
RECORDED VOICE: This meeting is now being recorded.

FABIEN BETREMIEUX: Good morning, good afternoon, good evening everyone. Welcome to the meeting of our security framework drafting team, on Thursday the 14th of January 2016. My name is Fabien Betremieux, with the Global Domains Division of ICANN.

As a reminder, before we jump into our agenda discussion today, to make sure you mute your line if you're not speaking. The meeting is recording and will be transcribed. For the purpose of the transcript, please don't forget to state your name when you speak. And finally, if at any time you would like to get into the queue to speak, please do so by raising your hand in the Adobe Connect room.

Before we get to the agenda, I just wanted to mention that Yasmin Omer will not be able to make the call today. And I understand that Crystal [inaudible] will be filling in the role of the registry co-chair for this meeting. Can you confirm Crystal?

Crystal are you with us?

CRYSTAL: Yes, just having a hard time...

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.

FABIEN BETREMIEUX:

We heard you for a few words here. Okay maybe you can type in the chat as well. I'll just get going with the presentation of our agenda, and hopefully we can hear you again. So in terms of the agenda, this call will mainly be focused on a presentation and discussion of the [inaudible] feedback on the first draft framework by the registries.

And we will make sure that we will keep some time at the end of our meeting to discuss our timeline and next steps. So without further ado, I propose that I leave the floor to you John, and I will make sure that you can use the document if you would like to take us through the comments of the [inaudible]. So let me stop here, give you the floor, and let me know if you need anything from us in terms of support from your discussion of your input.

JONATHAN FLAHERTY:

Thanks Fabien. Hi everybody. So, I'm just, yeah, it looks like I've got a handle on the document there. So just to introduce... Just to bring everybody up-to-date from the [inaudible] and just before Christmas, we got the registry and registrar written draft document, overall very happy with that to date really.

Before Christmas and after Christmas, I asked for, received, and collated different comments from the group against that document. And that's what is on the screen today really. I've got 30 comments for you in that document, which sounds like a hell of a lot of feedback. On the face of it, it's not actually that bad in terms of volume.

A lot of the comments that I'm going to go through, I've tried to separate them out into the following categories. Most of them are

rewordings. You could probably expect 30 of the 30 comments to relate to that, maybe a rephrase or a rewording. Some of the comments will start with the word consideration.

That's probably more for review and a bigger ask than the [inaudible] registry and registrars to draw out a bit more of the feedback. For example, consideration comments are going to be more about moving or expanding text, excuse me. Phone going off. Linking paradox, making something, some section.

So I'll explain a little bit more for that as we go along. Following this piece of feedback, we do have a meeting as a group in Brussels, on the 28th of January. We're going to see quite a lot more European Union GAC representatives at that meeting. And it might be that I come back with some more feedback.

I'm not sure I'm going to get a lot, but there is more attempts at getting government feedback there rather than public safety employees, who have given the majority of the feedback so far. So I'll just open up with the [inaudible] document. The first comment. Again, it's just [inaudible] to include the word monitor. For those monitor and respond to security threats.

We just thought that would be better to put in place at the start to define exactly what the framework should be. It's a response to threats, and quite a proactive monitoring by intelligence feeds, which [inaudible] put in the document as well that needs to be better reflected in the title.

And it also reflects paragraph via spec 11.

FABIEN BETREMIEUX: John, if I may interrupt? Yes, I can hear you very well. I just want to mention that Jim has raised his hand. Maybe this is related to your introduction. So do you mind if we ask Jim to ask his question?

JONATHAN FLAHERTY: Yeah, I mean, there is 30 comments so it might be better if we go along. That's no problem.

FABIEN BETREMIEUX: Okay. Jim, would you like to go ahead?

JIM GALVIN: My comment is about, yes please. My comment is about the suggested change here. So if Jonathan wants to finish his thought and explanation first, that would be fine. Thank you.

JONATHAN FLAHERTY: Yeah, Jim, that was literally it from me. I wasn't going to add too much more to that, so you can go ahead if you want.

JIM GALVIN: Okay, thank you. So Jim Galvin for the transcript. I don't feel very strongly about this, but I did want to at least say it out loud once. You know, I think monitor, to me, says more than periodic analysis. And that may just be a little bit of nit-picky wordsmithing, but you know,

insertion of the word monitor just sort of struck me as being a little more active, and more engagement on the part of, more than just saying periodic analysis.

So I'm not sure I agree with the idea that those are equivalent terms. I actually don't have a, you know, a good substitute, expect maybe just to go back to, you know, saying for analysis and response. But I put that comment out there to see if it garners any other support from anyone. If no one else is interested or concerned about it, then I'm fine with it and we can move on. Thank you.

JONATHAN FLAHERTY:

Thanks Jim. Yeah, I'm trying to rack my brains for a different wording, and I'm... Yeah, nothing is springing to my mind at the minute. I just felt something needed to be, to make it as proactive as reactionary. Just to outline that it's maybe more than a request or a response, because there is something in terms of monitoring or a different word, going on at the gTLD when requests are coming in for, you know, a PSWG request or something else.

So perhaps we can take that back to the groups?

FABIEN BETREMIEUX:

This is Fabien speaking. I just want to remind the drafting team that as we've mentioned on previous calls, there is a parallel effort on going regarding this specific section 3B of spec 11, which relates to an analysis and reporting on security threats. So I just want to mention it out there and as we said before, those two elements are ongoing in parallel.

So this is why for now, the title of the document has been, the framework for registry operators to respond to security threats. I just want to remind that to everybody.

JONATHAN FLAHERTY: So, I'll be happy to go on to comment two, and we can maybe create an action for that past the conference call. [CROSSTALK]

JIM GALVIN: ...apologize for jumping in. It was a new hand there, so I apologize for jumping in. So Jim Galvin again for the transcript. [Inaudible] proposed in the chatroom, and I just wanted to restate more clearly what I said in my comment. I would prefer something like to analyze and respond to threats, as opposed to monitor and respond. That, you know, at least suggests the action without also suggesting a particular frequency.

And then I also wanted to note in the chatroom that there is at least a little bit of tacit support for changing monitor out. Thank you.

JONATHAN FLAHERTY: Thanks Jim. I've just got one off the top of my head. How about the word protect? To protect and respond to security threats, something like that. Would that be more of an overarching phrase in terms of, you know, grant protection? And part of that behind the scenes in technical analysis can mean a number of different things, per registry, per frequency period. Something like that?

FABIEN BETREMIEUX: John, while we monitor the chat for a response here, question. We have Crystal in the queue. Crystal?

CRYSTAL: I just wanted to make it clear that the registry [inaudible] haven't, we've all received this, and I think a lot of us have reviewed the comments, but we haven't had a chance ourselves to get together and talk about it. So while this is a great forum for us to have a conversation about it, I'm not sure we are going to come to, you know, the exact wording on every situation in this call, at this time, especially because Yasmin is not on as well.

So just putting that out there as backdrop for this conversation.

JONATHAN FLAHERTY: Yeah, no problem for me. Okay, so we'll agree to review that post-call. Just bear with me one second.

So just moving onto comments two and three. Sorry about, I've got a really bad mouse here.

And these relate to the introduction. Again, it's just an expansion, I think, of GAC advice here in comments two and three. And just to add, and reflect some of the things in the document really that the creation of this agreement and the GAC advice, and the community's role leading up to this.

Whatever we propose in this framework is grounded as well in detail, these policies. And the initial GAC advice was an addition to Yasmin's

introduction paragraph. So they read from, as the old number of safeguards are still applicable and subject to contractual oversight.

And just at the end of that paragraph, where the registry operator identifies risks that pose an actual risk, notify the relevant registrar and/or suspend the domain name in question. So we kind of run in some action on the end of that paragraph there. And grounded in the TLD policies in [inaudible].

So again, there are a couple of raised hands. I think Jim has got a new one, and Maxim, and I mean, I can take them now or if you want to do them post-call. I'll take them now, Fabien, if that's okay?

FABIEN BETREMIEUX:

Please, please, yes, Jim. Go ahead please.

JIM GALVIN:

Thank you. Jim Galvin for the transcript. Just a quick comment. I'm always cautious when I see [inaudible] suspend the domain name in question, and it appears without any apparent qualifications. I mean, I'd be much more comfortable with that addition if there were a qualifier, if appropriate. Because otherwise, it always looks too much like you have two choices here.

Tell the registrar or suspend it. And, you know, or tell the registrar and suspend it. And it feels like you're limiting your actions. So if you don't have that qualifier, if appropriate, it always makes me suspicious and cautious.

I realize this is just the background, so it's not that big of a deal, but nonetheless, you know, it jumps out at me. Thank you.

JONATHAN FLAHERTY: Yeah. It's John Flaherty. I do agree with that. I think that's a good comment.

FABIEN BETREMIEUX: Thank you. Maxim?

MAXIM ALZOBA: Hello, Maxim Alzoba for the record. My question is about the, thus stated on this page, and the subject to contract to the other side. Actually, it's not decided yet. I think we need to remove this wording right now, because these documents is non-obligatory for the registries, and adding this to the text makes the reader think that it's not a question. They have to do it because of contractual obligation. And it's not correct, I think. Thanks.

JONATHAN FLAHERTY: Okay. It's John Flaherty again. I'm going to send that back to my group and then review that. [Inaudible] comments. The spirit of this document is that it isn't contractual. We understand that. So it may be that that's renewed, we again just like to monitor comment, you know. We look at play on words as appropriate for both groups.

I see that Maxim still has his hand up. I'm going to move onto the next comment [inaudible].

FABIEN BETREMIEUX: Alan in the queue.

ALAN: I just wanted to say, I'm [inaudible] registry. Just on that point there, I think you're just putting in extra [inaudible] to what the GAC had advised in that context. I don't really see a huge issue with it, it's just adding to the record what was said, I think that adding contractual obligations in there.

So I just want to say that I think it's just an addition and a reflection of the record. Is that what you meant Jonathan?

JONATHAN FLAHERTY: Yeah. I think what Yasmin, Alan, I think she has probably copied that from another document and omitted some of that, which it does lead to more PSWG strengths in that paragraph. So that's where it kind of got picked up. Now it's literally talking in that context, not actually saying this is the way the document is going to work.

Just because it's the introductory paragraph, to give you a background of where it came from. And...

ALAN: ...my thoughts. Yeah. Thanks.

JONATHAN FLAHERTY:

Okay. So if it's okay, I'm going to move on to 1.4.3, which is partly the introduction and just some comments and feedback on the best practice paragraph. We thought this paragraph was a little bit negative and didn't accentuate the positive of what a framework is or could become. So the wording of that was a list of what the framework wasn't intended to be, rather than what it could be.

So yeah, I think... I'm not sure. The [inaudible] registries in affecting and work [inaudible] referring to security to the relevant parties to resolve. Followed by, just going on to comment five. Then a quite important comment, this doesn't mean that it is a nonbinding investigation principle.

So it's a framework that has a policy development, rather than, I don't know, a registry pitch that the framework isn't there, it's not that, it's not intended to do that. It didn't read well for us at the start of the document. It was kind of, it was a bit too defensive rather than open and transparent forums. And we are omitted a bit of that text. We like you to look at the wording there. [Inaudible]

Just to see if you're happy with how that is written. It has still got, you know, the NomCom contractual and the limits of what the framework purports to be as well. But we just wanted to revise a bit of that text to make it sound a bit more positive.

I'm not seeing any hands, Fabien.

FABIEN BETREMIEUX: There is support expressed in the chat, but no hands raised. So we could probably move on...

JONATHAN FLAHERTY: ...don't say that for myself. You've had the feedback for a few days. If there is something strong that you think we deleted, I know you won't hesitate to come forward on that [inaudible] anyway.

Comment number six. Yeah, it's just an insertion and a rewording really or a rephrase. The registry operators 3.2, about the option of using the intelligence feeds, or having their own depending on the site that you're registering. So registry operators depending on the variables applicable to a new gTLD are encouraged to use repeatable and trusted, public and/or private data feeds to identify threats in the TLD.

So we changed the word may to encourage to use. It's not a big one for us, but we're just expanding on the document there, just to give a bit more insight in terms of the openness of what you could use. You know, you may have those already in terms of [inaudible]. You may have different monitoring capabilities. I'm trying to think of a different word than [inaudible], but I couldn't.

So that pretty much a low level comment, number six, from the [inaudible].

Okay.

So I'll just carry on moving down the document. Comment seven. This will [inaudible] a little bit more discussion. This particular feedback I'm quite strong on, from a [inaudible] investigation perspective. The

technical analysis on 3.2.3 of the document, should be bigger than two lines in the framework.

I think it necessitates, so sorry. My connection has just dropped.

Just bear with me one second.

Sorry about that folks.

So, in terms of a section [inaudible], the response section [inaudible], and the subparagraphs of accuracy, [inaudible]... Is it possible to considerate for the group that a, we make alternate analysis its own section, and b we look at the same subparagraphs in expanding our from that a little bit more, without being prescriptive?

I know [after we finish] all of this, it's going to be difficult to do. But maybe at the very least, just a paragraph to make it bigger in terms of a priority for registries. I think in terms of protecting or I'm going to have to say again monitoring TLD, that expansion and perhaps something in an annex or an appendix in terms of a generic example, would suit the PSWG and the GAC there.

You know, what kind of technical analysis in terms of [inaudible] that? I don't think it needs that, but maybe the same subheadings. Anybody from, I don't know, a backend registry, for example, a Google, a VeriSign, an Affilias, or a new style that maybe could take control of that, and put something that already goes on in that. Have you got that written down somewhere else in terms of how you [inaudible]?

You know, some [inaudible] already serves that purpose. Do you have a policy expert that equals, that could maybe review to put in? So

Richard Roberto with Google with your hand up. Richard, do you want to go ahead and speak?

RICHARD ROBERTO: Yeah, hi. Richard Roberto from Google. So I think one of the reasons this... I don't know if you guys can hear me or not. But one of the reasons why I don't think this has a lot of [inaudible] behind it is, I don't know that personally that we value Google, speaking about Google, automated analysis over any other form of signal, and the focus for us is on what do we do once we're aware of abuse?

And automated analysis, I think, is just one of the methods we may become aware of abuse, and I think that, I don't know personally if there is a lot of value in overprescribing this section, but it's just not [inaudible].

JONATHAN FLAHERTY: Okay. Any other comments on that one? None so far. Can we review that post-call? [Inaudible] something in writing from the co-chairs.

FABIEN BETREMIEUX: John, this is Fabien. We'll make a note.

JONATHAN FLAHERTY: Okay. Thanks Fabien. Just moving on to section, comment number eight, section 3.3, data analysis. What we're looking into now is this point is going to be probably repeated if you've read the feedback, and

it's relating to the need to insert a timeframe and a timescale for response, on receipt of a threat. So it's coming in on data analysis. It does appear a couple of more times where a timeframe is alluded to throughout the document.

And we don't manage or carry out any technical analysis of a TLD as public safety officers. From our side of the fence, that in terms of a variety of crime sites, and the lifetime of a domain, is probably being abused before it's dropped. We felt that one day, in terms of a receipt of a threat to get a response was appropriate. Again, there is different [inaudible] registries in the room.

You may have a quicker response in terms of existing security mitigation. That was what we thought was a balanced timeframe. So again, we, you know, have a look at that, possibly post-call. We'll make a note of that. If you want some [inaudible] for this on why we want that, if you want more answers, I'm sure we can come up with that for you.

We just felt the need just to document a timeframe there. Indeed, the word should be conducted as well. You know, it's not mostly conducted. It might be difficult for 24 hours for some registries, it might be easier under 24 hours. So again, we have to be a little bit prescriptive by getting some kind of time response.

Okay. I'm just looking at the text as well from Maxim.

Yeah, [inaudible]... So have a review of that. And try to put something together in writing to feedback like back as a group. What's practical and what comes through in terms of cost and resource and response?

Richard is still typing.

Yeah, Richard, I'm just going to leave [inaudible]... on that comment in terms of definitions of abuse and what's malicious. I'll probably leave that to the end, if that's okay. Maybe we can have a separate discussion about that at the end of my comment.

Comment number nine is 3.3.1 relevance. And again, it's a play on words again. A registry operator may receive security threat information relevant to that TLD. And instead of this review, may include verification of domain names involved with the threat, being within the TLD. We change that to should. I think that's quite self-explanatory really.

It [inaudible]... You should know your own TLD really, shouldn't you? And then the rest of the paragraph reads okay from where we stand. Okay. 3.3.2, accuracy. Registry operators and registrants, when reviewing the accuracy of reports regarding their submissions, probably subject to that technical analysis an automated response.

And just picking up from probably Maxim's point that if a registry operator is struggling, if there is an expertise issue, maybe even a cost issue, to respond to that threat. Yasmin has put in that request, and it might be a referral opportunity to a relevant law enforcement agency threat investigation follow-up.

And that's been pretty well respond, or we just put in comment [inaudible]. Again, it's just making it public safety working group friendly. So referring to your local public safety or law enforcement agency. I'm going to raise that one in Brussels, just to let you know, and

you probably do, that some law enforcement, some public safety agencies, might be more advanced than others in being able to take that referral along.

So that's a good idea, and the responsibility on our part is to organize ourselves and to help you there. So I think me and Bobby are going to talk about that one in Brussels. We'll have more feedback for you on that in time.

I'm just going to move on. Comment number 11. Yeah, it's the longer comment box with the consideration element again, concerns 3.7. Report on your activity, and your response to security threats. So that for the paragraph, the paragraph there includes some [inaudible] requirements in terms of gTLD reporting and risk profiling.

And you see quite right there, the reports may include a number of metrics and performance indicators. But again, non-contractually binding, which we'll totally accept as well. So this is insight into threat intelligence. Both the reporting maybe [inaudible] circles [inaudible] and LE agencies, who are very keen on understanding threat intelligence and seeing how we can combat there, and how we can look from what you're seeing at the [inaudible] in our investigations and prepare better for our response as well.

So it was a consideration of linking that perhaps to technical analysis. Technical analysis, I think, is going to follow trends, and patterns, and metrics that link to reporting on them as well. And you may have sharable threat intelligence that we benefit from. So the comment there is expanding on or linking to technical analysis section report on

action. There is also something later on in the document, in section 5.5 where you mention the expedited registered security request process, in order for ICANN and the wider community to be engaged when the registry puts in [inaudible] about a potential threat to the community.

That one was really interesting for me. I think that could maybe link into here in terms of [inaudible] part of your reporting. If you're analyzing and you're seeing something that needs to be, needs to be collated, needs to be shared, and this section 5.5 link better as a result, then section 3.7, or should it be separate?

So this probably... I've got Crystal with her hand up. It might be one to take back post-call. The example that I've thrown up there is engaging the SSAC and the CSWG any new threat. I'm using 5.5, that expedited process, to make it work quick and we can all review and respond to that.

Crystal, do you want to go ahead and speak?

CRYSTAL:

Hi. Just before jumping on this one, I just wanted to comment. Maxim, myself, and Stephanie all made comments about the particular groups or agencies that the public safety working group thinks does a good job and thinks that we registries could use as a resource that we mentioned. There is the willingness of you guys to compile a list of some sort for resources for registries, that would be very helpful, and something perhaps we can include here.

And then regarding this comment, I think there is just a different definition of report. I think a lot of us, when we drafted this, thought report was the report that we have to give to ICANN under good contract, and I think that's slightly different than the reporting on security threats that you're talking about here, which is why it's separated in our document.

That's definitely something I should take back and think about. And I think there is obviously a huge benefit in sharing information between all the various groups. What that looks like, ultimately, I think we should talk about, but I think this is a good comment, and we can [inaudible].

JONATHAN FLAHERTY: Yeah. Okay I've got both points down there. Thanks Crystal. Okay, I'm going to move on to the next comment.

FABIEN BETREMIEUX: John, before we scroll down to your next comment, can I make a suggestion that we try to focus the discussion on the most significant comments? So that we can keep maybe five, 10 minutes at the end of the call to discuss next steps as well as our timeline. Would you mind?

JONATHAN FLAHERTY: Yeah, no problem. So [inaudible]... comment we're expanding to public safety. Comment 13, yeah, agree with 4.3. Any response grounded in the TLD policy. We think there should be more reference potentially two types of policies. They will be grounded in. So there is some

continuity there. We know what we can expect you to be relying on behind that framework.

Comment 14, Fabien please.

Yeah, it's much the same. Again, quoting consistent TLD policy. Maybe registry agreement sections as well. I just list one though, and the registry/registrar agreement has the right to deny [inaudible] domain names, protection measure.

And there is also another one there. The new gTLD registry agreement, that paragraph. Okay. Comment 15, section 4.4, [inaudible] responses. This is again, a continuation of the 24 hour response to the GAC. And we've inserted that some of the reasons why we feel the 24 hour is needed.

And again, probably registry review post-call on that one. Comment 15, again, within 24 hours. Have a review of that post-call as a whole. [Inaudible] 24 hours on any, on both the response, [inaudible] by the way. You know, we were trying to make it as consistent as possible for you.

Comment 17.

So we've added the word malicious talks about, we've add the word severe threat. And the definitions of abuse. I've asked around the community here, I'm struggling on this one. I know the registries were looking at that as well. So maybe Fabien, that's the five or 10 minutes at the end to talk about that.

And so we're no further forward on the [inaudible] on that. Obviously, through Brussels, but for more definition debate. Comment 18.

Yeah. Appropriate actions, where we move into... [Inaudible]

I think any response ultimately, I think the document later on talks about a registry intervention when we have a nonresponsive registrar, we just, at the beginning of this section, we just wanted to quote in the framework, again if appropriate, registry [inaudible] should take all actions appropriate, if other parties in the chain of ownership are not responding to a security gap.

Comment 19.

[Inaudible]

Sorry, sorry, the other way. Go down a little there.

Just going to [inaudible]...

Yeah, that's fine. So, we felt this might be better inserting into best practice into the introduction part of the document, where you know, when we're setting up professional standards, limitations to the framework but also, this is the overall standard, and the people [inaudible] end of, and are doing all they can. And registries, registrars are all set to purpose, you all are acting in spirit in the same way.

So potential to [inaudible] and move that one to section 1.43 best practice. Comment number 20.

Yeah. So, this is probably pretty significant but for the PSWG and the GAC. But if we do have an incident of registry intervention response to a threat, and another party has to have a poor response, I think we owe it to ourselves to report them somewhere on that, [for me?] to [help on?] compliance.

And maybe of course a legitimate reason why that didn't happen, and I think we need to do be very mindful of that. You know, [inaudible]... And so again, probably more meat on that. There might be a history or a response that necessitates that that happens. Just coming up that last point, you know, if they're not doing it [inaudible] at some point, it might be worth naming and shaming them.

And ultimately that costs a registry time, and I think as Maxim would rightly state, if cost is such an issue, you can't afford to be let down by a registrant in the overall response to the threat. And so we thought you'd be interested in supporting that. [Inaudible] Maxine?

MAXIM ALZOPA:

Maxim Alzoba for the record. Actually, about 5.1. We might include something about interference with the actions of law enforcement. If they have some kind of investigation in place, we should not want to interfere.

For example, they do something to find some party doing something, and it should be added as the reason for not [inaudible] if such an investigation interferes with the law enforcement investigation, for example. Or something like that.

JONATHAN FLAHERTY: Yeah, okay. That's noted.

Okay, thanks very much. Alan?

ALAN: Yes, just on... Well, Alan [inaudible]... Another issue I have there is the wording that you're using there, it would suggest that we have a lot more expertise. As much as I would love to claim that I would know when I could negatively impact prevention mitigation or termination, you know there is not that level of expertise. I think it's probably a little bit too much to put that in, just purely because you're kind of expecting a lot there.

And that's why it was remaining at a bit more of a higher level, as not to kind of put it into that box where we're putting ourselves out there as being experts in that field. So I would just [inaudible].

JONATHAN FLAHERTY: No problem. Yeah, I'm just noting that Alan, thanks very much.

ALAN: Thanks.

JONATHAN FLAHERTY: Okay, Richard, would you like to speak?

RICHARD ROBERTO: Hi. Richard Roberto from Google. Yeah, just more on this. Again, I know you want to postpone the discussion on malicious, but I think it's very key to this whole section you just added in here. And I just wonder why correct party doesn't automatically imply not the correct party, which is what you're describing in a matter that I don't think is necessary, especially with respect to the term malicious.

I kind of know how you can avoid discussing if this keeps showing up.

JONATHAN FLAHERTY: Okay, no problem. So we're going to have that [inaudible] at the end. Currently [inaudible] is going to probably keep occurring to be honest. In fact, if I move on to comment 21, it's in there again. [Inaudible] stemming from, it might be my language, it might be cybercrime kind of language, yeah just comment 21. Registry operators ensure relevant malicious [inaudible] identified and kept current.

So [inaudible] and I mean, without going off piece or on a tangent, has anybody got an alternative to the word malicious?

Yeah [inaudible].

FABIEN BETREMIEUX: John, I see Robert, sorry. Richard is on the line. Richard, would you like to go ahead?

RICHARD: Yeah, sort of dominate this conversation about malicious. I just don't know why we care if the side effect of some condition is [inaudible] versus [inaudible] versus ignorance. And I think the condition we're talking about that's infallible is abuse. It's not necessarily malice or [inaudible]. Why do we bother [inaudible]?

FABIEN BETREMIEUX: John, are you still with us?

JONATHAN FLAHERTY: Yeah. So I'm sorry, I'm just reading the text. The [inaudible] registries [like?] abusive, and some registries are [like?] malicious, in the text from what I'm reading. So I don't think we're going to get through this tonight. Can we take that away and maybe other notes...? Can we get the mailing list [inaudible] this week, Fabien, maybe with some people putting some comments in?

FABIEN BETREMIEUX: Absolutely, sure. Can I just remind you that we are at the 10 minutes left mark? Just to let you know.

JONATHAN FLAHERTY: Just one quick comment. I don't think we're really strong on the word malicious, if it was given that impression. I mean, abusive seems fine to me. But we do want that general consensus. I think it's just a kind of phrase of what we used to talking about in terms of cybercrime, I think, and just [inaudible] there in the document.

So we'll probably [inaudible] as a group in terms of the right definition in. And [inaudible]... Yeah, notifications. I'm sure they're going to be written anyway. [Inaudible] said that that [inaudible] all of the responses that you do. Again, it's self-explanatory. And so comment 23. Yeah, skip that if I can Fabien, that's another 24 hours response.

And yeah, [inaudible] a response in 24. Comment 25. Limited direct contact with resellers and [inaudible]. We totally understand that as a group. And when you are potentially intervening, or responding in any way to [inaudible], the work comes down to what we thought, again, you know, this might start the debate off, but we wanted in terms of responding and mitigating, you might get some technical analysis that reduces the up time to abuse before the name goes back to, [inaudible] domain subject, domain shadowing.

You can spot that in your TLD before something goes live. So again, we thought that was a kind of a relevant comment to put in the rationale behind there, how you deal with a request. And comment number 26. Just bear with me one second.

Again, I take [inaudible] comments on board. I might go back and review comment 26 a little bit more, it should be grounded in the registrar policy. And in terms of the outcome of compliance review, when and where to report, we probably need more details on that. And in terms of that infrequency and reporting what to whom.

Comment number 27. Fine. Yeah. So ignore... Malicious conduct [inaudible]... in that, so I'm not going to worry about that for now. It was just the point of the comment, when you're talking about some of

the processes, some of the responses, we wouldn't mind an annex with some of those examples. The reason being, if [inaudible] and LE members read this framework, it means absolutely nothing to them in the form that it's in at the moment, but a registry and a registrar will totally understand it.

A referring agency, who is on the end of a registry referral, without an appendix, without a better insight, if they're just looking at a generic framework document, I'm not sure they'll know how to react. So we might need some abuse best practice. I've noted in the unified registrar approaches to this, it's a document that the registrars use, I think, for some case studies.

I'm pretty sure Theo is on the line, so perhaps the registries can do the same in this document as a pointer, and because the intention might be that this document goes to non-ICANN reps and working group members. So could you talk a little bit more about them in an appendix [inaudible] and traditional type of response?

Moving on to comment 28. Again, really, some kind of process, a diagram. I don't know if you can do a flow chart, if you have one. Would be good for us in our wider community in understanding the role of the registry and actions taken. Comment 29.

What's interesting for me on this, in terms of cybercrime, is again, the prevent aspect. I'd like the consideration in terms of both the response to security threats and a little bit more of the content in the framework on security standards and implementing RFC standards like [D MARK] [inaudible] and [SPF].

I know Inspect Six is the registry agreement. You've already signed the agreement to say that you'll sign the domain names would be a [inaudible] in your respective zones. I'd been keen on some more protocols there that potentially can help to combat spam and email security. [Inaudible] market is a big driver for me on that.

I'm not going to pretend to be a technical expert on that. There may be pros and cons, not to sign every domain off with [D mark]. Again, there is much more we can do with this framework. The reality for me is if you do more before domain goes [inaudible], and it's not, it hasn't got a bad reputation [inaudible], you know, you might create less responsive work for yourselves if some security measures, pre-shipping of the domain before wholesale to a registrar, are in place.

And I think DNSSEC specs is a really good idea. I know DNSSEC isn't exactly 100% implemented at the moment, and I'm reading the browsers don't always have the capability to authenticate some domains. But particularly, framework is a long-term one. And it may be more relevant in the future.

And again, you may have any existing registry practice. I think Afiliis, has a one click DNSSEC option, and maybe, I don't know if you're into any comments, but it looks like you're doing that already, which we would encourage for such provisions to then go into the framework.

Comment number 30, last one. If we do expand on technical analysis, we'll probably [inaudible] depending on your feedback, would you prefer to give examples of these technical analysis? If you think that's too prescriptive, that it's nailing you down a little bit, and you know, it

doesn't marry in between what registry A could do and registry B cannot do, then by all means, give me that kind of feedback and we'll take that onboard.

Okay. Stephanie has just gone off. That's probably it, Fabien. [CROSSTALK] If you want to come use the definition...

FABIEN BETREMIEUX:

So John, this is Fabien speaking. We are at the top of the hour. So I see we have Maxim and Crystal on the line, so let me get to them and if we can have a very quick discussion of next steps. I think this is important for us to conclude in this call. So let's take another minute or two to go through the line and talk about next steps. Maxim, will you please try to be as short...?

MAXIM ALZOPA:

Maxim Alzoba for the record. It's about comment 29. Registries do not have to follow each RFC, with has to comply with those, would not have to implement it. And I must remind, implementation of every new feature costs money and time. It's not possible to put everything on shoulders of registries and things that nobody is going to be out of business.

So, we should be careful about the current ecosystem. Thanks.

FABIEN BETREMIEUX:

Thank you Maxim. Crystal?

CRYSTAL: Thanks. And I put it in the chat, just letting you know we have never talked about adding all of the technical matters to this, so I think the rest of you should take that back in the next phase of our discussions and discuss that.

Maxim's point is well enhanced. Regarding [inaudible] technical analysis, I think that just gets back to what Fabien was talking about earlier, that how the technical analysis is being performed is still being discussed with ICANN as a guideline, so I'm not sure having it running in two separate places makes sense at this point.

But I'm totally okay with adding more specific examples and definitions of responding to threats and things like that in [inaudible].

FABIEN BETREMIEUX: Thank you Crystal for your feedback. So I suggest we keep that discussion going along with the other points that were identified. And Crystal please allow me to follow-up on what you just said. What would be a reasonable expectation for the registries to come back with a response on these comments?

I've heard John mention that there will be a [inaudible] meeting at the end of the month. So would it be possible that a few days before meeting the registries could provide feedback?

CRYSTAL: John, is that meeting, you said, the 25th, that's about a week away?

JONATHAN FLAHERTY: John here. Yes, it's the 28th. [CROSSTALK]

CRYSTAL: I can try, Fabien, I think, maybe if we could schedule between the registries and registrars a call next week, I definitely want to touch base with Yasmin, because she wasn't able to be on this call and see what her availability looks like before committing to anything.

But I mean, we can try our best at aiming maybe the 27th to get comments there.

FABIEN BETREMIEUX: Okay. So we can certainly follow-up and make sure we have a co-chair call and finalize this, but I think that would be a good target to keep us on a, as close as possible timeline, just show the slide here. Our timeline from ICANN 54 is the following where we were trying to have a final draft by the end of the month.

I think we surely want to have the registries input and then another round of response from the [inaudible] meeting. So we should probably agree that we're [inaudible] for a final draft after that meeting, so let's say meets February. So that we can get to Marrakesh, ICANN 55, with a final doc that may already be public comment.

So I'd be interested to have a quick feedback on whether you think that that would be reasonable.

CRYSTAL: Is that to me? Sorry, I wasn't sure.

I think it's an aggressive timeline, but we can see what we can do.

FABIEN BETREMIEUX: Thank you Crystal. So maybe we can take this offline, the finalization of our timeline. We'll follow-up with a meeting of the co-chairs to make sure that we have a common understanding on next steps and communicate with draft, the wider drafting team in the next few days, over the mailing list. And so that we can setup already our next call.

So if there is no any additional comments or questions, we can probably adjourn the meeting.

I'm not hearing anybody, not seeing any hands raised. Crystal, you still have a hand. Is this an old hand maybe?

CRYSTAL: It's an old one, sorry.

FABIEN BETREMIEUX: Excellent. So thank you all very much for joining our call today. Thank you John for your presentation. We apologize for finishing this meeting a few minutes late. And we will be in contact with the mailing list in the next few days. Thank you again for your time.

[END OF TRANSCRIPTION]
