HYDERABAD – Security Framework Drafting Team
Tuesday, November 08, 2016 – 09:15 to 10:30 IST
ICANN57 | Hyderabad, India

UNIDENTIFIED FEMALE: Security Framework Drafting Team meeting, starting at 9:15 A.M. in room G3.

DENNIS CHANG: Good morning, everyone. We'll get started in a minute here.

Alan, I see you there. Can you speak so we can hear you?

While we're waiting for Alan to get his audio – maybe he doesn't need to speak. Or he can chat. We have other leaders here from the registries in the room.

UNIDENTIFIED MALE: [inaudible]

DENNIS CHANG: Ah. Okay.

Alan, we're going to try to dial out to you.

While we get that started, let's get this meeting started. Good morning. This is the ICANN 57 open session for the Security

Framework Drafting Team. Earlier this week, we had a few closed sessions working to make progress on this project. Here we will see some of the results of that effort. The drafting team has been together for a long time and working very hard at it.

Now, before we get started, should we try to do an introduction around the table? I'd like to know who's in the room. If you are a member of the drafting team, please identify that. If not, just identify as an observer. Thank you.

Why don't we start at that end over there? Gentleman in the yellow shirt?

LUCAS DE MOURA: I'm a first time Fellow and observer.

LILI SUN: Hello. Interpol, PSWG member.

IRANGA KAHANGAMA: FBI, Public Safety Working Group.

LAUREEN KAPIN: United States Federal Trade Commission, Public Safety Working Group.

JOE WALDRON: Verisign.

NICK SHOREY: Good morning. U.K. government.

RAYMOND ZYLSTRA: Neustar.

JASON PLOMP: Good morning. Royal Canadian Mounted Police, Public Safety Working Group.

[MADIE NEWELSON]: [inaudible], [Canada], Public Safety Group.

DIRK BALLOU: Dirk Ballou, Drug Enforcement Administration, Public Safety Working Group.

FABIEN BETREMIEUX: GAC Support, ICANN staff.

KRISTA PAPAC: ICANN organization, Registry Services.

MERT SAKA: ICANN organization, Registry Services.

DENNIS CHANG: ICANN organization also.

BOBBY FLAIM: FBI, Public Safety Working Group.

BRIAN CIMBOLIC: PIR, Registry Stakeholder Group.

FREIDA TALLON: Registry Stakeholder Group; part of the drafting team with Brian.

JIM GALVIN: Afilias, part of the drafting team.

MAXIM ALZOBA: .moscow, part of the drafting team.

BETH BACON: PIR, part of the registry's drafting team.

RICHARD ROBERTO: Google, part of their drafting team.

STEPHANIE DUCHESNEAU: Also Google.

RICARDO ALVAREZ: ICANN staff.

ASHISH [AGARWAL]: Hi. I look after the network operations of the government of India. Thank you.

DESSALEGN YEHUALA From academia, observer.

DENNIS CHANG: Do you want to come and sit at the table or at least introduce yourself? [inaudible] – okay.

[SIDEMA]: System Administrator, [Skynet].

UNIDENTIFIED FEMALE: [inaudible] Media and Communication, Germany, [backend] – registry backend.

[RAMDAS]: I'm from academia and an observer.

M. CHAKRABORTY : I'm from Goa University.

Y. VARA PRASAD: STPI, Hyderabad.

UNIDENTFIED MALE: STPI, observer.

DENISE MICHEL: Facebook.

CARLOS ALVAREZ: ICANN staff, SSR team.

DAVID CONRAD: ICANN organization, CTO.

JENNIFER SCOTT: ICANN Contractual Compliance.

UNIDENTIFIED MALE: [inaudible] [I'm an observer.]

DENNIS CHANG: Is that everyone? Thank you for joining us this morning. We'll get started then. What we will do is start with Bobby, who's one of the Co-Chairs leading this effort. I'm going to ask him to give us some background on what this is and why we're doing this, why this is so important, and what the mission of the drafting team is.

Go ahead, Bobby.

BOBBY FLAIM: Thank you, Dennis. I may call upon Fabien and Krista Papac to maybe fill in some of the historical blanks if I go astray.

Basically, what we are doing here is we're trying to draft the security framework. It's a voluntary framework and it is pursuant to the public interest comments – Specification 11, specifically Spec 11.3b. The PICs are contractual commitments by the registries.

What this document is – the registry security framework – is basically voluntary methods to respond to the contractual obligations to look at security threats. So basically, how will registries respond to security threats?

Again, this is a voluntary document on how the registries would respond to security threats, whether it is a security threat that they find internally, a security threat that's reported through the

public, or a security threat that may be reported from a public safety agency.

To give you a little bit of the history on how this started, the GAC had provided advice in 2013 at the Beijing meetings concerning new TLDs, concerning safeguards, which were written into the contract as PIC Specification 11.

What happened after that is the NGPC had decided to review and see how we would go back. At that point, if I recall correctly, in June 2015 at the Buenos Aires meeting, ICANN had proposed to hire a third party to actually do this. The registries did not agree with that, so the solution was to come up with the registries and the PSWG to come up with a drafting team to actually draft this security framework.

So starting, I guess, in the summer but really in the fall of 2015, the registries and the PSWG, at that time led by John Flaherty who was with the National Crime Agency in the United Kingdom, started to draft this security framework.

So Version 1 – and again, correct me if I'm wrong – John Flaherty had written the document. I guess, upon discussions with the registries, that document was not accepted and we went to Version 2, which was drafted by the registries.

During, I guess, the spring of 2016 – this year, going into the summer – there were calls between John Flaherty of the PSWG and the registries, Alan – was it Alan Woods who was…? – okay, Alan Woods, who was the representative for the registries.

Then, unfortunately, John left us. He decided to leave the NCA and go into the private sector, so I was selected to lead the effort on behalf of the PSWG. Since, I would say, about May or June, there've been as series of calls and a couple of drafts that have gone back and forth between the PSWG and the registries.

Based on the document that we had started working on that the registries had provided, which we'll call Version 2, the PSWG added some provisions, which is what we started to talk about here this week; the two meetings that we had earlier in the week.

And that is where we're at now. Some of the issues that the PSWG had concerned the fact that the document just needed a little bit more specificity. It needed to just be clearer on what is was saying.

So we went back and forth with a few things and we have to say, just as the PSWG, number one: we're the PWSG, so we have to come up with consensus among ourselves. Secondly, we are a subgroup or working group of the GAC, which means we have to

go back to the GAC and report what we're finding and ensure that this meets the intent of the original GAC advice.

Another part of the dynamic of the PSWG is that, since we are government representatives, we also do have to clear it through our own agencies. So you will have to forgive us where we don't act as quickly and as flexible or on dime as we would like to.

At this point in time, the registries, based on some of the input that they have received prior to this meeting and in this meeting, have provided additional edits. That is where we are at right now.

I think I can end there, and if you want to jump in and add any additional comments or background.

DENNIS CHANG: Thank you. Now, if Alan is on the line and can speak, could you please speak so we can hear from you? Alan Woods is the Co-Chair from the registry.

ALAN WOODS: Can you hear me okay?

DENNIS CHANG: Yes. Thanks for calling in.

ALAN WOODS: Not at all.

DENNIS CHANG: Would you have anything to add in terms of background, the objective of mission?

ALAN WOODS: No. I think, actually, that Bobby did very well on that. The only thing I would say is that Yasmin Omer who started out at the helm for the registries, and I took over midstream as well. I think, Bobby, you laid it out very well, so I can't add anything to that at all.

DENNIS CHANG: Okay then. I want to then turn it over to Brian, who's sitting right to you.

BRIAN CIMBOLIC: Thanks, Dennis. And thanks, again, to Alan for dialing in from Dublin at 3 A.M. It's probably three days ago at this point.

The registries got together after our initial meeting with the PSWG and had a registries-only session and came up with a list of seven bullet points that represent probably the macro issues;

things that are really the remaining hurdles – not any particular edit; not any particular language. These are conceptually what we felt, when we got together, needed to be addressed to get us across the finish line.

I'd invite Alan or Freida or Beth or anyone else that was in the room when the registries met to jump in at any point if you feel like I'm missing anything. But I think it might be helpful just to briefly go through these bullet points just to hear what the thought process is and where our pain points may be for the rest of the document.

Something Bobby said is absolutely true. In certain points, the document was lacking specificity. I think that specificity helps not only the PSWG get where it needs to be, but the registries, too. The first two points are related on that point.

One is clarifying what's meant by a response. I think what we heard from the session with the PWSG and the registries was that what the PSWG seems to be looking for in a response is knowing that someone is on it, that they've received a response from a non-automated – that someone has actually answered your referral and you know that there's a pair of eyes on the question at the registry.

So we provided a basic outline of what a response is, and we think a working definition of response should be "a non-

automated response from the registry abuse point of contact that 1) confirms receipt of the referral, and 2) that the registry will investigate the security threat."

I invite input from anyone, too, not just the registries. If anyone in the PSWG has any immediate reaction to these, feel free to jump in. But [I] do understand that you do need to internally discuss these over, too.

The second part of that is, assuming that we have a working definition of a response that's similar to the definition that we just provided, the registries are comfortable with a 24-hour response time to high-priority security threats. But, again, I can't emphasize enough that the timeline is contingent on the definition of the response. If the response is somehow full remediation of the security threat, then we definitely cannot commit to 24-hour turnaround on this.

The next bullet is categorization of security incidents. In talking things over, we think the three categories may be more appropriately condensed into two. One, a high-priority incident, which would necessitate a 24-hour response time. I'll get to what's included in that high priority bullet in a moment. And then two, any other incident not listed above in Category 1, the high-priority issues, related to technical abuse of the DNS, which

will be handled according to the anti-abuse policy of the registry.

So we did add the caveat, which gets to the next point, of technical abuse related to the DNS. As Bobby points out, this all stems for Spec 11.3b, which does relate to technical abuse of the DNS. We understand that the high-priority questions of the threat to the life of another or critical infrastructure would be treated differently. But when the – going to the next bullet – registries aren't comfortable with, effectively, content regulation of the DNS.

So any sort of security incident that is just any other crime not related to the threat of another, we don't think is actually a security incident under Spec 11.3b.

Along the lines of what's included in the categorizations: the threat to life and limb. This was a term that the PSWG pointed out as a term of art. And while that's true, terms of art can vary jurisdiction by jurisdiction, as all the lawyers in the room know.

We thought that what this really got to was the imminent threat to the life of another. We think that removes some ambiguity, and I think it gets to the heart of what was meant to be addressed by the threat to life and limb.

For verification, Beth or Alan or Freida – do either of you guys want to jump in to briefly touch on the verification bullet?

FREIDA TALLON: Good morning. As part of the technical analysis, the registry will verify that the referral is from a reputable and known LEA source, acknowledging that the response shall be provided in line with the requirements of this framework and is considered separate to the process of verification.

Basically, we wanted to say that we would follow up on any serious request about a threat to life of another or other serious incidents with saying, "Right. This is something. We actually want to make sure that a human is touching this." So it may be that you get an automated response, but it will be followed up, where it is appropriate, with a human being that is saying, "Right. We are investigating this once we confirm that you are who you say you are." So we don't want to be responding to something…

Pretty much most organizations have the ability to say, "Well, we're not judge and jury, but we're actually going to be able to have a look at this and say, "This is a valid request for more information."" While we're investigating it, we will help and assist where it is necessary without becoming something that

we're not supposed to be and protect, both in commercial and in business terms, what is required.

Alan, would you like to add anything else on the verification?

ALAN WOODS: Thank you, Freida. Yeah. Very quickly, what I would say about it as well is that – Brian has already touched on this with regards to the verification point – if we are looking to a full response and resolution of the point, then we can't do that, say, within the 24 hours. So that's the main point of the verification as well: to say, "Yes, we will definitely acknowledge this, but please don't expect it to be resolved within the 24 hours." They are two completely separate things as well.

BRIAN CIMBOLIC: Maxim, did you want to jump in?

MAXIM ALZOBA: Just for a clarification to the verification item, when we say "reputable and known law enforcement," it means the relevant law enforcement because in every jurisdiction, the only law enforcement is the local one. That's it. Some exemptions could be a case where two governments have special agreements and

they recognize law enforcements from each other. But it should be in place.

BRIAN CIMBOLIC: The last bullet echoes something that we just heard from Bobby. Because this is a voluntary framework – these aren't going to be mandated practices – the next logical step from there is that this document isn't treated as some sort of baby step towards policy development because this group isn't the appropriate venue for actual policy development. That would need to go through the GNSO.

So just to quickly run through those. Those were the initial registry thoughts as far as the big ticket items remaining on the framework draft. Of course, there might be some nits and perhaps some smaller issues, but these were the high-level remaining questions from the registry side.

With that, I would welcome any thoughts from any registry members or any PSWG members, fully understanding that the PSWG hasn't had a chance to meet on this and that whatever you say won't be binding to the PSWG.

We met quickly to try to get this to you with plenty of time to review, so any sort of initial feedback you may have would be greatly appreciated.

[ROBYN]: Thank you. Actually, I'm not comfortable about the definition about the "response." Let me give you a vivid example. When I attended this conference, on the first day arrived at the airport, I hired a cab to my hotel. The driver failed to show me the meter, and he said, due to Internet access failure, he couldn't show me the meter. He charged me 1,500-something rupees for my ride.

I believed it was not reasonable, and I failed to bargain with him. So I called the local police. The police officer recorded my complaint and he asked what the problem was and where my location was. Ten minutes later, they arrived. They helped me to solve the problem. I believe that is the response. So from my point of view, that's a "response."

I'm not comfortable about the definition here of the "response" at all. Thank you.

BRIAN CIMBOLIC: If I may, what are you looking for from the registries, if not an acknowledgement that we've received and are going to investigate? To be clear, this isn't a "Thanks. We got it" and no action is going to be taken. There's a commitment on behalf of the registries to investigate and use its discretion to determine

whether or not this actually is a security incident and to take any remedial action moving forward.

[ROBYN]: Actually, I'm looking for the action list from this framework. This is not "I received your complaint. I will do something," but we can find some set actions to several security threats. It can be set actions.

FREIDA TALLON: Thank you. Maxim had a response, and then Jim. Sorry.

MAXIM ALZOBA: Yes, two notes. First of all, what you used as an example – actually, it was [paid]. The second thing. If you suggest that we run full-scale investigation in 24 hours, you can't imagine your internal spendings on lawyers, investigators, and technological stuff which will be necessary for a 24-hour window of investigation. And we will not be able to spend less.

Given that, we asked ICANN for additional funding for such a good idea. We were denied. We actually will kill small and medium registries if we demand that they have 24-hour access to security and technological experts.

If you combine those items and just come to the spending points, you will see that, effectively, we will have to do something which is in law enforcement's role without power or funding to do so. We cannot be a collection point for calls. Our contact centers cannot be compared to contact centers of police. For the high-threat items, we cannot collect them from all the countries.

We will accept such things from the trusted law enforcement sources because, otherwise, we will finish doing the registry job and start talking on the phone, saying, "No, no. Unfortunately, we do not understand…No, no. Unfortunately, we cannot run private investigations."

Also, I must say that, in some jurisdictions, legal bodies are actually prohibited from making judgments. So they can't rely on the judgment of law enforcement, the General Attorney's Office, or the court. So it's not that simple, and if you insist that we have to deliver a plan of what we do when…

Actually, first of all, we should understand how it's going to play because… Do not expect us to deliver public enforcement services to the public. Thanks.

FREIDA TALLON: Can I just remind everybody that this is an advisory, and all registries are self-regulating? It's in their interest to ensure that they have and monitor situations. We have always very much cooperated with all law enforcement requirements and requests, but the thing here is that we have to verify that it is an actual serious threat. This is what we're categorizing here: whether it's a really serious threat and not business as usual, which we refer to as BAU.

In this instance, we feel that it is very fair in how we would want to A) verify that the actual request coming in is legitimate because there have been very spurious requests coming in for information which has nothing to do with law enforcement. So verifying that from the start is important.

Making sure that we're working with law enforcement locally and within jurisdiction and within our legal requirements is always very important.

So you've got to step back a little bit on this and ensure that you realize that this is an advisory. We're willing to work with it. We're bound under Specification 11.3b and part of our registry agreement, and we will self-regulate. But we've got to be sure about this. We're coming to the table here, advising you that we are willing to work and make sure the public safety initiatives are in place, and that we want to help along the lines.

Jim had a query next, and I think that somebody else had –

UNIDENTIFIED MALE: [inaudible]

FREIDA TALLON: Yes. Sorry. Jim first.

ASHISH: There's an organization called CERT (Computer Emergency Response Team), which is an information security team for all the countries. Does ICANN also have a collaboration of some sort with them? Or can it have something like ICANN CERT or something to solve these sort of issues?

IRANGA KAHANGAMA: I don't have an answer to that question, but I think, before we discuss all the points, we really appreciated the efforts and the comments you gave. We had a chance to meet both before and after these comments came in as the PSWG. I think we were trying to really figure out, based off of our first initial meeting, how best to contribute and how to really create something that had our best interests.

Honestly, we had a little bit of difficulty doing that. I think, to level set, we went through a little bit of a process to realize that

we do want more specificity in the document. But I think the kind of structure that it was built on precluded some of that specificity. We were thinking that there could be ways to alter the document.

We haven't had enough time to talk about this, so this is very conceptual or whatever. But there may be ways, given that it's a non-binding voluntary contract, to maybe build in some more specificity, whether that's bucketing responses to separate out what the public is reporting and then what law enforcement is reporting or something like that.

I think we have some kind of internal analysis to do to figure out how it is, but I think a lot of our public safety members agreed – and feel free to comment – that the document as itself was still a little shaky for us and that we that we are still trying to explore some ways to build in some more specificity.

[JIM GALVIN]: Just to respond to the question about ICANN CERT. About seven years ago, there was initiative done within ICANN to create something called the DNS CERT, but the community largely viewed that as out of scope of ICANN's limited technical remit. So those efforts were curtailed.

If the community feels that CERT would be warranted, then that's something that we would consider.

FREIDA TALLON: Dirk is next.

DIRK BALLOU: To follow up on what Iranga was just talking about, I'm a bit new to this process and so perhaps naïve, but I think in a positive way, maybe, because what I've gotten from this is that it's pretty obvious that although the Public Safety Working Group has that piece in their title, everybody is concerned with public safety, and that's been evident. So that's been a good thing.

As Iranga pointed out, some of the difficulty that we had was, somehow, with the way that the format currently is, I don't think it really allows all the stakeholders to properly represent the different groups that they're designed to or sworn to represent. The difficulty is, with some of the definitions or some of the examples that we're trying to speak to and define, we've tried to define everything through one funnel.

That's not always to do because as Brian and Freida spoke about the other day, the scale of the different registrars is so varied that, as Max has pointed out, for the staff to internally do some of these responses is just not practical.

So this being a voluntary document, sometimes, if we are trying to represent the folks that we are to represent as stakeholders, it may be better to try to explain in the document: "Okay. These would be the security framework or perhaps the best practices that perhaps public safety organizations would have."

One of the things that I've learned in the short time that I've been participating with ICANN is that oftentimes we're not familiar with what each other does on a daily basis. I think sometimes we do our own jobs for so long that we assume sometimes that everybody is aware of what we do day to day, and the reality is that that's not the case.

So from my perspective, I thought that the document's intention is fantastic, and I think that there's a lot of things in there that everybody, in principle, agrees on. But to define it, it sometimes may be necessary to just structure it from the perspective of public safety organizations, from the perspective of registrars and so forth.

I'll leave it at that and stop being so long-winded. Thanks.

FREIDA TALLON: Brian, next.

BRIAN CIMBOLIC: Yeah, Dirk, that's true, and I appreciate the fact that I may not be aware of the nuances of what goes into your day to day. When referrals come to me, I'm not privy to what the process is when that comes to me.

But similarly, there's a lot of nuance in, when registries get security threats, what goes into the analysis and the response time. For instance, if we got something under this framework – let's use the working definition that we have here – that is a domain-generating algorithm, there's not a chance that we're going to be able to remediate the threat within 24 hours because we have to go to ICANN and request, through an ERSR, a waiver to certain portions of our contracts with ICANN.

ICANN is timely, but we're not talking a matter of hours. It's usually a day turnaround, and then there's coordination with their backend providers; whereas, if a domain has a threat to life of another, that's something that we can quickly address. But what we can't have is a one-size-fits-all solution to a myriad of varied, varied problems.

I think that something to keep in mind is that, because this is a voluntary document, any registry that adopts it is necessarily going into it with good faith.

So I'd be hesitant to get overly prescriptive because anyone that's signing onto this is going into it with the right reason in

mind. If we say a 24-hour response time is, "Hey. We're looking into this. We promise we're going to investigate, and we're going to do what's right for everyone involved," I think that should be enough; that there should be trust in this process; that those registries that have signed onto this document are doing so with the best of intentions and are going to handle things in the right way.

FREIDA TALLON: Jim, here to my left, is ready for another comment.

JIM GALVIN: Thank you. I guess I have a quick clarifying question that'll shape the comment that I want to make. Do I understand that what you're reacting to is you want mitigation to have been completed within 24 hours, or are you saying something else?

[ROBYN]: I need to clarify the response first. Then we can come to the timeline.

JIM GALVIN: Okay. Then I guess I'm not certain that I understand what the comment is. The response says that the registry will investigate. So what would you prefer it to say that would meet your need?

[ROBYN]: The response, according to my point of view, can be categorized in several classifications, like first class, second class, third class. So, according to which class, was the response action. Then we can come to the timeline.

JIM GALVIN: Are you suggesting that you would prefer that we list the actions that the registry might take in response to this particular incident type?

[ROBYN]: Yes. I believe most of the registries already help a lot to mitigate the abuse of some security threats. We can just share the best practices here.

JIM GALVIN: Okay. Then I actually don't have a follow-up comment because that clarifies for me what we're talking about. We haven't talked about that in the drafting team. So I'll leave that for the moment. Thank you.

FREIDA TALLON: We have another question within the chat. The question is, "What about the registry lock problems to the domain enterprise?"

For anybody that doesn't know what the registry lock means, when you have a domain name that is locked with the registry, it's got an extra level of security.

To be fair, I think this question is an example of the additional requirements and the additional work that's necessary for any and all investigations. So if you are going to have a domain name that is registry-locked and you've got a request to review that or even have it taken down, I think the steps of that are then progressed as necessary.

But if anyone would like to jump in and add anything – literally when a registry lock is in place, it's going to take more than 24 hours. But the response would have been to the request of the law enforcement that, "This is actually the situation. This is what's happening." And it would be on a case-by-case basis for what the response would be.

Does that answer the question, [Robyn], and is there any additional information you need?

BRIAN CIMBOLIC: Just jumping back in the queue. To Jim's point, the registries haven't talked about SLAs around exact responses, and I don't know that I'm personally comfortable with an SLA on a particular response, just given the varied business models and size and staffing of registries.

Larger registries might be able to deal with something in a particular timeline. Then you might have a registry with ten people on their staff that, if something comes in on the weekend, aren't going to be able to execute the same response in the same manner.

I think the danger here is painting with too broad a brush. We have to come up with a framework that works for all-sized registries – ones that have thousands of domains, ones that have millions of domains. So just be cognizant of that. If we get overly prescriptive from an operational perspective, it just may not work.

JIM GALVIN: Just a clarifying comment. I apologize, Freida. Let me jump in the queue. Brian, I guess I want to clarify this because I think I heard something different than what you just said. You were talking about SLAs for actions. I thought heard that the request was just to have a list of best practice actions. We're not talking

about SLAs yet, and I just wanted to make that distinction and see if you agree or not.

BRIAN CIMBOLIC: You're right, Jim. That's a fair point. You're right. Beth?

BETH BACON: Along the lines of what Jim was saying (and also Dirk), I think what might be helpful – and it's not an SLA because I agree with the concerns there. Informationally, just as you were saying, we don't know what goes on behind the scenes before we get our e-mail that says, "Please take care of this," similarly you may not know what actions we might take and what the timeline might be associated with each of those different actions.

Now we've already noted where we're comfortable with the categorization of security incidents, so maybe we say high-priority – again, not as part of the document, but as an informational exchange so that we can all understand and be working from the same playbook and using the same terminology and understanding when we speak to one another.

High priority, just as you described, Brian, will sometimes involve going to ICANN and asking for a contract waiver for this for right now.

So if that's what I'm understanding that you're asking for, I think that that would be helpful as an informational education between both parties. But SLAs, I agree, would be a different discussion.

Thanks.

JASON PLOMP: On the timeline aspect, as [a part of] response, I think it would simply be… [It wouldn't be, "8It would take two days to do this for every registry, and so on and so forth."] It would be simple that, "Yes, we're looking into it and you can expect some sort of response within a certain timeframe for this information or that information." And that would be completely dependent upon what registry you're looking for. I realize it's not going to be the same for each registrar or registry.

On the categorization side, I was looking through the document, looking for some sort of criteria as to what exactly a Priority 1 or a Priority 2 would be so that we're all working off the same playbook so that, when I have a file as law enforcement, I know that what I perceive as a Priority 1 file – and I go to the registry – they're going to look at basically the same way so that we're not giving mixed messages in that I think something is high priority and you're saying, "No, it's not." I think that's an important piece as well so that we're all playing from the same playbook.

DENNIS CHANG: We have a hand raised. Alan, please go ahead.

ALAN WOODS: Thank you. Two comments on that. Just to add to what Brian has said and actually to talk about that and then what Jim had talked about as well. This is even going beyond the difference in registries and going to a difference in the TLDs as well.

I'm sure Freida can talk better to this, but let's remember as well that this document also covers things such as brand registries, which is a whole different level of response as well. It's a completely different type. So, again, we're trying to paint with a very broad brush in order to ensure that everybody is more encouraged to follow this document.

But I definitely hear what the PSWG are saying. It is difficult, I suppose. We've held the pen on this up to this point. I think that's the second point I'd like to make. Absolutely, if the PSWG thinks that there are areas that need changing and that there needs to be a difference in this, then we are a drafting team at the end of the day, so we need to put that wording into the document.

We need to propose that wording through the drafting process and we can discuss it as a drafting team. This is something that

formed, going back, that had turned into the PSWG and the registries, but let's bring it right back.

We are a singular team, a drafting team. We're all making this document. It's not the registries and then the PSWG pushing back. We are all part of this team. Can we get us all working on the document? Where you need more specificity, please put that into the document and let's discuss that. That's the only thing I can really think of to move this discussion along.

I think the way that's being discussed at the moment, if we're looking at timelines, overall, of the process, this is probably going to slow us down a bit. But I think it's probably worth it; that we just get everybody up to the place of the drafting at the moment. We will get through this.

BOBBY FLAIM: Hi there. Just a couple of things. One thing we've been talking about is adding specificity, but one of the things that we also did talk about in the PSWG was actually shortening this document greatly. I think there's a lot of language in here that actually is – I don't want to say "confusing," but it's unnecessary.

I think if it was to be a much more concise document that actually states exactly what it is, which we can say in one sentence – "This is a voluntary response of security threats" –

that would go a really, really long way in clarifying this document and making it a more productive document.

At the same time, we are arguing or discussing – I don't want to say "arguing" – some points of specificity, but more about clarification as well. So I think that is going to be helpful.

The other point I just wanted to make is that we are talking about responding to law enforcement, but this document is really not just for law enforcement. It's also for when the public makes a security threat/comment/complaint. And also for the registries internally. When they see things, how are they going to respond internally?

Now, I know Anitha, who unfortunately had to catch her flight back to the United States today – Anitha Ibrahim from the U.S. Department of Justice – actually did have an idea, when we were discussing last time. Maybe, on special circumstances, for law enforcement, there could be some type of law enforcement portal so that you would know when it's coming from law enforcement, whether they're verified law enforcement, or whatever.

And when we say "portal," that's obviously open to discussion as to how that would work. But maybe put something in the document to clarify what the source of the complaint is coming from.

So I just wanted to bring that into the discussion as well.

BRIAN CIMBOLIC: Rich, and then this lady here and then Maxim and then Beth. Rich?

RICHARD ROBERTO: I want to thank the law enforcement people here for bringing a little more awareness of the differentiation of roles. I think that's really important. One of those roles is registry – and we're here representing that role – and, although we are not law enforcement, we do cooperate with law enforcement. We're careful not to ever circumvent due process as part of that. It's something we're sensitive to.

But I'm a little bit confused about what the purpose of what this meeting is because I think when we started out – Thursday, I guess it was – we were very focused on the remaining aspects of the existing document that were redlined or were part of our discussion. I think we worked pretty hard on Friday in good faith to address those sections of the document.

We came here, I think, ready to move that part forward. But it seems like we've taken two or three steps backward now in process and haven't really discussed any of those. But we're

about now restructuring the whole document and questioning where some of the motivations are.

I'm just not sure where that's coming from and if this is ever really going to move forward in truth because, I think, if we, every few months, think we make progress and then decide to throw it all away and restructure the whole thing – I just don't know what we're doing here.

Thanks.

BRIAN CIMBOLIC: [Ma'am]?

LAUREEN KAPIN: Hi. I haven't been involved in this process from the ground up, so this is my outsider perspective. And I'm certainly sensitive to the previous comment about not wanting to reinvent the wheel and frustrations. I do want to say at the outset that, clearly, this has been a process that has been entered into and has taken a lot of time and, it sounds like, a lot of good faith efforts by the participants to try to come up with something.

When I put on, again, my consumer-protection, outside-perspective here, nevertheless, I do have concerns. From a big

picture, the first eighteen pages of this document really don't describe what the security response is going to be.

Instead, there is a huge amount of descriptions and emphasis on that this purely voluntary (which I think I definitely understand), that it's not new contractual requirements, that it's not binding, that there's no attempts to standardize the process, that there's no one-size-fits-all, and that it's to inform rather than prescribe.

So your whole first message is: "This is something that no one is necessarily going to need to follow." In terms of messaging from a public safety perspective, from a law enforcement perspective, it seems to me that that sends the wrong message.

I'm not saying that this should be a mandatory requirement or proscriptive, but what I am saying is that, if you're starting from the premise that this is voluntary, why not then have a document that gets right to the point and says, "From a best practices standpoint" – and here's a phrase I'm taking from the document – "here are some good, sound principles to follow," and then come up with principles where there is agreement between the folks on the drafting committee about what would be those best practices?

To me, that sends a message that reflects the good intent that I'm hearing in the room about what the best way to respond to security threats would be. Again, I'm mindful – I hear the

message loud and clear – that you can't treat a Verisign the same way you would treat a very small registry that has limited resources and different practical restraints.

But I still think, if you were going to build on the conversations that have happened but perhaps haven't happened enough about operationally what law enforcement may be concerned with in terms of the security threats identified – and it's prescribed; it's malware and botnets; there's very specific language in the implementation of the GAC advice and the contracts – and also have that conversation operationally with the registries, it strikes me that you can come up with something that's shorter and sends the message that these are best principles that we will aspire to.

If you're already starting from the premise that it's non-binding and it's voluntary, it seems to me that you can aim a little higher than what the document has.

But again, I want to emphasize that this is me from the outside. I'm not pretending to have been in this group. I'm just telling you as an outside reader who's focused on consumer protection: "Here's how it strikes me."

BRIAN CIMBOLIC: We have Alan, remote, who is in the queue. And then Maxim, Nick, and Beth.

UNIDENTIFIED FEMALE: And Mark.

BRIAN CIMBOLIC: And then Mark.

BRIAN CIMBOLIC: Okay, Alan. Take it away.

ALAN WOODS: Thank you. I'm definitely hearing what's being said. I just wanted to delineate it again. I'll try to put this delicately, as the last time I brought this up it went awry.

Something that was just brought up there by Bobby is if there are – sorry. It's four in the morning here so my brain doesn't work as fast. Okay. So we're talking about the entire spectrum of the security threat. We can't just think of looking at the law enforcement or public safety organizations. I absolutely agree on this, but again, we're straying back into this concept of the identification of the security threats.

Again, this security framework begins on how we respond to those that have been identified. The identification of the security threats and the verification of those particular – regardless of source: whether it's from law enforcement or from a member of the public or from our technical analysis – they're all part of the technical analysis under Spec 11.3b.

We have to draw a line here and say, "This is where we're assuming where going from." Something has been identified by the technical analysis. We're not defining what the technical analysis missed. We can't. We're straying into a different area here completely.

So we are saying, "We have an identified security threat. We are accepting that this is a security threat." Even at this point, I'm assuming we have accepted that it is a high priority or of the second level.

So I agree that there are definite conversations that need to be had there, but I don't think that these need to go necessarily into this document – the identification aspects.

The second point then is with regards to, I suppose, the best practices. We have tried to avoid use of "best practices" because of the wide subscription that we're hoping to go in this. But I definitely see merit in what you're saying. If we can put down a response to a certain type of threat – would usually be the

escalation to a registrar or the involvement of XYZ. Absolutely, I think we need to work on that then. But again, that is a drafting team matter.

I also had another point, but of course it's gone. But I think my main point at the moment is: let's please be very clear here that, if we start straying into the identification and the verification, we're going to get very bogged down in something that this document is not about.

I don't want us to go back to that. That conversation is being had in several other areas. The one that springs to mind, obviously, is the Spec 11.3b Advisory. Let's put our efforts into the verification and identification to this, and then let us take us take off the reins after that identification. That is the response. What is the response? How do we respond? And how do we get these issues mitigated? I suppose that's my point.

BOBBY FLAIM: I just wanted to respond to Richard's comment, and it's very duly noted. It looks like we're going back and forth and we're not making progress. But with the PSWG, we realize all the good intentions and the good faith of this group, myself included, going back and forth with telephone calls.

I just beg of the indulgence. We're trying… This is the first time that the PSWG has met with everyone. This document has been on e-mails that people have received, but due to the volume of ICANN – you've heard it a million times – we are trying to act in good faith.

We're just trying to make sure that, when the PSWG is going to put its name on it, it's just going to be as tight and we're all very comfortable with it and there won't be problems. And we are definitely moving closer. I don't think it's a desperate situation where it's going to last an eternity. We're getting a lot closer.

I know we're hearing a back and forth on certain points. That's unfortunately part of the struggle, but we're all trying to work in good faith and we're trying to get to the point that we have a document that is concise and says what it means to say. And hopefully…it will work out.

FREIDA TALLON: Richard to respond back.

RICHARD ROBERTO: I just want to respond to that just briefly. I think what happens in the meetings that I've been in… I've been doing this for a little over a year, I think; however long this has been going on. It seems like we make a little bit of progress but then someone

new shows up and says, “Well, I don’t understand how we got here.” So we go cyclically back and we start over again.

It would be useful if we captured all of the points that got us to where we are today so that we don’t need to redo that every time. I think some of the comments made by the consumer advocacy person, whose name I’ve forgotten –

[LAUREEN KAPIN]: Laureen.

RICHARD ROBERTO: Laureen – I think have been covered in previous meetings. I don’t know if we’ve gotten notes for those or if we’ve got some way to provide guidance on how we arrived at some of these negotiations.

Some of what we’re talking about is compromise, which means it’s probably not going to make everybody happy. And it may not be anybody who’s completely happy. But we’ll wind up with something that we think satisfies our original goals, which I think was to have something that is practical and useful. I think, if it happens to be aspirational, that’s great. But I don’t think that was the original set of goals.

That’s all. Thanks.

BRIAN CIMBOLIC: Maxim? Okay.

[MARK SVANCAREK]: I'm from Microsoft. I want to strongly second Laureen's comments about best practices. This is exactly what we've done in the Universal Acceptance Steering Group. We call them good practices instead of best practices.

We were in a situation where, in order to achieve "greater compatibility," some providers were actually violating the RFCs. So we got together and we started establishing: what are the good practices for these various things? It only took us about nine months to come to a consensus on that. Really, we had a decent consensus after six months.

Since then, we've been sharing that information and getting some traction on it. Now it's a year later and we've moved into the next stage, which is simply measuring and monitoring who is following the good practices. Where are the gaps?

On a case by case basis, we can establish what we should do about that. Should we change the good practices? Should we augment them? Or should we do something else? But at least we have something that is socialized and memorialized. It's a

fulcrum we can lean against. That seems to be working pretty well.

I think this group would benefit from something like that. It doesn't have to be this very same document. It could be an adjunct document. I think you would all benefit from an approach like that.

MAXIM ALZOBA: A few comments. The first comment is to your recommendation to follow the worldwide best practices. Unfortunately, it's not possible because, in your case, universal acceptance is about representing symbols and you don't have legal implications. You don't have law enforcement which accepts only requests in a particular language. You don't have to classify them to just do things like that because some practices from the United States could be applicable, for example, in Canada, to some degree – but not in China.

Since we're trying to create something which can be accepted at some level by registries worldwide, we have to avoid specificity on the level which actually makes it incompatible with the ideas from other countries.

So it's not about the technical side. It's about the legal and contractual side. In your group, you do not have such implications.

[MARK SVANCAREK]: Well, I still disagree. As an engineer who's worked for years with lawyers, I feel that specs and contracts are relatively the same thing. It's all code. [It's all, "Yes, yes."] Anything is possible in software.

MAXIM ALZOBA: Do you want a request from FSB, for example?

[MARK SVANCAREK]: Yeah?

MAXIM ALZOBA: Okay. I will let them know. The next note is about the idea of a law enforcement portal.

[MARK SVANCAREK]: Well, actually. I wasn't finished with my comment.

MAXIM ALZOBA: Sorry.

[MARK SVANCAREK]: If you're looking at things only from the lowest, most granular level, all you see are the differences. If you start from a different level, where you say, "When there are two jurisdictions of these types that conflict, here is a good practice for resolving them," you can make progress.

At some point, you will still have to deal with the very granular details, but at least you've established some sort of framework for discussing those differences. If you only start with the very granular differences, yeah, then it is hard to get anywhere. I do think that it would benefit this group to think about things in that way.

Try to think about things in a general way and attach the details to them, as opposed to thinking about all the generic details and then trying to establish larger principles from them. I think you'll die if you do that.

BRIAN CIMBOLIC: We have ten minutes left and we have folks in the queue. We have to keep moving. Nick?

NICK SHOREY: Thank you very much, Brian. Okay, I've got about five or six points. I will try to be succinct. First of all, thank you very much to the registries for your comments that you sent through to us the other day. We've had a brief opportunity to chat with them amongst individual members of the PSWG, and they framed the discussion that we had previously, whenever it was – Thursday? I'm losing counts of the days now.So thanks very much for those.

I think, to come to – sorry, is it Richard? Richard. Sorry. To come to your point around progress, I'm inclined to agree that there is a bit of back and forth, and I think Bobby spoke to that.

I think the reason for that is that there's been several phases, almost, to this work. I've been monitoring it throughout the process. One my government colleagues, John Flaherty, was the previous Co-Chair from the PSWG side. And there was Yasmin Omer, as well, on the registry side.

I think both of them leaving their positions around about March has led to a bit of a breakdown in the flow and momentum. It may be largely avoidable. Well, it's probably unavoidable, actually, is what I mean. But I think that's definitely been a factor, and there's been, with the new Chairs, understandably a bit of ride getting up to speed. So I think that's probably part of the course, but I understand that.

However, I've certainly found these meetings that we've had to be very useful. There's lots of stuff that I've taken away from the discussion earlier in the week and the discussion today – new elements that I need to go back home and do further investigation on.

There has been stuff, I think, that's come up today that some people have felt has been discussed previously. So I do think it would be probably worthwhile for everyone around this table to take some time, go away, and – Bobby recounted the history of this working group. It would be worth everyone reviewing all the documentation.

I don't know if that's something, Dennis, that you might be able to collate and circulate – if we've got a chart somewhere that explains this – because I think it would be useful. There are some ideas, I know, that were presented in the original document that John Flaherty prepared that speak to some of the ideas that people have been talking about around the table.

Some of the things that we were talking about today and that are on the registries' e-mail: first of all, the threat to life definition. In the U.K., we do have some guidance on this that was developed by the Association of Chief Police Officers – that's the overarching body – which talks about what threat to life is and so seems to define that.

So I will certainly go away and discuss that further in more detail with the two experts back at home to get, hopefully, some more detail that I can share with you guys from the U.K. side that hopefully might help to tighten up something on that.

On the clarification of response, just for the benefit of those who weren't in the previous meeting. I suggested that, in my view, when we were talking about that immediate 24-hour thing, I was favorable to a 24-hour response time with that top-tier category.

But that in each case, the minimum expectation of response is that the request be reviewed and the security threat be resolved within the agreed timeframe, or an action plan agreed between the registry and the requesting authority that will lead to the resolution of the security threat.

My reasoning for that is one of risk. When you're an operational manager in a law enforcement agency or a public sector authority and you're dealing with a threat to life issue, you need to be able to identify an action plan going forward that would enable you to ascertain the risk of relevant actions and then decide a course of action. So that was my reasoning for that. That's just for the benefit of this group.

But just to summarize overall, I think there has been good progress this week. Yeah, okay, we haven't solved the world, but

certainly for me, there's lots of stuff that I'm going to take back and do further research on and bring back into this group.

But I think it's also worthwhile for this group not fearing that we're maybe seeming to take a step back. I think there's a lot of information that has been discussed through the course of this drafting team effort over the last year that would be worth reviewing on both sides that will help us to cover off maybe some of the issues that we're discussing.

Thank you.

DENNIS CHANG: Excuse me for interrupting, but this is an open meeting and we have some questions. I know this topic is hot, so I did not interrupt. But we have two questions waiting and a comment and we have three minutes to go. How would you like to take these?

Okay. I'll read the first one from [Robyn] real quick. "How domains can monitor DNS records against attackers?"

BRIAN CIMBOLIC: I appreciate the question, but I think it's outside the scope of what we're talking about here. We're not talking about any particular measure.

DENNIS CHANG: Okay. Should I go on with the other question?

UNIDENTIFIED FEMALE: Yeah.

DENNIS CHANG: Okay. The second question is from Idris, and he's asking, "Is there a policy to prohibit the TTL value to be controlled by the registrant for the registries or registrars to avoid abuse of DNS with the known threats like fast flux, double fast flux, and so on?"

BRIAN CIMBOLIC: Again, appreciate the comment, but it's outside the scope of what we're talking about here.

Next in the queue we have Beth and Jim. And then, if there's time, I'll jump in. But I don't think there is – oh. Alan can go before me. Beth?

BETH BACON: I have one question, 32 parts.

[laughter]

Just kidding. I recognize we have very limited time, and I want to echo a lot of what Nick said. When we end these meetings every time, we are so much closer together than we are far apart. I think that that's something that we should keep in mind.

I think, Nick, what you said, you actually responded to… We tried really hard to be concrete, and you gave us some really concrete actions on your part. You're going to take it back and look at it. I think it's wonderful that we have so many of the PSWG here so we can hear your ideas and we can respond to those.

But I think, as we wrap this up, we need a constructive next step, which might be the PSWG taking a look at what we've sent and then taking a look at the document. If there are things where you say you would like us to also include, "A human has received this. We are investigating it. We agree it's a high priority, so we will respond to you in 24-hours."

If that's something that will push you over the edge of happiness, then let us know. We can talk about it and talk about it. I think it's super helpful and I actually find it incredibly interesting to learn more about what your needs are, but I think we need to start writing it down and moving along.

Thanks.

BRIAN CIMBOLIC: Jim?

JIM GALVIN: Thank you. I want to make a specific suggestion. Coming back around to the original question of what the good practices are as opposed to best for registries, it occurs to me–

I want to categorize that question in a different way because I think the sticking point is not what actions a registry could take. Frankly, the actual actions a registry would take are really quite limited. I've got four that I can think of off the top of my head that we could probably agree to.

You can remove the name from the zone, you can redirect it, you can refer it, or you can block – if you're talking about names that are coming in the future. So that isn't really the sticking point.

The sticking point is the verification step. The sticking point is that there's just no way to completely time-bound what it takes to review the evidence that's presented in the request to take some action. It's hard for the response to do more than say, "Yes, we agree with you that this is high priority and we're investigating, which means we're actually confirming that we agree with the evidence that you gave us."

The largest part of that analysis is the legal review of whether or not it's okay for us to go do that and what it means to go do it. I think that really is the answer to your question in terms of actions. There's no way to prescribe or even describe in any significant way happens in that legal analysis. Every case is different. Whatever evidence you present is just different. We have to figure out what to do with that.

Anyway, thank you.

BRIAN CIMBOLIC: Thanks, Jim. Excellent point. From where I sit, you hit the nail on the head. Alan?

ALAN WOODS: Very quickly, thank you again for the great discussion today as well. Beth, it would appear, has a psychic connection to Ireland at the moment because she said everything I wanted to say. I just wanted to add one extra thing at the end there, saying that, at times during the drafting group calls, we are prone to deafening silence.

Today, we have heard the complete opposite of that. I want, and I think we should all strive to have a lot more of this chat and discussion during the phone calls because, without this discussion, we're not going to move forward.

So it has been positive in that sense. I look forward to seeing where we go as long as we have something concrete to run with going forward.

FREIDA TALLON: Great. Thank you, everybody, for attending today. Next step: Bobby will be speaking with the PSWG and then will come back and review on our next call.

BOBBY FLAIM: Okay. Thank you, Freida. I think for the PSWG next steps we're going to look at the latest document that Alan has proposed. We will go through it very thoroughly and then we will, I guess, give our input on that last document. So that is our only next step.

BRIAN CIMBOLIC: Real quick, Bobby. If you could also, in that review, factor in the seven bullet points that we provided. If I could add one caveat to that, it would be the excellent point Jim brought up, which is what registries can actually do. We have very limited options to respond to security threats, so I think that should help frame the discussion.

BOBBY FLAIM: Totally agree. We will add those steps, and I think what Jim said actually was very, very good and should be part of the document.

DENNIS CHANG: Thank you, everyone, for joining. Just one point of clarification and a reminder. This has been an open public session, and therefore we fully expect to get some outside first timers' views. So that's okay. We all learning from that.

We do have working group sessions for members only where we do talk with the people who have been working together. The next meeting with be an online call, and we will schedule it when Bobby says he's ready. Correct?

Thank you all. Bye-bye.

**[END OF TRANSCRIPTION]**