

---

SAN JUAN – ICANN GDD: Privacy & Proxy Implementation Review Team  
Sunday, March 11, 2018 – 18:30 to 19:30 AST  
ICANN61 | San Juan, Puerto Rico

UNIDENTIFIED FEMALE: ...ICANN staff. We'll get started in a couple minutes. This is the Privacy and Proxy IRT meeting.

JENNIFER GORE: Hello, everyone. This is Jennifer Gore, ICANN staff. Thank you for joining us so late in the evening for the Privacy and Proxy IRT.

We have slides.

Thanks, everyone, for joining in the Privacy and Proxy IRT meeting today. We'll get started on – will you advance the slides? – the agenda. We're going to have a presentation from Becky Nash. Welcome, Becky Nash. She's a V. P. of Finance at ICANN. She's going to walk through the fee schedules and some of the activities related to that, as we promised to deliver that during that during this IRT meeting.

After that, we're going to walk through some of the outstanding issues that are still presented: the update to the LEA Disclosure Framework spec, pending updates to the report spec, data escrow requirements, IRT feedback on the privacy-proxy draft of

---

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

---

the agreement, the program status, timeline, and AOB (Any Other Business) to discuss.

With that, I'd like to turn it over to Becky Nash. As I mentioned, she's going to walk through some of the activities related to the fee schedule. This is what was presented to the IRT late February as far as what the new entities are, the existing accreditation entities, the application fee, which is the accreditation fee, and then the annual fee.

Thanks, Becky.

BECKY NASH:

Thank you, Jennifer. Good evening, everyone. This is Becky Nash from ICANN Finance. As Jennifer indicated, I'm going to walk through supporting activities for the privacy and proxy program phases.

Essentially, as we see up here on the screen at this time, we've prepared from a finance standpoint estimated costs identified for two main phases of the program, which is the evaluation of the applications for new privacy and proxy service providers and then the ongoing accreditation for the program, along with the operational and management support related to that.

For the first part, we have the phase of application processing. As indicated here, the services that are supported are numerous

---

but related primarily to the intake, review, and processing of applications. That results in managing the overall program administration and coordinating on each task and project related to the program to facilitate and execute the contracts and documents related to documentation. This includes vendor costs for background checks and other evaluation-supporting activities.

Another key step is overseeing the applicant evaluation process, including evaluation and all the decision-making steps related to applications, point of escalations for application issues, and also subject matter experts related to application and program requirements.

We've also identified support related to defining and documenting informal and formal resolution processes for the new program and complaints related to the program – including communication templates, forms, staff training, and documentation on the program – defining and documenting the privacy and proxy audit program, and also defining document and preparing metrics and reports related to the privacy-proxy compliance and audit programs.

That is all of the activities that we've evaluated from a finance standpoint as it relates to application processing. I'll just pause here for a moment to see if there are any questions related to

---

that phase. Then I'll move forward into the next phase of the program.

[VLAD]:

Quick question. Do you have [amount] to assign to each of those bullet points?

Secondary question: the second-to-last bullet point says, "Define and document privacy-proxy audit program." That seems like that's a one-off thing. Do you have some sort of assumption about how many applications you're going to have and then you define a cost amongst them or split it amongst them? Because I think that's only there once, and then the audit program follows on from there. Thanks.

BECKY NASH:

Thank you for your comment. We have activities related to the design and startup of the program that are just one time. They are actually extra costs related to the design and startup of the program. Here, we are just identifying that there's an ongoing audit program and the documenting of it and reports and metrics related to compliance and audit programs.

Maybe we could change the terminology if you suggest that. It's ongoing, not necessarily at the startup phase.

---

The second point is that we've evaluated overall all of the supporting tasks, resources, and the activities supporting this process. We don't have discrete unit costs available in that respect, but that's the evaluation that we've done internally in order to develop the application cost.

UNIDENTIFIED FEMALE: Hi. We have a question from Steve Metalitz: "What assumptions do you have are made on the number of applications that are expected?"

JENNIFER GORE: Steve, hi. This is Jennifer Gore. Thank you. We looked at the number of privacy-proxy providers that are in existence today. That doesn't mean that we have them in totality. Some of the assumptions that we made, though, we based off of that number. But again, this is a program that's being introduced for the first time, so we don't have a concrete number that we're referencing as far as expected or forecasted applications to privacy and proxy providers.

I'd like to ask those members of the IRT if they would be able to comment on that. We do have the activities associated to what are the one-time activities on the initial startup versus the

---

recurring activities that are directly correlated to these two costs.

A while ago, we did take some assumptions based on numbers that we received from registrars in the range of 200-250, but again, these costs are not correlated to those total units because it's been quite some time since those numbers were calculated or that information was received from the registrars.

Greg?

GREG DIBIASE: Will the last three points be performed by the current ICANN Compliance department?

BECKY NASH: The assumptions are that all of the internal departments that performed these functions will do those same things, so that, even currently under other types of application processing, those departments are involved, and then they will be involved in these activities as well.

JENNIFER GORE: Steve has a follow-up question, which is, "Without a concrete number of applications expected, how can you calculate per-application costs to the right-hand column?"

---

Looking at this is not based upon how much they're going to cost from a volume perspective – like, if we get 200 versus 250, what's going to be the cost? This is an activity for every application that comes through the door – a direct application correlation for each application to activities listed.

Hopefully that answers your question.

UNIDENTIFIED FEMALE: Are there any more questions on this section? If not, we'll move in – Volker?

VOLKER GREIMANN: Maybe not a question but a reiteration of statements that we've made again and again [on the] list. The prices are for accreditation of a service provider that gains no benefit from that accreditation. The registrar and the registry, when they accredited or if they get their contract, have a concrete benefit of being able to sell domain names. Privacy and proxy service providers may well sell their services but usually at cost, just as a door opener for other services.

So this is something that just adds cost to an already expensive service that does not really make money for a lot of providers. There are exceptions, of course. Pricing this in this region will just lead to a lot of unaccredited providers that will switch

---

names every couple of months – an underground that we don't really want.

We want to have as many people onboard as possible. The way to do that is to keep the costs low and not to burden the providers with costs that they should not be bearing for something that essentially benefits only the community and not them.

JENNIFER GORE:

Thank you for that comment, Volker. I just want to point out that, per the final requirements, registrars will not be able to knowingly accept registrations from an unaccredited provider. So one may consider that a benefit.

VOLKER GREIMANN:

Not really, because, once they change their name, we don't know who their registration is coming from. There's so many ways around it, and we want to have as many people aboard as possible. Pricing them out of the market is not the way to attract providers to join this scheme.



---

JENNIFER GORE: Volker, thanks for that. I just want to remind everybody that, from a non-profit perspective, this is a cost recovery exercise that we're walking through here.

GRAEME BUNTON: Thank you. Graeme Bunton from Tucows. Also as a reminder for everyone in the room, the value that this service provides is very likely to be minimized come May, so it's going to be less attractive for most providers.

JENNIFER GORE: If there are no other questions or comments, we can move on to the annual fee summary.

Thanks, Becky.

BECKY NASH: Thank you, Jennifer. Again, this is Becky Nash, ICANN Finance. On this next slide, what we're describing is the approach for the evaluation of the costs to provide the support for the annual accreditation fee.

What we do from a finance standpoint is look at costs related to ongoing programs for direct dedicated costs and resources. Then we look at our direct shared, and then out shared services.

---

Let me start with the direct dedicated costs and resources. These are basically dedicated costs and resources that directly deliver the accreditation services. Again, the types of things that are tasks and activities that are done here are to finalize all projects and tasks needed to complete the program development, including developing a roadmap for future program milestones, deliver services and provide contract administration for contracted parties – that’s one of the main activities – deliver relevant educational outreach and engagement materials and relationships related to the program, implement new requirements for providers that may be necessary as a result of future contractual or policy changes, and conduct compliance checks of existing contracted parties to support the accreditation process – included in this for activities is conducting community outreach regarding privacy and proxy provider compliance with requirements – process complaints regarding this program and providers and all of the requirements, including enforcement, conduct audits of the providers, ongoing reporting of performance of metrics related to the privacy and proxy impacted areas, and the management of general inquiries related to the program. That would be the dedicated costs and resources.

From a direct shared, basically these are additional teams that support the program, but they may also be spread over other

---

types of activities within ICANN. This is work performed to support the delivery and maintenance of the program. This would be comprised of activities like product management, information technology, engineering, and my key area of billing and accounts receivable and cash collection, accounting, and maintaining all of the records related to the annual accreditation.

The final aspect of this costing study is the shared services. This would be the cost of support functions shared within ICANN, so work performed by all other functional areas within ICANN for maintenance and support of the program. That's very consistent with how we look at other costing areas within ICANN where we can't have resources and costs without some rent, without some shared services like human resources, to take care of the people that are performing the services in either the direct or the direct shared costs.

I'll pause here if there are any questions related to this.

VOLKER GREIMANN:

Two points. First point: please copy my comments to the accreditation clause to the annual costs as well because they apply one-to-one here as well.

---

Second point: how are contract management, administration, general support, and service delivery dedicated costs? These are clearly services that can be provided by the existing teams on the side that would not have the need to set up new teams/new staff. This is has to be, in some form, shared costs – the same for the education/outreach teams. This can be done by staff that’s already there. Compliance support – you while hire extra compliance people to handle this? I doubt it. These costs should be next to zero, even with the details that we see here. There’s no justification for these costs.

BECKY NASH:

Thank you for your question. The process that we reviewed for all of the activities is using existing teams, but this is considered additional contracted parties and additional account setup evaluation. So we don’t view it with view of it being just purely incremental at any kind of lower cost base. So it’s an extension of the work that we do. That’s how we’ve done our costing study.

JENNIFER GORE:

Volker, this is Jennifer Gore. I’d just like to – Greg, you’re next – also point out that we have to take into account contracted parties that are affiliated with a registrar and those that may not

---

be affiliated with a registrar – so, standalone privacy-proxy providers.

Greg?

GREG DIBIASE:

This is curious. So it is going to be existing departments. Did you go to the existing departments that would be handling the work and ask them for an estimate of how much money it will add on? Is that \$4,000 because the different departments came back and said, “Yes. This will increase our costs this much”? If so, can we have a breakdown of that?

BECKY NASH:

Thank you for your question. Definitely, in any kind of activity evaluation, we collaborated internally across all teams to review what it would take to perform these tasks. I think the difference is that we’re not discussing building an infrastructure that’s totally separated. That may be something that came up or was being alluded to, but it’s not. It’s not that it’s an entirely new department or new infrastructure. So it is within the existing team. However, these are new contracted parties. It’s not that they are treated as anything, just as extra work or whatnot. It’s not that you hire necessarily new teams until you get to a certain

---

volume. It's all within the same infrastructure. However, these are the costs to perform these duties.

GREG DIBIASE: Let me be more specific. For example, the current Compliance department is doing the compliance work. When calculating this, did the current Compliance say, "Yes, we estimate this added amount of work will add this much money"? I'm just trying to figure out how that input from the existing departments came about.

BECKY NASH: Yes. From a financial analysis standpoint, we did collaborate with each time and identify tasks. Then we did go through an evaluation to price those tasks and understand what activities we would be doing.

GREG DIABISE: Do you have a pricing of those tasks that were provided?

BECKY NASH: We did not detail out a schedule of all of the actual tasks, but we looked at each time and did an aggregate activity study and then, again, evaluated it through the direct, the direct shared, and then the shared service costing allocation process.

---

JENNIFER GORE: Volker?

VOLKER GREIMANN: Just out of curiosity, going to extremes, let's assume we only get one provider that accredits themselves because everybody is just pooling their resources and going through one's privacy-proxy service provider and be done with that. Or, the other extreme: every single service that currently offers it offers it in the future. Let's say that's 1,000 providers. Will ICANN have enough money with 4,000 U.S. dollars? Or will 4 million U.S. dollars be over the budget? How does this scale? How is this number calculated over expected numbers?

JENNIFER GORE: Volker, can you repeat your question?

VOLKER GREIMANN: As you're saying, this is cost recovery. Does it recover the cost if you only have one provider, and does it cover the cost if you have 1,000 providers? Or is it maybe overpriced/underpriced at some stage?

---

BECKY NASH: Thank you for your questions. Again, in looking at the setup of a new application, a setup of a new contracted party, meaning through all of the financial systems and operational systems, if I'm hearing you correctly, if it was only one customer, this would be the cost recovery of just one contracted party, whereas, if it was hundreds of different contracted parties, you then have hundreds of different individual application processing tasks and operational and financial tasks to do.

I hope that answers your question.

JENNIFER GORE: Volker, it's a one-to-one correlation.

VOLKER GREIMANN: How many staff would be hired for \$4 million?

JENNIFER GORE: It depends on the department and the activity.

VOLKER GREIMANN: I'd like to see that broken down for both extremes, please.

UNIDENTIFIED FEMALE: Noted. Thank you, Volker. Any other questions related to this in the room or on the Adobe?



---

I just want to thank Becky for joining us today. I appreciate it.  
Thank you so much.

[BECKY NASH]: Thank you.

JENNIFER GORE: Let's move onto the outstanding issue associated with the LEA Framework. We're nearly finished due to all the work by the IRT. Thank you for all the hard work. We do have an outstanding issue as it relates to the required timeline for a provider to respond to high-priority law enforcement requests involving threat to life, serious bodily injury, critical infrastructure, or child exploitation.

The PSWG has recommended 24 hours or less. The registrar members of the IRT have supported a requirement in business days. Darcy Southwell asked for a poll for the IRT about whether this should be taken back to counsel. The poll suggested that it should not be taken back to counsel with a result of 14 members saying no and four members saying yes to the poll.

A few registrars and the PSWG members met informally earlier today to try to resolve the outstanding issue. It appears as if we may be nearing an agreement or compromise [on] text-to-share

---

with the IRT. The compromised text will be hopefully provided by the end of this week.

Where do we provide that? [inaudible] I don't think we have. Okay.

I'd like to welcome and ask for any IRT members that were in that discussion to elaborate further to provide any comments from that meeting today.

Lindsay?

LINDSAY HAMILTON-REID: We had quite a tense meeting earlier today to discuss whether it was going to be 24-hours/one business day. The registrars that were there, myself included, were not very keen on agreeing that it should be 24 hours. Our concerns were that, if it was a small provider, they would not necessarily be in a position to answer with that time.

Obviously, law enforcement pushed back on that because they did say that several registrars already have in place provisions and resources to deal with issues on a 24/7 basis.

Yeah, that's fine for the bigger registrars. They probably do. Smaller ones, again, maybe for their businesses have – we're not sure. There were no small registrars at the meeting.

---

We did come up with some other wording to put to the group. There were suggestions, which, as Jen has just said, we will look at providing. Just seeing what's on the screen now...

We also had issues with things like action – what does that really mean? We asked for further clarification on that and to tie it in with all the things that we could do, like refusing if we don't have the information and different things like that. Also, we can ask for more information.

Currently, we have moved forward a slight bit, but I'd say we're still at a bit of an impasse. But that's up for the group to decide whether or not they would be happy with that wording or whether they're happy with 24 hours as opposed to business days.

JENNIFER GORE:

Thank you, Lindsay. Would anybody else like to comment?

Peter?

PETER ROMAN:

I just want to walk through it real quick. Looking at the language that's here, there were two major concerns raised by the providers. One of the concerns was that they weren't sure what

---

it was that they were supposed to be doing within the period of the response to the high-priority request.

If you look at the language up here, it specifically says that the response will be in accordance with Section 4.2. Section 4.2 outlines your options. One of your options is to respond with data. One of your options is to respond and say, “We need more time. It’s going to take us some time to assemble this stuff,” or, “We don’t understand your request” – that kind of thing – and one of the options is to respond and say no. If you respond and say no, you can say no because either you have a problem with the request or you just don’t have that information. So that is that issue we hope is addressed here in this language.

The other issue that was raised a lot was the possibility that a provider would not respond. They’re having some catastrophic problem. They’re sick. They’re in the hospital. They’re the subject of a hurricane. They don’t respond, and then ICANN is going to basically de-accredit them for the single bad response.

One of the points that we addressed, which is actually in the accreditation agreement as it stands right now, is that that’s not actually the mechanism for de-accreditation. There’s a whole section on it. I don’t have the number right in front of me, but there’s a whole section on – I’m sorry?

---

UNIDENTIFIED FEMALE: [That’s three strikes].

PETER ROMAN: Yeah, I’m getting there. Do you want to talk?

UNIDENTIFIED FEMALE: No. You’re doing a great job.

PETER ROMAN: Okay. There’s a whole section on what you need to do in order to get de-accredited. In particular, there have to be three violations of the agreement, three breaches, and they have to be significant breaches. They can’t just be minor breaches. So this is not something where you have a bad day and your phone falls in the toilet and you don’t respond and then you get de-accredited and you lose your business. So that piece is covered.

The other point I wanted to make is that the law enforcement ask actually is not 24 hours. If I had my way, I would be asking everybody to respond immediately. The high-priority mechanism is designed specifically to deal with things that have to be acted on immediately. They’re imminent threats of life and limb. That means somebody might die if you don’t respond.

So 24 hours is the compromise. You guys want it one businesses day – actually, I think initially you wanted two business days and

---

some extra time – but our preference would be that you respond immediately to it. This is the middle ground that everybody can kind of agree on so far. I hope you’ll take that under consideration. I’m happy to talk about this with anybody that wants to. That’s pretty much where we stand at the moment.

JENNIFER GORE:

Thank you, Peter. I have Volker in the queue, and then Lindsay.

VOLKER GREIMANN:

Having never seen such a high-priority request, I cannot really judge on how many there actually ever will be in connection with these services. I note that other services, such as hosting services, do not have any requirements to respond in a certain time other than those specified by law. There, people might die, too. Yes, people may die. That’s the course of life. Sometimes it’s unavoidable. It’s asking what is reasonable when you compare the risk on the one hand to what is actually reasonable to expect a provider to do.

You are not creating laws or lobbying for laws – that everyone who offers any kind of service in any country in the world would be subject to such a requirement. Yet we are supposed to be subject to this.

---

Is there any justification for making such a differentiation? Why should privacy-proxy providers who cannot even touch the content be subject to such a turnaround when other services are not? What's the justification for that?

I realize there may be such cases. I've never seen one of those. No one here at the table who offer such a service has ever seen such a request coming from law enforcement. Law enforcement has always been very happy with our turnaround times. We try to offer them as quick a turnaround as possible. But to put this into a contract as a requirement goes too far, I think.

We can offer best efforts. We can offer that we will respond as possible, as soon as we see it, but to make it a contractual requirement? That would essentially force providers to guarantee a readiness that they have no qualification for and that they are not equipped to provide. That is going too far.

One-man operations that do exist and offer these services are allowed to go on a holiday and turn off the e-mail. This would prevent that.

JENNIFER GORE:

Peter?

---

PETER ROMAN:

There are like eight things in there. I'm going to try to respond to each of them in turn.

The first thing – well, there really are eight things in there. Okay. We were given a number earlier today by GoDaddy, I think, who said that 80% of the people who provide these privacy-proxy services are small providers. So the first thing is: why put this into the contract? Well, we put this in the contract not because I'm worried about your response, not because I'm worried about GoDaddy, and not because I'm worried about anybody else who's here – Tucows. It's here because there are people who are small providers who will not respond to emergencies. There are people who are bad actors who will not respond. They are marketing their services specifically to the bad guys. There are people who will look at their bottom line and say, "You know what?" – more or less the equivalent of what you said earlier – "People die. This affects my bottom line. I'm much more worried about having to hire people. I'm going to have to have somebody with a pager or a phone available 24/7."

We're not asking a lot here. The response is one of three things. The response is, "Yes. Here's the data," "No. I don't have it/I can't get it," or, "I need more time." This is not an unreasonable response. All you're asking people to do is to be available.



---

Anybody who's running a technical company, like yours, is probably available 24/7 anyway. If they're not, they've got somebody on staff who can be. When I was an Oracle DBA in the '90s, I carried a pager. I responded. I didn't work for Oracle; I worked for a small consulting company. When systems go down, you're available 24/7, holidays and weekends. Somebody has to be available. It's a technical market. It's global. It's all day, every day. You have to be available for that.

I actually don't remember the other eight or nine points, so I apologize. If you want to give them to me again, we'll address them each in turn.

JENNIFER GORE: Greg and then Jody – Roger. Sorry.

GREG DIBIASE: I'm the shorter one. Just talking about the small business thing, saying it's not a big deal to make them have a pager? That seems like a really big deal. I just feel like it has to be one business day. There really are small providers that are not – that is such a large change to be stemming from this one section in the privacy-proxy accreditation to their business model. They're signing up to all these agreements. They're complying with all these different things. This is going to change their, basically,

---

entire modus operandi, when a business day, I think, is reasonable and should be sufficient.

PETER ROMAN:

Can I respond? There are two parts to that. The first one is that the business day is problematic for a number of reasons. Like I said before, if it was up to me, it would be an immediate response.

When I was an Oracle DBA, when I was out there in the world and I was doing IT stuff, I didn't understand this. What we're talking about here, when we say "imminent threat to life and limb," we mean people die. I get a week of duty 24/7, where I'm duty for a week, and I get these calls and I deal with them. If I don't handle them and I don't respond, somebody dies.

So the balance, to some degree, to your question here is that, for the small provider, there's a minor inconvenience, where he's got to be available, or he's got to have somebody available who can reach him who can respond. Again, the response isn't necessarily, "Here's the data." The response can be, "I can't get it right now," or, "I need more time," or, "I don't understand." That's part one.

But if he doesn't respond, somebody dies. You say one business day. That means – because we batted this around earlier – that,

---

if I send you a request Friday night, I may not get a response until Monday night. If I've got an imminent threat to life and limb, that means somebody is going to die imminently. "Imminently" basically means "now." A three-day response time? You get to me in 48 hours, you get to me in 72 hours? That means the victim – and it's a victim – has been dead for 70 hours by the time you get back to me.

I know that seems extreme – this is the point I was trying to get to before – because you guys don't deal with that all the time. But those of us who do what I do – there are a bunch of us in the room here right now – deal with life and death situations on a regular basis. People actually die if people don't respond to these kinds of issues. It's very important to the person whose life is on the line.

I think that, on balance, it's more important to the person whose life is on the line than it is to your small provider.

UNIDENTIFIED FEMALE: Roger, and then we've got a comment and a question in the Adobe. And then Volker.

ROGER CARNEY: Thank you. Two things. Because you mentioned it, the response being – I don't know. I don't have the data. You mentioned no

---

response and someone can die. With those responses, someone is going to die. Just to be clear, a response doesn't stop the death.

PETER ROMAN: Not necessarily.

ROGER CARNEY: Okay. The interesting thing that I thought Volker said out of those eight things – the one I was waiting for that didn't get touched – was, “What other businesses/industries are held to this level?”

PETER ROMAN: Actually, that's easy. The registries just agreed to this, for starters.

How's that?

This is not an unusual requirement. This is a requirement that a number of the people who were sitting around the room earlier with me today who were, granted, large – it's GoDaddy, it's Tucows, it's....I forget who the other one was; I apologize – 1&1; I should know because I interact with you guys – have systems already set up for this. You've already got a compliance system set up. You're already responding to subpoenas and search

---

warrants and whatnot. This is the smallest addition to the entire thing. You're really just talking about having one guy be available who's just got to be able to get back to us. If it turns out that it's not something he has immediately available to him, he can talk to us and we can work it out and try to figure out if we can solve it.

Because you're right. If the answer is no, or the answer is, "I can't help you. I need more time," that may result in somebody dying, too. But at least we're trying at that point. If you're talking to us within that window while the person is still alive and there's something we can do about it, then the conversation itself may lead to a solution that gets us to the point where the person's life gets saved.

ROGER CARNEY: Are there any other industries that follow these? You mentioned registries, but outside of that, do shoe manufacturers?

UNIDENTIFIED FEMALE: A life and death shoe situation?

ROGER CARNEY: A domain? A life and death situation?

---

PETER ROMAN: We've had life and death domain situations.

ROGER CARNEY: I'm sure there's a life and death shoe thing too, but a domain doesn't kill somebody.

PETER ROMAN: Right, but this isn't what you guys are doing. You guys are providing privacy-proxy services, which means that you're essentially hiding the name of the registrant from public availability, which means that we can't go get it and figure out who this person is without your help.

So in the tradeoff, you guys get to make money and do business and hide these people's information, and the tradeoff is you have to help us when there's an emergency. We're not doing this all the time. We're not going to be knocking on your door every 15 minutes. There isn't necessarily going to be a huge volume, but what volume there is really matters. These are people's lives we're talking about. I realize you guys are looking at, "My bottom line is" – not necessarily you personally, but for small companies – "how do I do this? How do I pay for it? How do I get somebody who's available at this time?" It's a cost. There is a cost to this. But it's a cost that has to be balanced against what it can do. What it can do is save people's lives.

---

UNIDENTIFIED FEMALE: Hi. I first have a comment from Amy Bivins, ICANN Staff. Some additional background [she wanted] offers: “The requirement for the provider to respond under this framework will be limited to the [LEA] from the provider’s jurisdiction. See Section 1.1 in the LEA requestor. The requestor is the law enforcement, consumer protection, quasi-governmental or other similar authority designated time to time from the national or territorial government of the jurisdiction in which the provider is established or maintains a physical office.”

I also have a comment from... Sara Bockey. “This isn’t just about U.S. LEA. It’s the largest providers on the planet. You have considered other countries and governments. The language can be abused by other law enforcement countries and that do not have the constitutional rights. This must be considered.”

We also had a question from Steve Metalitz. “What is the basis” –

PETER ROMAN: I’m sorry. Can I respond to the first question before we go to the next question?

UNIDENTIFIED FEMALE: Sure.

PETER ROMAN:

Right. We were talking about this earlier in the meeting this afternoon. One of the issues is: what if you get somebody who's a bad actor? What if you get law enforcement from some country that we all don't trust, or that we think we should not trust? What if you get somebody who's abusing the process, who's sending you lots of requests that actually aren't emergency processes?

Obviously, that's a problem. For the record, I have not seen that, but GoDaddy told us earlier today that they had seen these kinds of requests. To some degree, the protection against that is that you're not going to get the request directly from that foreign government. The request, as written in this agreement, goes to your local law enforcement. Your local law enforcement is going to vet the question before it comes to you. When they say, "I've got an emergency situation/I've got a high-priority situation," that goes to local law enforcement. Local law enforcement says, "Yeah, you do," and then passes it on to you. So it's already gotten a certain degree of vetting that's going to happen before you see it.

We do this all the time. I get emergency requests from overseas when I'm on duty all the time. I'm forever telling people, "I'm sorry. That doesn't mean our standards. But we'll help you get



---

whatever core process you need in order to go get that information.”

UNIDENTIFIED FEMALE: Okay. I appreciate that, but you completely missed the point of the comment. This isn't about people in the U.S. and you guys. This is about people that are in other countries, in third-world countries, that are dealing with this and the way that those local agencies in that country could potentially abuse this language. So this isn't about you and what you do. This isn't about GoDaddy. This is about other providers in other regions of the world. That's the point that we have to keep in consideration.

PETER ROMAN: I'm sorry. I don't understand how that changes the analysis. If you don't trust your local law enforcement, then your local law enforcement is going to be abusing your position regardless of whether this emergency request process exists.

[JENNIFER GORE]: Can I remind people to state their name and affiliation before they speak?

We also have additional comments in the chat that have been waiting for a while. Steve Metalitz had a question: “What is the

---

basis for the estimate of “80% of the providers are small”? Does this include affiliates or wholly-owned subs of accredited registrars which are subject to a 24-hour turnaround under the RAA?”

UNIDENTIFIED FEMALE: Steve, I think your question was related to Peter mentioning earlier about GoDaddy stating that 80% of the privacy-proxy providers are small entities. I’m not sure that James is in the room. I believe he might have been the one that mentioned that.

ROGER CARNEY: When you look at it – is James here? Oh. I thought you were looking for him. 80% of registrars are small. It’s the same effect. I’m sure that’s what James was just mentioning.

UNIDENTIFIED FEMALE: Reg Levy?

REG LEVY: Thanks. Reg Levy from Tucows. Peter, you said that we registrars are already dealing with warrants and subpoenas as though this isn’t a warrant and subpoena issue. Can you please speak to that?

---

PETER ROMAN:

Yeah. The whole point, real quick – Peter Roman, U.S. Department of Justice; sorry about that – of this exercise, the whole point of the high-priority request, is that there isn't time for a subpoena or a search warrant or any other court process. We've got an imminent threat. We don't have time to go to a judge. We don't have time to go to a grand jury. We have to get your help now. If we had the time to go to a judge or a grand jury, we wouldn't follow this process. And we don't. These processes exist in the United States. You've probably dealt with them too.

Now it's an emergency. I've got a kid who says he's going to shoot up his school this afternoon. I've got a guy who says he's going to bomb the train station in an hour. There isn't time to go get a search warrant. We don't have time to put that stuff together. It's an emergency. And we need help. That's the difference.

REG LEVY:

And you said that you're okay with me responding no – sorry, this is Reg Levy from Tucows – so I could just actually set up an autoresponder that says, "Bring me a subpoena instead." That would be a 24-hour response.

---

PETER ROMAN: And that would be a failure under the terms of this agreement. There are very specific reasons why you can say no. You can say no if you actually cannot access the data. You can say no if I'm asking you for something that's illegal. You cannot say no because you feel like going on vacation and it's okay with you if people die because people die.

REG LEVY: No, no. I didn't say I was on vacation. I said that it's illegal for you to ask it of me without a warrant.

PETER ROMAN: Then you would be in violation of the terms, and every time you did that it'd be a serious breach and somebody would die.

VOLKER GREIMANN: Let's try to keep this reasonable. We've asked again and again for concrete examples where a person had died – actually physically lost his life – for the simple reason that law enforcement was not able to penetrate WHOIS privacy service within 24 hours. Three very specific conditions. We've asked for this again and again. Not a single case. Until I hear details of a single case, this will all be hypothetical, theoretical. Unlikely. One in a million cases where this actually applies. For that, to apply a general requirement that is unwieldy and very hard to

---

implement for very small providers out there, I think it's unreasonable.

I think you said it before. Your main concern is not getting an answer because some of the services are unresponsive. We've dealt with that. We've offered a business day. That's a lot more than you will get from any other industry.

If you can provide these cases, which we've asked for again and again, we might reconsider because, when we are confronted with reality, then the picture might change. But we haven't. Until I hear one of these cases, this is theoretical. And for theory – I don't know.

PETER ROMAN: Okay.

UNIDENTIFIED FEMALE: We have a queue.

PETER ROMAN: Okay. I was going to respond. That's all right. Message board. It's a domain. Guy who registered the domain used a privacy-proxy service. We don't know who it belongs to. A woman advertises on the board that she's going to sell her six-month-old baby to

---

the first person who can give her meth. That’s what we’re talking about.

This is not hypothetical. It’s is not one in a million. It’s not every day. I’m not making this up because, for some random reason, I feel like you guys need more work to do. These are real issues with real people and real responsibilities. You’re small companies. You want to do this job. You have to accept the responsibilities of doing this job.

VOLKER GREIMANN:

Again, this doesn’t answer my question because the owner of the message board likely doesn’t even have the information of who posts on that message board. He might have it, he might not have it. This is a case that sounds horrendous, but I don’t see how the privacy-proxy service provider would be able to help in this case.

PETER ROMAN:

Because I went to the privacy-proxy provider and I said, “Hey, do you have this information about this? Who has this board?” They said yes. We went to the board, they said, “Do you know who this person is?” They said, “No, but we have a phone number.” Then we went and we tracked the phone. We were able to get

---

her before she sold her kid. It turned out she was also offering up her three-year-old.

Not hypothetical. Not making this stuff up. Don't understand why anybody would think I would go to all this trouble flying all the way out here so I could make stuff up to give you guys more stuff to do.

UNIDENTIFIED FEMALE: Thanks, Peter. After Lindsay, I'd like to close the queue, but I'm inviting everyone for comments to the proposed language that's been presented to the list and that's up on the screen.

Lindsay?

LINDSAY HAMILTON-REID: Peter, we spoke earlier. I realize that you feel incredibly strongly about this. I think we all can see that.

I think the problem is... Again, you've just mentioned that one example. As I said to you earlier, I've only ever had one high-priority thing. And that wasn't anything to do with the domain name. The rest of us haven't had any of these. So to me it looks like you're trying to solve a problem that, currently for all of us, doesn't exist.

---

Plus there's the fact that you're not a party – law enforcement is not a party – to this contract. This is something else that you want to be involved in. You want to try to influence what we do in this contract. I understand that. But you're not a party. ICANN is. The registrars are. The proxy providers are.

At the end of the day, it's what those providers can do. If they fail – they can't answer within 24 hours and want a business day instead – I appreciate that that's going to be hard for you. But that might be what it ends up being.

JENNIFER GORE:

Thanks, Lindsay. Greg, and then I'd like to just move on to the last slide. I'm just going to read it but table the questions for the next IRT session.

Greg?

GREG DIBIASE:

I'm just going to say that it sound like we respectfully disagree with each other. Maybe we need to just accept that we're not going to compromise here. What are the next steps if that's the situation?



---

JENNIFER GORE:

Thank you, Greg. If that is the situation, it'll be noted in the executive summary for public comment as an open item.

If we could move on to the next slide – thank you. Just for the purposes of the last five minutes, the other items that we still have open with the IRT is the reporting specification, seeking feedback from the IRT for the use of the RRI versus the e-mail form, and the separation of request by category – LEA, IP, and other. The draft will be updated and we will distribute that this week.

The next one is the data escrow spec to be part of the privacy-proxy agreement. Question included in the privacy-proxy draft for the IRT feedback. We're seeking feedback. Putting technical specification into a separate document would permit updates to be made as text specs evolve without requiring an amendment process and seeking feedback from the IRT for that. And also seeking overall general feedback to see if there's any additional comments on the current draft of the privacy-proxy accreditation agreement. Again, we will open the next IRT session with these particular items here.

With that, I'd like to thank everybody for your time today. I appreciate your participation. Have a good night.

Please stop the recording.

**[END OF TRANSCRIPTION]**