing than doing things between countries where mutual assistance agreements exist versus between countries where nothing of that nature is in existence. So I think that probably what we need to do is put down different scenarios. And I think it's relatively easy to define shorter periods of time when it comes to domestic disclosures, but then work from there and allow for more time if additional legal safeguards need to be tested. Because I think that one of the areas of disagreement that you specified on the slide at the very beginning, that some in this team think that if you receive a request from an authenticated law enforcement authority that you're exempt from liability, that's not an area of disagreement. That's just legal la-la land. It just doesn't work that way. And so I think we can remove that. So we always have to see the combination of who is authorized to send urgent requests, i.e., are you a law enforcement authority or not? And then a second layer of tests needs to take place absent other legal basis for that, by which

you check whether the request is duly substantiated and allows for the contracted party to disclose.

ISABELLE COLAS: Thank you, Thomas. Did you want to answer to that, Gabe? Okay, go ahead.

GABRIEL ANDREWS: Hi, this is Gabriel Andrews, just partially responding to Thomas. I want to tweak a little of what you said. I don't think that we're asking for disclosure to occur within 24 hours. We're asking for a disclosure decision to be made within 24 hours. And that decision might be go pound sand, right? That isn't something that could happen. But I don't think that there's any reason to say that it couldn't be done swiftly. A swift no is still useful sometimes. I will say that if you tell me based off of my jurisdiction that's the reason for the no, if you tell me that swiftly and tell me what jurisdiction you might be only exempt from, that's still helpful to me, even if it's not what I ideally would have wanted. So swift responses are always better for situations such as this.

THOMAS RICKERT: Gabe, I appreciate that. I actually meant it when I said that we want disclosure, right? Because I think that in cases where it's legally feasible, it's desirable in these cases of urgency that disclosure can actually take place. And I think that the policy, whatever language we come up with, since this is a policy that is globally applicable,

we should not give the impression to anyone or raise expectations that you get disclosure within that period of time. But there might be instances in which disclosure actually can take place, given the correct legal parameters between the two parties involved. And I think that more work needs to be done on that. But I do agree, and I think that we've discussed the mechanism of an initial response by the contracted party sometime earlier in the IRT to say that you need to be responsive, i.e. within, let's say, 24 hours, you need to come up with a response. And that response can include either a no, or it can say we're on it, but we haven't completed our legal checks. And then you get an additional period of time to complete the assessment. Because I think that for the requestor, the worst thing that can happen is no response whatsoever. But if they know that they can expect either a disclosure decision or refusal after getting an initial response, then that's something that they can work with and bake into their planning.

ISABELLE COLAS Thank you, Thomas. Sarah, and then Reg.

SARAH WYLD Thank you. This is Sarah. There was a very specific question a few minutes ago about timing and what timing problems are there. Where are the timing gaps? The answer I heard was that there is a policy gap and that we have not completed implementation of the policy recommendation. And that is not the same thing. So we can have a conversation about whether the policy recommendation

requires further implementation. And I know it might not be everybody's opinion, but I think we have actually already fulfilled it. Because the recommendation 18 says a separate timeline will be considered. And boy, have we considered. And still, I haven't seen a lot of real data and hardly any anecdotes about situations falling into the definition of urgent that we do all agree with, where the registration data would actually make a difference in resolving it, and where the timing is the problem. So I do think we should go back to looking for specifics in order to be able to address them constructively, and focus on the timing and not, yeah, thank you.

ISABELLE COLAS Thank you, Sarah. And Reg took a hand down. Great.

REG LEVY Go ahead. Reg Levy from Two Cows. Kind of the same point as Sarah's, which is why I took my hand down. But the question does say, what are the gaps? And what I heard Gemma say was, we said there was a gap, so there is a gap. And I'm not hearing a lot of examples where registration data was not, could not be disclosed within the timeframes that we are considering, whatever they are. And therefore, there needs to be policy to solve that. So, and in the example that Gabe gave with the botnet, you don't want the registration data, you want suspension. So again, where are the situations where registration data is both necessary and lacking?

And I'm just not hearing it, and maybe I need to go back and listen to prior recordings. But I'm not hearing it from anyone here.

ISABELLE COLAS: Gabriel, go ahead.

GABRIEL ANDREWS: Yeah, I'll expand on the anecdote. Maybe I did a poor job of explaining it. But no, we're, and this anecdote with CISA, in particular, the pre-ransomware alerts that they're doing, it's an attempt to notify victims that they're about to have ransomware dropped on their systems. And it is an initiative that in 2023, they notified, I'm looking at a slide now, so I have these numbers in front of me, but they notified more than 1,200 victims in 2023, and that number doubled in 2024 to more than 2,400. They would have been able to do a lot more if they had swifter access to contact data, is what it was told to me. But this is, just to explain, this is absolutely an attempt to get contact data for the victim. So you see internet-based identifiers as your trigger. You don't immediately know who that actually is. You might be able to do some sort of public queries to identify where in the world they are, right? But you're trying to convert those internet identifiers into conversations. And one of the ways that that was doable, it might not be the only way, but one of the ways that that was doable was using the WHOIS records associated with those internet identifiers and using the abuse and telephone numbers. And I will go one step further and just note the extent it's helpful. Contact information to include telephone

numbers is superbly useful in situations like this where you suspect there's a compromise of victim networks because you can't trust using electronic communication. You can't write to them because that might tip off the bad guy if the network's actually compromised and then they take action even faster. So the ability to locate things like names and telephone numbers to reach out to are superbly useful to conduct victim notifications in circumstances like these. And at least as told to me by CISA, they saved more than $8.7 billion in value of preventing ransomware attacks in 2024. These attacks continue in 2025 and they're still trying to do their job, but they could do their job a heck of a lot better if they had easier access to contact information and that's the key point that was made to me by my counterpart.

ISABELLE COLAS Thank you, Gabe. It seems like Reg wants to respond to that.

REG LEVY Thanks, Reg Levy, Tucows. Thank you very much, Gabe. I do appreciate that there is at least one example out there.

ISABELLE COLAS Okay, thank you, everyone. Is there anyone else before I go on? Okay, great. Thank you, everyone, for the discussion so far. It seems like roughly questions three and four are kind of tied, but given the discussion so far, what additional safeguards are needed to confidently commit to a response to urgent requests from an

authenticated law enforcement agency within 24 hours? Noting that what we've discussed as well, that a response doesn't necessarily mean that the data is disclosed but that there's a response or decision as Roger mentioned.

REG LEVY

I'm going to respond to part of the question. What I need to confidently respond to an urgent request is jurisdiction. And I need to know the information about the case. So just saying this is urgent, that doesn't actually help me. I would like to know also why it is urgent but not exigent. Because if it is exigent, then there's a different set of requirements that they need to, that the law enforcement officer has to commit to. And I would like there to be due process in place. Due process adequate to the location of the relevant law enforcement officer's jurisdiction. I continue to maintain the right to decline to respond to non-local law enforcement. But the due process piece is necessary even if it is local law enforcement. Because just because the FBI comes to my door doesn't mean I have to let them in.

ISABELLE COLAS

Thank you, Reg. Can you give a bit more of an explanation in terms of what's the difference between urgent and exigent?

REG LEVY

Sure. Law enforcement officers have duties with regard to due process when there is an exigent situation. So if someone gets shot

and runs into a house, that is an exigent circumstance, they can run into that house after them. They don't need to stop and get a warrant. But they can't run into the house next door. And there are magistrates on call at all times to get a warrant quickly. Exigent means it's so urgent that we can't even take the time to prove to a judge who is on call that we need this data. So I want to know why I have to accept the law enforcement officer's judgment in a circumstance where they did not feel the need to give that judgment to a judge or a magistrate. Typically in exigent situations where the exigency is not necessarily running into a house but more of the data situation, we get the warrant after the fact. But in this case, because there's no information with regard to due process, they can just say, yo, it's urgent, and I now have a contractual duty and my license to sell domain names is on the line if I say no or if I say come back with a warrant because they have made the determination that in this case due process simply does not apply.

ISABELLE COLAS

Thank you for that. And forgive me for my ignorance here, but would an exigent case – well, let me rephrase it – the criteria that we have under urgent requests, so imminent threat to life, seriously bodily injury, critical infrastructure, and child exploitation, would those fit under what you would consider as exigent case?

REG LEVY

I would say there's probably a broad Venn diagram and that in almost every case, if it is urgent, it is probably also exigent, and I should be able to expect to receive a warrant within 48 hours after I provide the data because that's what exigent means, that they still have to go get that warrant. They just give it after the fact. But in this case, again, because there's no mention of due process – and I'm speaking from a North American perspective, so this is how exigency works in Canada, this is how exigency works in the United States. And I have dealt with law enforcement in Germany, and they have a different set of rules in terms of when and how I can respond to them and that kind of thing. But they have rules, and that's what due process is, is the rules that law enforcement has to follow. And what I see right here is ICANN policy undermining due process.

ISABELLE COLAS

Thank you. Go ahead, Gabriel.

GABRIEL ANDREWS

Hi. So Gabriel Andrews again. Yeah, there's a little bit to tease out there. There's going to be differences between one nation's laws on exigent circumstances and what has to occur versus another. There are laws in the U.S. that I'm familiar with that allow for voluntary disclosure of data in emergency situations. I'm not immediately able to recall any requirement to follow up with legal process, but we very often do as a matter of practice. And maybe Reg can, after the fact, point me to what legislation she's thinking of too. That's sort of beside the point. I guess the key point is, however, that we're

talking in this case about registration data that was previously public. And the reason why this data is no longer public is because there's been changes in privacy law in places like the EU. And there's also within those same legislation the considerations for public interest access to that data, right? And so really we're talking about the balancing test that's referred to there. And there's an expectation that the due process is the consideration that's being made by the registrar as to whether or not the right of the public interest does or does not outweigh the otherwise reasonable expectation of privacy that the registrant would have. And I would articulate that that is a form of due process. At least that's my opinion.

ISABELLE COLAS Thank you. Reg, and then Beth.

REG LEVY Thanks. I want to tease out a thing that Gabe said about voluntary disclosure. Yes, absolutely. If the FBI comes to my door, I can let them in. But I do not have to. I can say, come back with a warrant. That's the voluntary disclosure. And I have the same right as a custodian of business records to say, yes, I could give you anything that is private to Tucows. Can make that decision. That's a voluntary disclosure. But I don't have to. I have the right to say, come back with a warrant. And this removes the voluntary nature of that.

GABRIEL ANDREWS

I'm sorry. I guess I was just knee-jerking. This is Gabriel again. So I don't know in what way this does remove your right to say no or to come back. I guess I'm not saying that that's not true. I'm failing to see it. Because I thought we were talking about you have to make the decision, but the decision could still be no. Or the decision could still be no but X.

REG LEVY

Yes. So on the one hand, it creates the expectation that we don't need to ask for due process. Because again, we're not talking about it at all. This is ICANN policy. If law enforcement comes to you, you have to make a decision. Yes, the decision can be no. In the case when the decision can be no, then it becomes ICANN compliance's decision. Because they are going to look at this and say, local law enforcement came to you, said that it was urgent, but they didn't say that it was exigent, and you said come back with a warrant. How dare you? This falls under urgent. Why did you determine that you were not going to provide the data? So there's the expectation here that we're going to follow ICANN policy above our local due process requirements. And probably, because that's my contract to do business. That's at risk.

ISABELLE COLAS

Sorry, Gemma. I know you want to respond to Reg, but Beth was in queue for us to meet. Okay. Go ahead, Beth. Yeah. Go ahead. Okay. Go ahead, Gemma.

GEMMA CAROLILLO

Thank you. First of all, I would like to recall that ICANN policies do not supersede laws. It's on the other way around. So this is a very important point. I don't think under any circumstances ICANN policies that violate laws can take precedence. And I think it's also not correct at all to say that this process or any other policy or any other process under the registration data policy, which is not out, was trying to supersede law. Actually, it's even a requirement at the very beginning of the overall registration data policy that laws supersede policy.

Secondly, considering that, of course, we are here talking about decision of disclosures made in lawful circumstances, we do not seem to think that due process is abolished in any way. On the contrary. And the other point is that since it seems clear from what was said at the beginning and in previous meetings, that usually response to this very rare type of requests take place well below the 24 hours. Can we get to understand what are the cases where more than 24 hours were needed? Because we heard a lot about anecdotes from law enforcement. It would be useful to know what were the cases where urgent requests were addressed, I don't know, in like three, four, five days and what were the reasons. This would also help understand the blocking factors. Thank you.

ISABELLE COLAS Thank you, Gemma. Go ahead, Beth, and then I have Amanda then Sarah.

BETH BACON Thank you guys very much. So I think maybe if we're considering three and four as we discuss this, we understand that this process, not all things, nothing is going to say this will work 100% of the time. I think we all understand that. But in the context of three, we can say these are the things that make a good request and really will up the possibility of that. And I think Reg nailed that list on the head. You need to know who the requester is. We need to understand that there has been due process. These are all out of guidance we've gotten under GDPR requests for law enforcement. So simply those things. And I think we understand and agree that 100% is not a number we're going to hit, but it will be 100% response, maybe not a disclosure. But those are the things that I think are important to get out of this conversation. Those are things that make a good response that you could then confidently commit to respond to an urgent request.

But when you get to more of the discussion, I think it's in the context of four. I think Reg has identified something that you could keep in context and say, you know what, this might be a thing that would keep me from responding in 24 hours because I might go back and say, hey, I have some questions. And that's okay as long as we consider that, and I think that as long as that is very clear,

again, in the language. Per the thoughts about compliance, I think I imagine I can stance on that will be exactly the same as with the general requests for registration data under the registration data policy, which is they will ensure that you follow the SLA or SLT in this case. You did the process. They will not dispute the decision made by the operator because, again, that's based upon your jurisdiction. It's based upon your requirements as well as your needs and what you have with regards to data. So I think that we are getting a little bit in the weeds of, like, what's urgent? Maybe I think the acknowledgment is there are different things to consider under question four that might say, this is going to take longer than 24 hours. We understand that it's urgent, but we're responding to you to say, yikes, we might need more help. We might need more information, and that's okay. But under three, I think that Reg sure nailed it when she said the list of items that should populate a good request. So I just wanted to kind of try and, like, put that in a little bit of context because I think this group, we go down rabbit holes really hard because it's important and we care and we want to get it right. So I appreciate everyone indulging me as I frame that.

ISABELLE COLAS Thank you, Beth. Amanda.

AMANDA ROSE Hi, Amanda Rose with ICANN Contractual Compliance, and, Beth, you are correct. That is exactly what I was chiming in to say, which is that in response to one of the comments earlier that ICANN will

be coming after the disclosure decision and trying to force an outcome, that is not what our role is, both under what will be the registration data policy and under the interim registration data policy that applies right now. So we are looking to enforce the requirements that exist, and that is not our position to make the disclosure determination on behalf of the contracted party. We also make that clear in all of our compliance cases, both in response to registrars as well as the complainants. Thanks.

ISABELLE COLAS Thank you, Amanda. Sarah and then Owen Fletcher.

SARAH WYLD Thank you. This is Sarah. Gemma asked a question about specific reasons why more than 24 hours might be needed. I like that question. That's useful to talk about. I hope I can help with some information. I have three ideas. One is some registrars, even though they are fully staffed with many people, do not employ full-time a lawyer who is able to make a data processing disclosure decision of this nature, and so they may need to engage an external legal counsel who, it just so happens, does not work on Sundays or is not available on a particular local holiday. So that might extend the period to a day or a business day instead of 24 hours. Second reason, perhaps, they do have an internal lawyer, and that person is flying to Mumbai for the ICANN conference, and they will look at it when they get there. But it's a 20-hour travel process, and they can't make that decision in the airport, so they have to wait until

they get there, and that takes, instead of 24 hours, maybe 36. Third possible reason, the request comes in, and it's from an authenticated law enforcement, and they're in the right jurisdiction, but there's not quite enough information to be sure or clear that it meets the definition or that the disclosure of the data will help with resolving the issue. And instead, maybe they need something else, so that conversation needs to happen. And as they're waiting for the information to come in or having that interaction, maybe it takes more than 24 hours. I hope that helps. Thank you.

ISABELLE COLAS Thank you, Sarah. Did you want to answer to that, Gemma? No. No? Okay. Go ahead, Fletcher.

OWEN FLETCHER Thanks. This is Owen Fletcher. Reg, you identified this concern that when compliance is enforcing any contractual requirement, they may question whether you were giving a legitimate response by saying no and asking for a warrant. Is there a solution to this concern? Could perhaps there be something about the way this is implemented that makes clear that you're allowed to do that and you won't get in trouble with compliance for it? I'm interested in solving problems instead of just identifying them. Thanks.

REG LEVY

Reg Levy from Tucows. Thank you, Owen. Yes, absolutely. We can say subject to due process right in the policy. That's part of what we need in terms of, and again, not necessarily making sure that it's going to happen within 24 hours, but that it is going to happen at all, because if I don't have that information and potentially even have the due process, then it's going to be like I can't make the determination. In the case that I spoke of earlier with regard to New Zealand law enforcement, there's no due process they can give me. There's no due process that they can reasonably give me. So in that case, absolutely, I voluntarily waived it, and that remains my right to do, but I also could have stood and said, you know what, I'm real sorry that your people are dying, but I'm American and I don't care. That's callous, but it is legal. So, yeah, if we talk about due process in the policy, that would give me way more comfort.

ISABELLE COLAS

Perfect. Thank you. Roger, go ahead.

ROGER CARNEY

Thanks. Gabe, I think you said something about, maybe it was in chat, maybe you didn't say it, about loving the idea of the back-and-forth conversation when an urgent request comes in. So is that a possible time trigger is when you are actively discussing it, then the 24 hours is no longer the goal. It's when you guys decide that you're done. And, again, it's a little tricky there, I know, but I'm just trying to look for a middle ground of if both sides are actively working this, doesn't that basically eliminate the need for a time

frame because it's either going to be done, it's going to be done as efficiently as possible is what I'm assuming. So just something to think about.

GABRIEL ANDREWS

This is Gabe responding just because it was a question to me. I think I need to chew on that a little, Roger. I will say that just as a general principle, though, it is always great when you submit something to a company and they call you back. That is, yes, definitely a good thing to do. And in chat, just to your point, there was a little bit of topic on this about the conversation. And if and when a registrar does try to reach out for clarifying information and maybe the requester is nonresponsive, that might adversely impact their disclosure determination, right? I think that is, personally speaking, I think that's reasonable. I don't know. I need to chew on the notion, though, of like how clocks are started and stopped based off the conversation because I just that's a new idea to me here. But it's a reasonable path to explore, I think, in follow-up conversations, put it that way. Thank you.

ISABELLE COLAS

Anyone else? No, it does not seem so. Okay. So thank you, everyone, so far for the lively and very helpful discussion. I think we've been able to run through all these questions with a lot of insight. Based on what I'm hearing so far, it seems like a task for myself and as well as the rest of ICANN Org is to potentially draft some draft language based on everything that we're hearing and

then circulate it with the IRT for further discussion to see if we can start getting an agreement or at least get closer to an alignment on how we can potentially add a response time that includes some of these critical points that we've discussed as well as potential pathways for continued discussion between the requester and the authenticated LEA. And then seeing that we have maybe a little less than 15 or a little bit above 15 minutes, I'll leave the floor open for any additional questions, AOB. Go ahead, Gemma.

GEMMA CAROLILLO Hi, just a question on process. Do we have a timeline ourselves to establish a timeline?

ISABELLE COLAS You mean for this group? Yes, good question. So definitely the intent was not for us to have the discussions forever, right? So when we initially reconvened this group, I had said that we were going to have about three or four meetings. Today's meeting three. So ideally, not many more. There's not a specific timeline that we have in mind, but I think the next goal is, you know, to draft the language and see how I can get the IRT to agree on that. And the sooner we can get agreement on that, the sooner we can hopefully close this discussion. But no particular timeline at the moment, but not forever, that's for sure. Thank you. Anyone else? Reg, go ahead.

REG LEVY: Thank you. Reg Levy from Tucows. Can you go back one slide? Because I actually want to read what that question that we didn't answer was.

ISABELLE COLAS: It means like question four? Yeah, it's, I think we discussed it in question three, so thank you. Yeah, sure. And I can also offer if you have any other suggestions, you know where to find me. Feel free to reach out. And other than that, I will give you guys about 15 minutes. A break early. Thank you, everyone.

[END OF TRANSCRIPTION]