DENNIS CHANGE: Thank you. Greetings to everyone, welcome to the Security Framework Drafting Team meeting on the 29th of September, 2016. Today, we have Alan Woods and Nick Shorey, who will be leading the call, and the agenda is to review the draft that has been provided by PSWG and the Registry Group. So Alan, I'd like to start with the Appendix [B]. This is the newest addition to the draft, if you don't mind to start with this.

ALAN WOODS: Sure. I promised last week when we were considering Annex B, and the whole concept behind Annex B was trying to give an idea of the written procedures and policies that are already in place, but on the registries, we decided that it was probably best to go on a much higher level, and that is to provide a listing of the current registries, and then from there, because it is a requirement of the Registry Agreements that we have publicly available terms and conditions, that we would then – people could find it from that listing. So that is what, in effect, this is. It's just a link to the ICANN listing itself.

Actually, just on that point, Jim Galvin just sent an e-mail through querying, just because it is a particular link that we're using there – as you can see, there's a date on that. So we might look into getting a non-date-specific link in there, but that's something we can work on. But the second half is kind of the more meaty part of this, and it was just purely to ensure that it was, again, a high enough level to ensure that all types of registries are covered in this, but also the fact, in the spirit of the document as being a voluntary framework document, that one terms and conditions or one acceptable use policy is not going to be the

Rosetta Stone for anybody else, that it is getting very clearly across that one registry's policies are not necessarily representative of that of another and not necessarily directly comparable to that.

So a little bit of disclaimer going on in that, but at the same time, again, providing that all important link that if you want to see a particular registry, you'll be able to find it through that. So it was a very straightforward Annex B. Generally speaking, I think there is a lot of agreement from the registry side that this seems to be the way to go, and I'd be glad to see other comments or queries on it.

DENNIS CHANGE: Any comments, questions?

NICK SHOREY: Hi.

DENNIS CHANGE: Hi, Nick.

NICK SHOREY: Can everyone hear me okay?

DENNIS CHANGE: Good, yes.

NICK SHOREY: Thanks very much for showing the Annex B. Unfortunately, sort of due to timings and things, we haven't had the opportunity to take this part back into full discussion within the GAC and the PSWG subgroup yet. So again, I know we keep sort of worrying about the timeline sort of drifting on this, but I think we're all of the same mind that actually, things are slow, but it's better to get it right. So we will take this back and have a fuller discussion in the PSWG and see if there are any tweaks. As you mentioned, there's some dating element there. We'll see if there's anything else that we might need to tweak or [inaudible] add it into it, but I certainly agree with the principle of trying to keep this sort of [inaudible] inclusive and that you're certainly on the right tracks.

UNIDENTIFIED MALE: Great. Thank you very much, Nick.

DENNIS CHANGE: Krista has her hand up. Go ahead, Krista.

KRISTA PAPAC: Thanks, Dennis. Krista Papac from staff. Nick, just a follow-up question for you, understanding you need to go back to the bigger group and discuss this. I just wondered if that principle that Alan sort of articulated linking back to registry sites where each of the acceptable use policies could be accessed. If that made sense [inaudible] on behalf of the PSWG, it just made sense as something that when you do go back and talk to them, you're able to share where the registries are coming from.

I'm just trying to find a way to see what the gaps are, so that we can kind of try to focus on those.

NICK SHOREY: Sorry, Krista, I missed a bit of that, you were breaking up slightly. Would you be able to cover that again?

KRISTA PAPAC: Sure, sorry about that, let me try again. I guess I'm asking if sort of the principle about how to access the acceptable use policies from the framework that Alan just shared, if that makes sense from your perspective, or if that's something you think is going to be problematic with the PSWG? To me, it seems very reasonable, but I don't know exactly where the PSWG is coming from in this. If you do think that's going to be an issue, then maybe we should talk about it, and if not, then maybe we should just move on to other items where we think there might be gaps between the registries' view and PSWG's view.

NICK SHOREY: I think in principle, it seems a sensible starting point. But obviously, do we think this is detailed enough and all that kind of stuff? Yes, we'll have to take that back to the PSWG and then the GAC just to top and tail it. But yes, in terms of this, the approach, yes, it seems a sensible starting point to me, I think.

KRISTA PAPAC: Great, thank you.

DENNIS CHANGE: Thank you, Krista. Any other comments on this Appendix B? If not, I'd like to go back to our other document. Here's the PSWG [inaudible] the larger document here to see if anybody has comment on this now. I know that last week when we looked at this, it just came up, so people didn't have time to read it. So now, you should have had time to read it, so any comments and feedback?

ALAN WOODS: Dennis, if you don't mind, I can get the ball rolling here.

DENNIS CHANGE: Yes, go ahead, Alan.

ALAN WOODS: Okay, so I think the best way to put this is that when we were waiting for this update from the PSWG – so I'm looking at the update that begins on page 21, I believe. Of course, I can scroll to that, because I have access, don't I? And I'll go start. Basically, the registries were wondering how it will be phrased. It was, in principle, considered to be an interesting way of moving forward, and we wanted to see the substance of what was behind that. Now, having seen the insertion – and I appreciate that it is a brief insertion, but – the one issue may be in that that this would have been a very specific, very detail-oriented insertion that is needed, as opposed to something that is a bit more light.

So with that in mind, people have had comments on that. Certain members of I suppose the registry groupings have had comments and had some reservations on that, and I think that probably these are people who are best to discuss that, and I think we should open it up to those people who have those issues so that we can share it with the entire group and have a good discussion back and forth and see what's the sticking points, and more importantly, what can we do to move past us and are there any changes?

So I would like to suggest – and not jumping in as Chair of this meeting, because I would like to suggest that opening it up to those people who do have specific reservations about it, and let's just talk them out.

DENNIS CHANGE: Maxim, go ahead.

MAXIM ALZOBA: I'd like to talk about sinkholing, which is mentioned in this document. I think we need to define the procedures and the [extras] and obligations before we agree that we are happy to apply sinkholing, whatever it is. The reason to think so is that not all stories where sinkholing and ICANN together ended up well. Just to be short, it's the situation with the ccTLD .kz, and one big manufacturer of phones and tablets from Los Angeles, and situations where things got out of control of the registry, where the third party which was introduced by ICANN just started doing these wild and crazy things in the zone file, and basically without any – I'd say feedback – attempts of feedback from the ccTLD went nowhere.

So we need to know – given that the parties are, I'd say the same, we need to know procedures before we agree that we will be happy to, for example, redirect or effectively redirect traffic, or allow unknown third parties to do anything they want in our zone files for which we might be responsible in our jurisdictions. That's the first point.

The second is about the damage to Internet infrastructure. I think we need to limit this term a bit because in current reading, basically, registries will have to respond to any damage to any bit of Internet infrastructure. It means any ISPs [bits] of infrastructure like routers, switches, maybe hosting companies' equipment, maybe even contents of those hosting servers, maybe even, say, contents of private databases such as social networks. And we need to be responsible for what's in our control because at any moment of time, some network is under attack over Internet. We can't be responsible for that and to hold the line 24 hours a day, to say, basically, "No, we cannot do anything about it." So we need some demarcation points because like in the ISP or telecom world, there are things called demarcation points where your responsibility ends. Thanks.

DENNIS CHANGE: Brian?

BRIAN CIMBOLIC: Yes. This is Brian Cimbolic with Public Interest Registry. The third category gives me some real heartburn. The use of domain names for furthering of non-life-threatening crimes. That's a very broad category. It covers anything from potentially trademark infringement to copy right

infringement to this, that and the other. What's illegal, what's a crime in one jurisdiction may not be a crime in another jurisdiction. If it's a non-life-threatening crime, then I don't see it as an actual security threat at all. I think that it should be removed from the document. I think if it's a non-life-threatening crime, the appropriate means to address it is through a court order.

DENNIS CHANGE: Okay. Frank?

FRANK SCALZO: Yes, I wanted to pile on to what Maxim said a little bit. One thing that I think is missing from the document overall is I think it could benefit from an entire section on appropriate due diligence for a registry before they take action. Maxim highlighted one case, but there are others that we're concerned about, right? We started talking about phishing and farming. It's pretty easy to do a phishing run and put a URL in there that you'd like to get taken down, so I think registries need to perform some due diligence there. I think registries also need to perform a due diligence for potential name servers that may be located within a domain.

I might have some malware or something using something, a domain. I may delete it, there may be name servers in that that affect another domain. You actually kind of have to map out the entire transit of trust and looking at every domain and every name server that it calls and every name server that that depends on and what dependencies are you going to break in there. I don't know what the right answer is, but I

know I've got a couple of – I think checking the transitive trust between domains, understanding dependencies with name servers, making sure it's not a false flag or a false positive action trying to trigger a deletion in addition to points Maxim brought up I think are really good in terms of what action you take and what the implications are there with sinkholing or other techniques. But I think the document would benefit heavily from it. It could be a whole [inaudible] section on that.

DENNIS CHANGE: Thank you, Frank. Sean, you're on.

SEAN BASERI: Thank you. For me, the concern I saw was that when we began this framework discussion, it was focused on technical abuse: phishing, malware, botnets and farming. And in time, as we've expanded this, we see an expansion of scope, and so some of these [for example] – I think Briand already talked to this – non-life-threatening crime, or even more broader items like threats to a critical infrastructure, where we're no longer speaking about anything related to the Internet, but chemical plants, for example.

I have some concern that we've strayed – to me it feels – a bit away from the original mission to an area that's going to be much more difficult to address in this form, through this framework.

DENNIS CHANGE: Jim, go ahead.

JIM GALVIN: Thank you. My suggestion for this third category – I know that I have, at least in the Registry Group have been pretty supportive of this idea of these three categories and having some timelines, but having seen the words that I hear, I like the first category, 24 hours. The second category, other folks have commented on this interesting distinction between Internet infrastructure and critical infrastructure. The fact that that is written that way does cause one to want to ask the question, "What's the distinction between Internet and critical?" Because I agree with others, I'd prefer that we focus really only on Internet infrastructure here, everything else kind of falls into a different category which is quite subjective. Our role really is only on the internet, so that's an interesting clarification to get, and I would prefer that it be limited to just threats to our critical Internet infrastructure, is the way that I would phrase it.

In my mind, the kind of things that fall into that category, just to be very clear, are things like botnets, command and control systems would fall into that category. And as the APWG group has shown us year over year, one of the most critical things that we can do on behalf of the Internet is the uptime of those kind of systems is decreasing, and continuing to move in that direction is obviously a feature.

The third item there, I kind of always had imagined the third item as being kind of another catch-all, "Whatever else is there," and I never imagined that there would be a timeline on that. I'd rather just have a category three which is "Everything else falls into this, and we'll deal with it according to whatever other externalities may apply, but in the

fullness of time," so to speak. Court orders would fit in there, and they might have a timeline associated with them and any other complaint falls into there and it just becomes part of your day job to deal with it, so I'd rather see no timeline on the third thing and just have it be a catch-all for "Everything else falls in here." If it's not clearly called out as something which we want to address, just slot it down here, and it'll get dealt with according to whatever is appropriate for whatever event it is, which will evolve and be decided on a case-by-case basis. Thanks.

DENNIS CHANGE: Nick, maybe you'd like to address that, clarify what –

NICK SHOREY: Yes. Well, I see Chris has also got his hand up. Should we have Chris first, and then I'll just come back with some comments?

DENNIS CHANGE: Yes, go ahead, Chris. Go ahead first.

CHRIS KLEIN: This is Chris Klein from Verisign and I'm interested to know, especially in this third category, how do these best practices either conflict or coincide with involving review of content and ICANN's stated position that it's not the content police? So that's a concern with this catch-all category here.

DENNIS CHANGE: Okay. Nick, would you like to speak now?

CHRIS KLEIN: And I should say, what is the differentiation here?

DENNIS CHANGE: I'm sorry, Chris, go ahead, continue.

CHRIS KLEIN: And I should say, what is the differentiation? Because these best practices in Spec 11, from our knowledge, is that it doesn't address content or we're not supposed to scan for content.

DENNIS CHANGE: Right, Nick, I think you can go ahead now.

NICK SHOREY: Yes, thank you very much. Okay, so thank you Maxim, Brian, Frank, Sean, Jim and Chris for your comments, very helpful. It seems to me that there are some very useful points regarding the specific terminology that we've included here in the three categories. I think, it seems to me there's a general recognition that there's a benefit and an advantage in being a bit sort of clear about the separation of certain types of threats that we're talking about. So the categorization of that is helpful. However, maybe there is some sort of work to be done around the specific terminology. To pick up on Jim's point, he was talking about

what we mean, what's the difference between internet infrastructure and critical Internet infrastructure.

Those are some worthwhile things that we can take back, think about, and maybe we can sort of [inaudible] take a look more clearly to yourselves what we're talking about with this language, or maybe we can even refine this language a bit better to state this more clearly. There were some comments around the third category being a bit of a catch-all, but maybe being a bit too broad. I do recall way back we did seek to specify – and it is articulated sort of elsewhere, sort of in ICANN documentation – around the types of threats that we're talking about here in terms of the sort of botnets, all that kind of stuff, and that is the intent.

In terms of content, obviously, the reason for public safety body requesting some action would be articulated in any such request to registry operator. I think in terms of timeframes, I know someone did mention – was it Jim? Yes, I think he mentioned about the timeframe of category three, the catch-all, and so we probably don't need to do a timeline. I think – no, I do recall from one of the previous calls we had a few weeks back, there was some discussion actually about what we mean by response and PSWG are also sort of looking at this and looking if we can provide you something that will answer that query about what we mean by a timely response.

I know someone said, "Well, an automated e-mail is a response." So we're working on that, and I think we're going to provide that very soon, if Bobby hasn't already. I'm not sure he has. So I think when we sort of get this text, that might help to sort of support the timeframe

that we're talking about here. I think it is good to have some ambition about how quickly we should be responding to a particular threat, but being mindful of the different approaches that individual businesses take. But I would say having a timeframe is a good thing, but we can probably improve this document by being clear about the type of response within that certain timeframe.

ALAN WOODS: Thank you. Krista, did you want to speak?

KRISTA PAPAC: Thanks, Alan. Just to address I think it was Chris's comments or questions around content and this document, and Specification 11. So just kind of as a reminder to everybody, this framework is separate. It's a voluntary best practices framework. It is not contractual, so that's the first thing.

The second thing is, there is contract language in Specification 11 that relates to security threats, but that is separate from this. That language is different from what this document is.

Thirdly, as far as ICANN and content, again, this is a best practices document for registries to use for addressing security threats. It's not – while we're helping fact late the drafting of this and the community input, because of an NGPC resolution, it's not ICANN regulating content. We're still not in the content business. That has not changed, and so I assume that registries come across content related issues in your day to day business, regardless of what ICANN is or whatever it may be, from a

court order or some other mechanism. And so I think this would fall more towards those types of categories rather than ICANN, the entity being involved in content.

DENNIS CHANGE: Thank you. Alan, you're up next.

ALAN WOODS: Great, thank you, Alan Woods, RIghtside Registry. I'm speaking in a personal capacity, not necessarily as co-Chair on this. Just I suppose quickly to respond to Krista there – and I appreciate what you're saying there absolutely – the thing that always flashes in my mind when I hear saying, "Oh, this is a voluntary best practices document," and even the initial document grounding this framework had that wonderful line in it that it may be used for future policy development, so we still have to be very careful in how it would interplay, even in future, with any Registry Agreements. So that is always a thorn in the back of my mind, anyway. But that wasn't my point, that was an add-on.

My next point is just with regards to the framework, and maybe Nick can talk to this as well. The discussions that we'd had previously about the hierarchy, this was specifically with regards to notifications that we receive from law enforcement. This is some of the details which I think personally are perhaps a bit lacking as well, that these timelines were considered and envisaged with regards to requests specifically from law enforcement that were verifiable law enforcement, our local law enforcement, and language such as that is not currently in this draft.

I think we need to draw a separate delineation as well from those reports that we receive from non-law-enforcement agencies, because again, timelines – yes, for things that I think we've all come to agreement, for things such as child exploitation, anybody is going to react quickly to that. But if there are other, more nuanced type security threats, there is a lot of investigation that may not have the same level of evidence, it may not have the same level of severity. It will be up to the individual registry at the end of the day, even if it ultimately falls into one of these particular categories, these categories were only meant for the law enforcement reports. So I think that needs to be a little bit clearer. Well, actually, it needs to be very much clearer in that. So perhaps we could look at that too.

DENNIS CHANGE: Thank you, Alan. Jim, go ahead.

JIM GALVIN: Thank you. Jim Galvin from Afilias for the record. I have a question which I think speaks to one of the issues that we're sort of struggling with here. Somewhere there needs to exist a filter as to what is a security incident that we're going to need with or not. So to make this concrete, this is a framework for dealing with security threats and security incidents. Well, does this framework come into execution when we know we're dealing with a security incident, or does it come into execution when any kind of notification comes in? The particular distinction I'm making, I'll use content evaluation and content review as a good canonical example here. I've been thinking of this framework as,

"This is what it looks like for your abuse team," and in fact, it is invoked and comes into action whenever any kind of notification comes in, regardless of who it is from or anything else coming into your abuse e-mail address, phone call, whatever. Law enforcement, court orders, this is the entry point. And in that context, a category three of "Other" makes sense to me, because then if somebody tries to toss in any kind of content filtering thing, it falls into that category. Somewhere down the road, it'll eventually make its way up on my to-do list, and I'll say, "Oh, content filtering? I'm not doing that. Never mind." And I'll toss it out and probably respond in some way and say, "Sorry, you lose" to whoever made the request.

So that's one way to approach this. Alternatively, we can be having discussions here about whether content filtering requests ever come in the front end, and then, of course, there needs to be some process on the other side which his going to prevent them from getting there, and in that sense, then I would understand that category three needs to be much more carefully defined, because we're only trying to define the things that we're going to act on.

Now, I actually don't like that option in any case because my feeling is security threats and incidents evolved with time. So even if we prefer that latter position of, "Content requests should never come in the front door" as opposed to having a possible action that says, "I'm simply not going to react to them when they come in because I know I'm going to get them from somebody somewhere along the way," I like the preferred action of a catch-all third category three, because security incidents evolve over time and a framework should be something which we're either going to have to change over time, or perhaps it has a way

to work within whatever happens as the Internet evolves and innovates and progresses.

So what I want is a category 3, and I want a response section that says, first step is to decide and agree on what category something is in with whoever the category notification came from. Then the second thing is, once I decide what it is, I'm going to execute some set of procedures based on whatever that is and I'm going to act on it appropriately, including if it's a content filtering request, not doing anything.

So again, my question is, when does this framework get invoked? Is it the overarching filter of everything? Or is it intended to only be responding to particular types of notifications? Thank you.

DENNIS CHANGE: Maxim, do you want to comment?

MAXIM ALZOBA: I have a question to Krista: do we expect public comments for these documents? And if we expect, for what reason? What is going to be done with it? Thanks.

KRISTA PAPAC: Thanks, Maxim. Yes, this document will go for public comment, and the reason is that was the directive from the NGPC. I don't have the resolution in front of me, so I don't remember the exact words, but basically, the NGPC directed us to work with the community to come up with this and specifically to work with the GAC. So the way we've

approached this from the beginning is to come up with the draft by working with the affected parties, which is the contracted parties and the GAC. The GAC appointed the PSGW sort of as their representatives here, and I know we also have GAC members that join in. So the idea is to work with the two most affected parties, and particularly the GAC, because of the NGPC resolution, and then the community part comes from public comment, which again, the NGPC said they'll also work with the community.

MAXIM ALZOBA: Could you advise us what the next steps are going to be? Because there are no public comments for simple things and most probably it will end up in some report on the Board's table, and so if it could be a policy earlier than we expect, what is the next step after the public comments? Thanks.

KRISTA PAPAC: Public comment is a funny thing. It sort of depends on what's in the public comment, because we don't know what we don't know, but normally, we publish for public comment, there's a report that comes out afterwards. Depending on what's in the public comments, the framework can possibly be published after that, it might need to be further revised depending on the substance of the further revisions. If that were to happen, that could go for public comment again. As far as the Board piece, I don't know about that. We haven't really even talked about that bit, so we should probably start thinking about that.

At a minimum, we would advise the Board of it, because [inaudible] even though the NGPC isn't in existence, it's still a Board action and we would want to make sure the Board knew that we completed the work they directed us to complete. So at a minimum, they'd be advised. And then as far as policy goes, nothing can become policy without a PDP as far as I know, so just because something ends up on the Board's table doesn't make it policy, it's just for Board review or what have you.

MAXIM ALZOBA: Okay.

KRISTA PAPAC: Thanks, Maxim.

DENNIS CHANGE: Chris, you have the floor.

CHRIS KLEIN: Yes, thank you. I wanted to thank Krista for her earlier comments and clarifications that this is a voluntary best practices document. One of the topics that we've been discussing in the Registry Stakeholder Group is that – I just wanted to make a comment and sort of this is one of the reasons we're suggesting that registry policies should lead before taking any action on a domain name. Thank you.

DENNIS CHANGE: Thank you, Chris. Anyone else?

KRISTA PAPAC: Hey, Dennis, I wanted to come back to Jim Glavin's question, if we can.

DENNIS CHANGE: Go ahead.

KRISTA PAPAC: I thought that was a really good question, Jim, about when do people think the framework starts. And I don't know, I haven't been to all of these meetings, so maybe it's been discussed and I'm not aware of it. But I'm kind of curious to see, Dennis, if maybe we can get a sense from the group. I think Jim sort of – there might be more than two options, but his question sort of had two places where this starts: one is when a complaint comes in, and one is when – I think how you put it, Jim, I might mess up the words, but when it becomes an actual security threat. I think it'd be interesting to get a sense from the group when people think that this should be effective, to see if we're all on the same page.

DENNIS CHANGE: Anybody want to speak up? You can also chat your opinion on this.

KRISTA PAPAC: Maybe we could even just do a show of hands in the Adobe.

DENNIS CHANGE: Go ahead, Maxim.

MAXIM ALZOBA: Krista, one of the reasons for different levels of security threat is that, formally, we have obligations before registrants and registrants via the contract with the registrars. If we break something and there was not enough reason to do so, we're formally just liable for damage to their business, etc. So that's one of the reasons we need some reasonable thresholds, and we'd like, sometimes to avoid being the party which decides something, because in some jurisdictions, we don't have right to actually say that something is a crime. It's for law enforcement and courts, and maybe general attorney office. Thanks.

DENNIS CHANGE: Anyone else? Go ahead, Jim.

JIM GALVIN: Thank you. I want to respond to Maxim's question that he just had and also to the question that he had there in the chat room. It happens in a situation where [inaudible] e-mails subscribed to some spam [scheme], do we have to investigate it all.

What's important to me is process. We do often find ourselves sort of digging into the details here, but to the extent this is a framework, I think the answer to your question, Maxim, is it's covered by the framework. I'm imagining the framework overall as it's got these categories. Something falls into a category. And if something falls into category three, which I'm going to go with my model of that's a catch-all

category, then a registry has to respond to it in an appropriate way. Appropriate is guided by a number of things I believe we're all in agreement about, one of which is that, certainly a registry is the sole arbiter in what it will and will not do, and a registry is only going to do things that it believes it can do and are within its legal and liability framework, whatever that happens to be. And three, a registry is going to do whatever due diligence it thinks it can and should do in order to protect itself, and justify I guess is perhaps the word, or at least to support whatever action it wants to take.

It's going to have whatever set of policies and policies that it has in terms of service, and for example, a detailed suggestion is – even a relationship with registrars. Sometimes an appropriate response to a request is, "Oh, let's just delegate this to somebody else," and the typical, logical delegation is to a registrar. You might give them a first cut at trying to deal with it, rather than you, even though the request might have come in to you.

So I believe that all these edge cases that we bring up from time to time and talk about in this discussion are covered by that catch-all case, and we have to find the right words so that we're all satisfied. But I think we're all in agreement in principle that a registry ultimately decides what it's going to do, when it's going to do it and how it's going to do it. And it does that in whatever way works for that registry. We just need some words in black and white that sort of say that and satisfy all of us that we're covered. Anyway, thank you.

DENNIS CHANGE: Go ahead, Alan.

ALAN WOODS: Great, thank you. I think Jim just really made – his question was fantastic, because it got me thinking, and I was thinking, have we just gotten so bogged down in these key areas that we're back and forth between the PSWG, have we kind of lost the run of ourselves? So I went back to the document itself and at the very beginning where we actually set out the scope, and the scope of this document – and following on the words of the NGPC resolution – is only limited to responses to identified security threats as identified via the technical analysis that we're required within.

And also, one of the scopes we put down was how we would respond, and if necessary, how we would bring other people in. And it seems to have flipped somewhat, where we're now saying, "Well, when people ask us specifically, when people report to us specifically, how do you respond to that?" A pure application of reading the scope and just taking that moment to, I suppose, come out of this in-depth conversation and going into the pure scope, that's actually even not enough anymore.

It's a bit of an eye opener, so thank you, Jim, for opening the eyes a bit on that, and bringing me right back to the purpose of what this was. I think it's a very valid question, and it might help us move forward, in fact.

DENNIS CHANGE: Thank you, Alan. If there aren't any more questions, I'd like to reserve a few minutes for logistics. Go ahead, Chris.

CHRIS KLEIN: Yes, this is a general question, as I noticed that a colleague had forwarded to me a draft advisory that ICANN plans to distribute in and around October 10th on Spec 11, and I was wondering, how does that advisory relate to the best practices? Thank you.

KRISTA PAPAC: I can take that one, Dennis.

DENNIS CHANGE: Go ahead.

KRISTA PAPAC: Yes, Chris, as I was trying to say earlier, the contract is separate from the framework, and what we're talking about here is the framework, the voluntary best practices framework. The advisory you're referring to is also an effort that's been underway for some time. We've been working with a small set of the registries to get that drafted, but basically, again, separate from the framework project. The language in Specification 11 Section 3(b) of the Registry Agreement says – again, paraphrasing – that registries will periodically monitor for security threats, they'll keep statistical analysis reports, and if ICANN asks for those reports, they'll supply them.

We've gotten, ever since we launched – and this is the new gTLD base agreement – we've been getting inquiries ever since we started signing contracts a while back about what does periodic mean, what should be in the statistical analysis, etc. What we've told people over that period of time is we'll evaluate those on a case-by-case basis, and should Compliance or ICANN come ask for it, we'll get the details then and we can have a discussion.

There were a lot of registries that didn't really like that response, they wanted us to give them something that they could just go implement, so what that advisory is is one way of implementing this analysis and this reporting to meet the requirements of Specification 11 3(b). It's not the only way people can continue doing what they're doing. They can come up with their own processes, but it's a non-mandatory advisory just saying that, "Hey, if you do it this way, from ICANN's perspective, it would meet the requirements of Specification 11 3(b).

CHRIS KLEIN: Krista, thanks. Just a follow-up question, because some of the wording in here is specific. It says, "Registry operators must conduct analysis and be able to report data collected as frequently as needed, but no less frequently than on a monthly basis." That's different from the contract's language of periodic, right?

KRISTA PAPAC: Right, so as I said, it's one way that a registry can conduct this analysis. So if a registry were conducting it to the letter of the advisory, Compliance would say, "Great, thanks." They would ask for the

information, the registry would supply it, it would match what's in the advisory, and they'd be like, "Okay, great, thanks." There are other ways that people can do it, and it doesn't mean that they're out of compliance. This is just basically providing, for those who want to use it, a set of instructions that they can follow.

There is a number of registries out there who just want to do what they're supposed to do and don't want to think about it. They have a toe in the registry business, or they're halfway in or whatever, so rather than them inventing the wheel, they're looking for us to say, "Hey, here's a way that you could do it." So it's specific to anyone who's following the advisory, but if you're following something else, what would happen is the same thing that happens today. If compliance would ask you for these reports, or you would be subject to an audit, it would be evaluated on the case-by-case basis that we're evaluating those on today.

CHRIS KLEIN: Okay, so this advisory is not prescriptive, as you're saying.

KRISTA PAPAC: It does not apply to every registry, it only applies to a registry that wants to use it.

CHRIS KLEIN: Okay, thank you very much for the clarification.

KRISTA PAPAC: Yes, absolutely. Thanks.

DENNIS CHANGE: Alan, go ahead, we have three minutes left.

ALAN WOODS: Fair enough, a very quick [enough]. I appreciate actually what Chris is saying there in the questions, I just would like to say that the advisory, I'm sure, is going to be discussed on many other forums. This document comes after all events of the advisory have taken place, and we have taken that into account at the very beginning of the document as well, where we discuss about things such as phase one and receiving data, and actually, in the current draft of this document, there's a reference to the advisory saying that one should refer to that, if you wish to look to the advisory to see how you receive data and how you get the technical analysis or how you achieve the technical analysis. But this comes in after all that has been said and that. But as I said, I would love to talk more about this, the advisory, but I think there are other forums that we'll be having that conversation in as well. Thank you.

DENNIS CHANGE: Thank you, Alan. We need to get this meeting to a close. And just quick, logistics-wise, we are going to have to set up new meetings for October, and we will – I think [inaudible] will send out meeting invites and we will use the new rooms starting October, and we'll make sure we have enough IT support to make sure everything is working before we join the meetings next week. We are going to meet again next week and for

the following few weeks, to make good progress that we're making here.

The request should be for PSWG now having listened to the registry, Nick, would you mind going back and talking to Bobby and talk about what the PSWG will do and maybe take some inputs? And Alan, I don't know what you would like to do on your side, continue feedback inviting to the PSWG, perhaps? I'd like to hear from you, the co-leader.

NICK SHOREY: Right, so thank you very much, I've made a note of all the feedback that has been received on the call today, and thank you very much for that. And I would encourage everyone as well to continue to post feedback to the mailing list as well, because it all helps. So I've made a note of the feedback, and I'll be taking this back into the PSWG, and yes, as we see fit, we'll provide some further feedback to yourselves ahead of next week's call.

ALAN WOODS: Perfect. From my point of view, I think what's best for the registries – if the registries are listening – the feedback that was given today, I think Nick has taken a good note and he can bring that back, but I do think that we should continue having the discussion in our own forum, and then if we can put together and agree when we want to pass that feedback straight on to the PSWG as opposed to having to wait for the call, I think it'd be very supportive of ensuring that there's a good flow of information that way. So if we can look to using our mailing list, letting us agree on those things we should pass to the PSWG after

hashing it out between ourselves, I think that would add greatly as well. So let's please continue on that way.

NICK SHOREY: Yes, you're so right there, Alan. I think that's definitely the best approach, and it might help us to sort of expedite some of these sort of discussions in the run-up to when we all get together on a call.

ALAN WOODS: Perfect.

DENNIS CHANGE: Perfect. Thank you, everyone, for today's call. We will continue the discussion and make progress on the draft on the online. We will meet again next week in your new room.

[Crystal] is typing, "Do you want me to wait for you to finish typing something on your chat? Stop…" Okay then, I'll stop the recording. Thank you everyone, see you next week.

[END OF TRANSCRIPTION]