RECORDED VOICE: This meeting is now being recorded.

DENNIS CHANGE: Hello everyone. Welcome to the 22nd September 2016 meeting of the Security Framework Drafting Team. Today we will be reviewing the input from the PSWG kindly provided by Bobby and his team for the team to review. So, let me just turn it over to the co-leaders, Alan and Bobby. Who would like to start first?

ALAN WOODS: If I can just jump in very quickly first to say, because we only got this unfortunately just yesterday. I haven't [inaudible] fully [inaudible] the entire group, and apologies there. We [inaudible] yesterday if there was a bit lack in responding to that. So, I'm sure we have plenty of discussion that will come up on the input and thank you Bobby for the input [inaudible], so I do appreciate that. But of course that means it may take that little bit of extra bit of reading and discussion and that. So from that point review, I'm sure we'll have plenty of discussion but we just haven't discussed ourselves.

BOBBY FLAIM: Yeah, no problem, and apologies for trying to get this out and we're still even trying to make sure that we can get it out to the entire PSWG just to make sure that they're still going to be okay. But, basically what we did, just for the sake of the call, what was added based on the last call we had discussed a tiered approach to the response of security threats

because when the last version I had, or the PSWG had put in a response of 24 hours, there was concern about that from the registries, so we decided to have more of a tiered system in responses. So we came up with three tiers: imminent threat to life or limb, child exploitation, we said the response time should be 24 hours; threats to the internet infrastructure, critical infrastructure, 48 hours; and basically the third tier is "other", you know, use of domain name for furtherance of other non-life threatening crimes, and that was 72 hours. And then we did provide some background to that as well, including some of the definitions of critical infrastructure and some of the other laws and regulations that it's based on, so you have that there in so far as a footnote, further explanation.

The other thing that we had included as well was a case example. I now that last time one of the things Alan had asked about was if there were specific instances, or maybe not specific instances but what are the instances where law enforcement or public safety agencies would want to directly talk to registries as opposed to registrars. So, we did provide that, we used the case of a CryptoLocker and Gameover Zeus malware botnet case, where multiple international law enforcement agencies, such as Interpol, Europol, the FBI and others had worked directly with major registries to take this malware and botnet down that had big implications worldwide and the damages were in the millions. So, we provided the background of that and how we had worked with registries, specifically both gTLD registries and ccTLD registries, and what we did, not only with registries but also with ICANN, because it was a very international and multi-layered coordinated effort. So, we put that in there as well to kind of demonstrate the need for such a

framework for security and also to demonstrate why it's important for law enforcement and registries in particular to work hand in hand, especially when criminal or abusive activity arises.

So, hopefully that will… those were the big changes or the real edits, if you will, and I hope that they're going to be helpful to the group and provide more insight and assistance. So, that's kind of a summary of the additions, or the edits.

DENNIS CHANGE: Thank you Bobby. Any questions? Follow up, comments?

ALAN WOODS: I might as well jump in if nobody has put their hand up [inaudible].

And thank you Bobby, as I've said, I had a chance to read over that this morning and I made a few comments and I sent to the group already from my own personal point of view and both you know, from the co-chair point of view, trying to leave some discussion on that. So, [inaudible] I want to say is from the tiered approach point of view. My first observation was that what you put in I thought it was quite measured, but at the same time I thought that we could potentially work on getting a little bit more clarity with regards to the details of the proposals that have the tiered. So, things such as that we would consider the tiered approach, one on the source. So, again the fact that it's coming from a public safety agency that is verified needed to put that in, is where the tiered approach would come in. I can't envisage in my mind where a tiered approach would apply to a normal member of

the public, and we've discussed this before, that we would have to go through our own [inaudible] and we can't really put any kind of [inaudible], and that sort of thing. And again, putting in context, such as, what is the discussion of the registry or how is the registry review, you know, certain details like that are very important.

So, again, I think that's a good discussion point and it definitely has a [inaudible] and I think we need to discuss around that right now and see if the registries are more on board with this, and I would like to encourage as many people on the call today to give their viewpoint on this and [inaudible] as possible.

[AUDIO BREAK]

DENNIS CHANGE: Thank you [Alan]. Anyone else? Yes, Robert is typing, I haven't had a chance to read what that is.

ALAN WOODS: Well, I suppose, if I could just jump in again there and tell [inaudible] once again. Then just to say, obviously there is still a level of reluctance from the registries to tie us down unnecessarily, so that's why I'm really interested in seeing how people come back on this.

So, on this… Well, maybe I'll just need a, very quickly, [inaudible] because I'm going to pick on somebody who is in the call, because he came to mind when I was reading it this morning. And, with regards to the ALAC [inaudible], the inclusion of the CryptoLocker case, and again this is speaking as me personally, not necessarily as the co-chair, Bobby,

when I was reading it, the impression I was getting, and I know you have said it was key to [inaudible] action, that the registries were key, and yet I was reading through it and I was saying I still quite don't understand why it wasn't the registrars that were more to the point on this one than the registries, considering we would've had to escalate to the registrars [inaudible] of the points during that. So, it didn't come across as quite as clear as I was thinking, why the registry was [inaudible] in that, and the reason I'm going to pick on somebody is perhaps it just comes down to my lack of technical understanding of [inaudible]. And I see Sean Baseri is on the line, and in my mind he's me go-to fellow for the more technical side of the abuse management. So, I was wondering if somebody on the call could give a bit more information as to technically what was required in a sinkhole. Maybe that would help me, personally, so sorry for piggybacking here, as to why and how registry sinkholes and why is it more suited to the registry and not necessarily a registrar.

SEAN BASERI: Hi Alan, it's Sean, can you hear me?

ALAN WOODS: Can do, Sean, thank you.

SEAN BASERI: Great. I can chime in a little bit there. Realistically, what's usually done in a sinkhole is the DNS, the name servers of a domain name are changed to a name server that will be then, usually has a wild

[inaudible] record that will resolve everything to a set of machines that will simply record traffic, or the name server itself would just be the sinkhole. That can happen at the registry or the registrar level, usually it's just changing the name servers and then locking down the domains so that the registrant can't change its name servers back. So, that can happen on either side. I think maybe it's the registries are used [inaudible] these situations because if it's [inaudible] maybe it's left parties, but realistically, it's a change that can be made at the registry or the registrar level.

ALAN WOODS: Okay, thank you Sean. Just in again, Alan Woods here. So, I suppose the next question, what occurred to me when I was reading it then was, considering when the CryptoLocker case occurred in 2013, there wasn't many of the new registries at all, so has the landscape changed in so far as a, take for instance one of those [inaudible] these days, would that be spread across, would you be looking at more across multiple TLDs now, therefore a co-registrar approach probably would make it more specific because there's probably more of a correlation in a registrant, as opposed to in previous times where it would've been a more limited number of TLDs, and it makes sense to go to the registry because they would have broader swipe at us, but with the new TLDs then it might make more sense to focus on the registrars so they have a broader swipe at the same registrant. Again, [inaudible] understanding on this, but it occurred to me. I'm wondering if anybody can answer that.

BOBBY FLAIM: Hey, this is Bobby. There are going to be more, obviously, registries involved now because you are talking about a new landscape, but I still think it's going to be very critical to go directly to the registries. I wouldn't think the methodology would change just because there are more registries. You know, the main goal is to go to the registries, they are the front line, they are the ones that are putting things on the internet, they are putting things in the root zone, and that's really the purpose of this and that was really the purpose of the safeguards in Spec 11. So, we are hoping that this can go hand in hand with that, we are not looking to kind of… we're not really looking at the registrars, we're trying to still kind of focus on the registries, even with sinkholing. Could be the registry or the registrar, but in our experience, the best experience to get this done quickly and efficiently is really to go to the registry and that's why we've done it this way with this case and obviously a lot more. So, we're hoping just to focus strictly on the registries with this. So, even though there are more registries that you have to deal with, we are currently working on another case where we do have to deal with a lot more registries, but the methodology is still going to be the same.

ALAN WOODS: [inaudible] Thank you Bobby. Again, this is just a learning, just to make sure that we're touching the right thing in the most efficient way, and if your methodology has not changed in that, well then obviously that's the key that we have to look for. So, thank you for the clarity in that.

DENNIS CHANGE: Are there any other questions from anyone? Would you like to see a certain section of the document together? No immediate reactions from any point on the document?

ALAN WOODS: Dennis, Alan Woods here again then. Perhaps I should just touch very quickly on B, which is the one that we said we'd write, which I put together a draft and we have had some content on registry side from it. I just want to make sure that people are [inaudible] send me the specific wording but we have talked about the different terms of use of particular registries and what was, should I say, [inaudible] decided on our side is that it would just be a link to the ICANN list of registries, which in their [inaudible] includes a list of the… the website from the links to where the terms and conditions are. The reason why we are thinking about that line is just purely so that the document will dynamically change itself instead of not having a set list, the ICANN listing would be much more up to date and frequently updated, therefore it wouldn't stagnate the list. The only question on the wording is just that we want to make sure that there is an understanding as to what we mean and what is the point of having the listing included in this document, and that is its purely for demonstrative purposes, that you know, one particular registry's terms and conditions is not a measurement for another and it should not be taken as a baseline or a sample, but that we all have our own individual requirements. And [inaudible] was a little bit of a disclaimer terminology that needs to be worked in. So it's a pretty simple annex, but you know, it's in the spirit of what was [inaudible] hopefully in the last one, so I will hopefully get agreement on that very soon and get that to the full group as well.

DENNIS CHANGE: Good point. Yes, let's do that. I think that would work for everyone, so hopefully that takes care of that data annex. Now, what I'm getting from the chat is people really would like more time to read it and then people providing input, so my suggestion to the leaders is why don't we conclude this meeting so everyone has half an hour to read it?

UNKNOWN SPEAKER: I agree.

DENNIS CHANGE: Bobby?

BOBBY FLAIM: Sure, that sounds totally fine.

DENNIS CHANGE: Okay. So, no excuses now. Next time when we meet everybody has read it, and of course the ongoing email discussion should happen, and I think the next thing I would expect to see is Alan providing that Annex B explanation, he just verbalized it, in writing. And then the team responding to the document with the comments. We'd like to hear yes, we agree to the changes as well as any other changes that you would like to make. And remind you that we have another meeting next week and we will look at it again and by that time maybe this will be more firmed up.

We're still moving toward our goal of posting for public comment in mid-October, and earlier the co-leaders had discussed the ICANN57, we will certainly have a drafting team session with the entire team at ICANN57, but also we are going to go ahead and schedule a couple of closed sessions for you, one for registries and one for PSWG, timing-wise preferably before the entire group session. So, with that I'm going to conclude the meeting and let me know if anybody else has a question or comment, if not, thank you everyone for attending and we'll see you next week.

ALAN WOODS: Thank you very much Dennis.

BOBBY FLAIM: Yeah, thank you both. Thank you.

[END OF TRANSCRIPTION]