ABU DHABI – ICANN GDD: Security Framework for Registry Operators
Sunday, October 29, 2017 – 17:00 to 18:30 GST
ICANN60 | Abu Dhabi, United Arab Emirates

MERT SAKA: Good afternoon. October 28th. ICANN GDD Security Framework for Registry Operators.

DENNIS CHANG: You're welcome to come and sit at the table. Make yourself comfortable. This is going to be the best ICANN meeting ever. I promise.

UNIDENTIFIED MALE: The fireworks come at 5:30, right?

DENNIS CHANG: You like the generosity of our host? Look at the size of that.

UNIDENTIFIED MALE: Yeah, that's pretty impressive. I think I might be getting one of that.

DENNIS CHANG: Welcome, everyone. Shall we get started? Yes, so go to the next slide, please.

Welcome to the Security Framework Public Session at ICANN60. The title of our document now is officially Framework for Registry Operators to Respond to Security Threats. Next.

Our agenda today, we're going to do a short introduction and tell you what this is and give you a short background, and we will present the framework to you if it's needed. So I'm going to ask you a question soon and that'll gauge on how detailed our presentation to you will be and give you a short illustration. Illustration is not part of the framework document but I think it's an important informative example of how this framework can be used. And then we'll talk about the next steps.

So before we go, there is a very important thing we have to do and that is everybody needs to get a drink because this is a special meeting. Why we're here today, the purpose of this meeting is to celebrate the accomplishment of the Security Framework Drafting Team who's been laboring for two years to present this product to you, so they certainly deserve this drink.

So feel free. Take a moment, go get a drink and for those of you, Maxine, who are non-alcoholic advocates, I think they have special drinks just reserved for you. Everybody's welcome.

UNIDENTIFIED FEMALE: Dennis, you put up with us for two years. Do you want to go get a cocktail?

DENNIS CHANG: Yes, I do. So as we are getting our drinks, let's do some introduction. My name is Dennis Chang. I am GDD Services and Engagement Program Director and it's been my pleasure and honor to serve as the project lead for the Security Framework.

We will go around and introduce ourselves. Please step up to the mic and if you are a Security Framework Drafting member, please identify that along with your affiliation. Thank you. Let's start with Iranga.

IRANGA KAHANGAMA: Thanks. My name is Iranga Kahangama. I work in the deputy director's office of the FBI in the Unites States of America. I was one of the authors of the Security Framework Drafting Team, kind of entering mid-session but then working with all the other representatives to pull it across the line.

MICHAEL FLEMMING: Michael Flemming of GMO Brights Consulting. I would like to say I'm an observer of this team's work and I just have to say it's an

amazing job everyone has done. Japan hours prevent me from attending the 3:00 morning [meeting].

MERT SAKA: Mert Saka from ICANN organization, RPM for today, Remote Participant Manager.

BARRY LEIBA: Barry Leiba. I work for [inaudible]. and I'm just here to listen and thanks for the wine.

JIM GALVIN: Jim Galvin with Afilias, part of the original Drafting Team and the Registry Drafting Team. So looking forward to declaring completeness.

UNIDENTIFIED MALE: [inaudible] from DNS Africa. I work with the [inaudible] all the way out of South Africa so I'm more of an observer on this, but honestly very, very proud of all that has been done here especially toward our registry which is [organized outside] the planet where things aren't so [involved] like with everybody else in the developed world out there.

[MAX MOZO]: [Max Mozo], .moscow, was with the original team.

ALAN WOODS: Alan Woods from Donuts. I am the co-Chair for the registries.

BRIAN CIMBOLIC: Brian Cimbolic, Public Interest Registry, member for the registries.

[DEMALENDEN VALIDEAS]: [Demalanden Valideas]. I guess observer would be good. Speaker sometimes.

BETH BACON: Beth Bacon, Public Interest Registry.

SIMON JOHNSON: Simon Johnson. I'm a Director of auDA and the Chair of the Security & Risk Committee. I'm an observer. We've just put .au up for an RFT, as some of you may know, so this is of great interest to me.

DENNIS CHANG: Anybody else? Behind me, want to come introduce yourself? Do I have a microphone to pass by? Yeah, okay.

[BASUKI]: I'm [Basuki]. I'm from [.id] registry. I'm [inaudible] this.

HAMAD: Hi, I'm Hamad. I'm from Kuwait Finance House.

[JORTHY]: [Jorthy] from UPC University.

[WINSENSEN]: [Winsensen] from Taiwan as a non-profit organization. Thank you.

UNIDENTIFIED MALE: [inaudible]. I come from Taiwan. I work for National Communication Commission.

MICHAEL: Hello. [inaudible], the company from Beijing. I'm Michael.

JEFF: Hello. My name is Jeff. I'm also from Burma.

FERNANDO: I am Fernando from the University of La Plata in Argentina.

J. C. VIGNES: I'm J. C. Vignes from San Francisco [dot] Paris.

CRAIG SCHWARTZ: Hi. Craig Schwartz. I run the .bank and .insurance registries out of Washington DC.

[KEVIN COPAS]: [Kevin Copas], I run a registry based in Luxembourg and we're working on acquiring a couple new extensions right now.

.

[YON GENRO]: [Yon Genro] from Taiwan. I work for Ministry of Justice in the [inaudible].

PETER: Hello. My name is Peter from Taiwan.

ERIC: Hi, my name is Eric. I'm from Taiwan Law Enforcement Police Agency.

[JOHANNES LOXEN]: Hi, this is [Johannes Loxen] from [Sharenet] Risk & Compliance Company in Germany.

[SENA GETRA]: Hello. I'm [Sena Getra] from .global.

BOBAN KRSIC: Hi. Boban Krsic from DENIC and member of SSR2 Review Team.

THOMAS DARKER: Hallo. Thomas Darker from Knip in Germany, registry backing provider.

LILLIAN FASERS: Lillian Fasers from Ferowins. We have .ferowns and work with a number of brands.

DENNIS CHANG: Well, thank you and is there anybody we're missing?

FRED CARL: Fred Carl from Nominet in the U.K.

RAY KING: Ray King, Top Level Design, .wiki, .inc, .design, and ICANN wiki

ELISE: Elise. Also Top Level Design.

RICHARD SHRIAR WOSIRO: Richard Shriar Wosiro. We are in .ca and with a backend operator for .qe.

SARA MARKALA: Sara Markala , Europol and the PSWG.

JASON PLOMP: Hi. Jason Plomp from the [inaudible] Police. I'm part of the Public Safety Working Group.

[MARIO]: Hi. I'm [Mario] from .barcelona and .cart.

JOAN GREGG: Joan Gregg, ICANN Org.

YUKO GREEN: Yuko Green, ICANN Org.

[LYNETTE NARDO]: [Lynette Nardo], ICANN Org.

MICHAEL FLEMMING: Sorry, I was wondering if we're going to do like a cheers to start drinking or not.

DENNIS CHANG: It's a great idea, Michael. So everybody, as I said, you're welcome to join us in a drink. It's for everyone here because why we are here, our primary objective is to celebrate so I'd like to raise a glass to all those participants, authors, observers and our cheer leaders along the way for two years for having completed this just fabulous product, so here, here.

I'm really heartened to see the registries and the law enforcement participating in this session because that's what it's all about, how we can come together and work together as one team to do something that benefits the public along with the special interest groups here.

So let me just recognize the presenters here. We have Alan Woods who has been right from the beginning, as he said, and really the primary author.

And then Iranga, he is very modest but he has been sort of a savior for us when we got stuck and we had complications, as most projects go, with the product to a point where we were struggling and he came in and gave us a very clear and clean version and really made the job easier for us.

And then obviously Brian, of course. He's been there all along and a very wise counsel to us. So I want to recognize our leaders and this is the team that will be presenting to you.

[JIM GALVIN]: Just to say as well that I just know that [Frieda Talen] who started out at the very beginning is currently watching as well. She is part of this so I just wanted to do a shout out to her and thank her as well for or her work as well on this process.

DENNIS CHANG: So what is it? Very briefly it's a voluntary and non-binding document that's designed to articulate the guidance as to the ways the registry operator may respond to identify security threats.

That's a lot of words but the key words there are "voluntary" and "non-binding" because this is a team that came together as a voluntary team, has produced a document that's voluntary, and the result is, of course, as I said, two years of work. And then it was published just last week. So that's why we're so happy to be here because I wasn't sure at one time that we're going to make it. But it was published and but we still decided to go on with the meeting because it gave us an opportunity to present our product to the public and kind of show it off and then also

answer any questions. This is a rare opportunity and probably one last opportunity for anyone to ask questions to the Security Framework Drafting Team as a team. Maxim, you have a question?

MAXIM ALZOBA: It's more [nod] than a question. It's not just a document we prepared for registries who are ready to accept or to partially accept. I think since one of the parties in charge of this document is relevant to GAC, the structure of document could be used easily in ccTLDs all over the world because GAC members they have some influence on what's going on in their countries. That's why I think we just created something which is going to be used all over the world. Thanks.

DENNIS CHANG: Quite right, I agree. So I'm talking about Security Framework Drafting Team for those Newcomers. You may be wondering what this team is and how it's made up and I wanted to just review briefly, tell you here that it's a team that is composed of representatives from registry operators, registrars, and members of the Public Safety Working Group (PSWG), who are part of the GAC (Governmental Advisory Committee). PSWG is primarily made up of law enforcement representatives. And then currently at our last count we have 63 members from 45

organizations, so it's quite diverse and well-covered, and we have already introduced the leadership team.

There's a lot of bullets here but I just want to mention that I think the success factors, when I look back, is the way we have worked together as one team and really understanding one another. And I think at one point it dawned on us with one meeting in Hyderabad when Jim pointed out there's only five things we can do as a registry and here are the five things and I think I will say that was sort of a breakthrough moment because I think a lot of people do not have clear understanding what a registry operator is actually capable technically able to do.

So thanks for that education and understanding and then of course working continues together and the amount of dedication and the willingness to meet. I think we have like four sessions in one ICANN meeting and another four sessions. We set the record in having a number of the sessions in one ICANN meeting subsequently and that really accelerated our progress.

So I'd like to recognize the methodology as well as our product, the way we work together and it's something that I'm often questioned about, "How did you do it?" and I have to really think about how I did it or how we did it and I think those are some of the components that – oh, that we did it. I just wanted to point that out.

I want to turn it over to Alan here to give us a quick background. You don't have to go into a lot of details. Maybe spend a minute or two, why and where did this come from.

ALAN WOODS: To preface this, I got the slides this morning so I wasn't particularly prepared to go through this. I suppose it came originally from the Beijing GAC communiqué, as far as I can remember, where it was effectively the onset of Spec 11(3)(b) within the Registry Agreement, and it was an undertaking made by the NGPC in order to – and you can see it there up on the screen that… well, I can see in this screen because mine is a bit too small – that it was to access whether domains in the GTLD are being used to perpetrate security threats such as pharming, phishing, malware, botnets. And effectively it was the area on how we responded to such security threats was there was a pin put in it for a later date and it was put to the community to come up with a method to respond to the security threats as they were identified.

So we all met together again two years ago, put together calls for volunteers for this. It was always going to be a voluntary framework. We thought that was the best way to proceed at the beginning in order to find a way that would be most applicable to as many registries as possible, noting that there are big

registries, small registries, registries that have very different local requirements not just that which is in the URA, and of course different resources, which is another things.

So we tried to aim throughout this process at finding a method that was definitely not universal, because it would be impossible to find universal, but one that would cast the widest net and be able to give guidance to registries on how best to respond.

There was I suppose at the beginning of this an awful lot of resistance to even calling it a Best Practices document because a Best Practices document almost suggests that it's going to be monitored. But we didn't want that. It was a guidance to people that they could read this and put it actively within their own registry policies. This was another very important part that went throughout the entire document itself and that is that everything that is in this document is for the framework but it is always subject to the policy of that specific registry, not because it's a get-out-of-jail card free in any way, it is a way of recognizing that we have so many other outside factors as registries that we must take into account, and again to encourage the most possible amount of registries and to be able to voluntarily follow this framework.

I think one of the key things is that we had some excellent conversations across the table both with the PSWG as well, and I

think just to extend and expand upon what Dennis had said there that one of the biggest things that I took from this process by the fact that it was my first proper foray into an ICANN working group of sorts was being able to have the connection on a human level with people who were not registries or people within the ICANN Organization. That we were able to discuss practically as opposed to subjectively, and I thought that was an excellent, excellent step.

Again I would like to point out that Iranga coming in and putting a red pen through the document was excellent and it opened our eyes. We all kicked ourselves in going, "Oh, no, what's going to happen here?" but it was probably one of the best things that could have happened to us.

Ultimately that is what the document should be seen as. It is a voluntary framework that we want as many registries to be able to look to for inspiration to help them navigate what is can be a very tricky area, so from a stuttery start to a roaring finish, I think.

DENNIS CHANG: At this time I'd like to bring up the framework. It's posted, published, as I said, on 20th of October and it's on icann.org right now. We'd like to show it to you and present to you. There it is.

So let's see, Brian do you want to say something about the objective and the scope?

BRIAN CIMBOLIC: Sure, although I was just here for the beer. Before we do that, two people that deserve further recognition, Dennis himself for guiding us through the process and being firm when needed but just so cooperative and helpful to all sides at all times. So thank you, Dennis. And also Yasmin Omar in the room was former Chair of the group so thank you, Yasmin, for getting us where we are.

I don't want us to spend too much time actually going through the framework because hopefully now it's published people have read it because the cat's out of the bag.

I think that the issue of the scope and the objective, I think Alan actually really already covered so to the extent we cannot retread harsh grounds, let's save that time for questions.

Should we move on to what are the actions the registry can take? And actually if you could scroll up a bit actually, up, up, up, there you go, keep going down, okay.

So just quickly within the framework we try and articulate what actions a registry can take when a security threat is referred to it. One of the first things a registry will do is refer the domain to the

registrar and that is not an exercise in punting but for a number of reasons:

One, the domain may be compromised and the registrar is in the best position to help remediate that. Two, the registrar is the entity that actually has the contract and the contact with the registrant so they may for business reasons and for remediation purposes, they're the first step that registries traditionally look.

The next step, if the registrar does not resolve the issue is to suspend the domain, to place thorough hold on the domain and basically wiping the domain from having any function in the DNS.

You can also lock the domain. This isn't typically done and would usually require a court order so you can't transfer it. Can we scroll down a little?

Redirect the name, basically sync holing. It's kind of an extreme remedy that also likely depending on registry policy would require a court order. Transfer the domain name, same thing, an extreme remedy that likely would require a court order. The registry can certainly do it but it's not going to do it without a getting proper authorization from the relevant authorities.

Delete the domain name. This is something the registries typically don't do because it's not very effective. Once the

domain is deleted and then available for re-registration, it's oftentimes re-registered by the same bad guy for the same bad purposes. If you could scroll down just a bit.

UNIDENTIFIED MALE: Can I have a second to share the screen for the online? Because I didn't do that and I have to do that.

BRIAN CIMBOLIC: Absolutely. Everyone enjoy watching me drinking my beer.

UNIDENTIFIED MALE: Like a commercial.

BRIAN CIMBOLIC: I'm not getting any royalties either.

UNIDENTIFIED MALE: Now we can continue.

ALAN WOODS: Where's your glass you heathen?

BRIAN CIMBOLIC: If I had a nickel for every time I heard that. So moving on, taking no action. This is an option available to the registry and this isn't a curve-out for a registry to do nothing, but it's important to realize, as Allan pointed out, that the framework it's a voluntary framework and it's subject to the registry policy. So if something is referred as a security threat but it doesn't actually fit within the registry's definition of a security threat, the appropriate action in that instance is for the registry not to take any action.

One particular type of security threat that's worth pointing out, and it has its own categorization within the framework, is unregistered domains for domain generating algorithms.

These are malware, botnets that will generate tens of thousands of domains at a time, henceforth law enforcement will work hand-in-hand with the registries to prevent that from happening and to do that the registry can do one of two things: it can block the domain names, it can put it on a reserve list, or it can actually register the domain name itself. And for that to happen, basically the registry, the law enforcement and ICANN need to work hand-in-hand because for the registry to register names in its own right, we have to get contractual waivers from ICANN for both the probation one acting as your own registrar as well as the waiver for fees. Really that's it as far as the registry responses. I think Iranga are you handling reporting?

IRANGA KAHANGAMA: Sure. Just in the same way everyone else said, I'd like to thank everyone for the great work we did. I think it's a really good product of a cooperative framework that had everyone's input satisfied. I can't really quickly go through the security threats.

I think the big thing for law enforcement is that one of the issues that we wanted to highlight is the fact that we often aren't in a position to exactly know what happens and that any reporting that registry operators can give are often a very big help and benefit to us.

So we wanted to categorize the different threats and infuse that with a little bit of prioritization knowing that when you have recognized law enforcement authorities and the proper jurisdiction, that those are very feasible reports that should be given a higher priority and that should be considered considerably more severe than any other reports realizing that other reports do exist.

And then kind of in that middle tier is where you have option B where there are law enforcement but there are other potentially legitimate sources of data abuse that come through third party data aggregators or whatever. And if they are at an industry level the other national [CERT] or any other may utilize these reports. These are something that could potentially have a little bit more

legitimacy than another source, which leads us to the third because we didn't want to neglect the fact that there are individuals, public, other people that could actually be seeing these things, researchers who still obviously can make this referral to us either anonymously. They kind of have fidelity but again oftentimes those are going to reside within their own policies within the respective companies and that's fine but we want to still acknowledge that there could be some voracity to what they're saying.

And then I could go into the registry response too if you feel that's appropriate.

ALAN WOODS: Thank you Iranga. So then we came up to discussing the actual response from a registry. So we receive something and from one of the sources, we have done our review of that particular source and we decided that we probably needed to have a little look at are there specific timings that we could look to in order to get that response out and then what would inform our decision to respond within a particular amount of time.

So the first one, and this caused a lot of discussion, and we accepted it at the end that an initial response, once you get a report in and especially from sources such as from law

enforcement, it is not only a courtesy but you should give an initial acknowledgment to that report.

It kind of goes to that saying but it also needed to be said at the same time. We said that that should ordinarily occur as soon as possible but definitely within – we would suggest within 24 hours but more importantly it's what comes after that initial response.

So the way we put it is that within 24 hours of acknowledging the initial receipt, we should make as a registry operator reasonable efforts to respond with an assessment of what that security threat is and that is if we can isolate and decide a plausible cause of action that we should be able to tell what that cause of action potentially is as well.

But again, when creating that decision, when deciding how soon and how quickly we can respond to that, there are certain things and we list them out that we could look at.

The first one there is the level of priority. The first one, for something that is considered to be a high priority response, something that we should really be responding to within 24 hours of that and issue acknowledgment is something that should be self-evident that when you get you need no further real knowledge or evidence other than that presented that you know that that is a high priority.

You can see from the framework we gave some sort almost examples within that that is imminent threat to human life, critical to infrastructure, child exploitation. So we're setting the bar quite high in that and they are ones that are definitely indicative of a quicker response on those ones.

Another thing that we would then look to is the origin of the report itself. So again, going back to the actual sources that we were talking about earlier that where did that report come from, and again given the source of the report, do we afford a greater speed and alacrity to the response on that one.

Another consideration then of course is the content. When we get a report in, what comes with that report. If it is just a bare report saying there is X problem with X domain, well, obviously it's very hard for a registry operator to turn around with a method of how to respond within a very short period of time so we would always ask that there is sufficiently evidenced, effectively that you can't turn around and you can be able to respond and report within that.

I'm going through very quickly. There's a lot more detail within that and obviously you should have a good read of it but that is the high level of that.

And then finally is the responsible parties. As Brian already touched upon, there are times in which the registry operator is

not the appropriate responsible party and we should go through and ensure that the most responsible party to that reported security threat should be the person who is notified and should action it in that.

We give a few examples about that but ultimately I think, Brian, you covered them well enough on that. The registry is always an option as the first port of call but more so when it spans many TLDs or spans many registrations that the more of the blunt instrument that the registry can wield is of more effect to the issue itself.

I can move on with respecting privacy and confidentiality as well. This is one of the additions, thanks to the public comments period that we went through, and again showing the benefit of going through a public comment period. It was a slight operation that a voluntary group such as this would have a public comment period but considering the collaboration that we'd gone through, we thought that it would be best to get even more buy-in as possible.

And it was pointed out by one of the commentators that we did not actually say anything about respecting privacy and confidentiality within the framework, which was true. We had actually flagged it at the beginning and then subsequently it got buried within everything.

So we put in an extra paragraph as that is all its need effectively again in the spirit of understanding that there is a lot of differing privacy regulations out there – and I'm not going to mention the four letters but they are there – that we need to be very careful with it so we just put in an acknowledgment that we should always assume that there are considerations of privacy and confidentiality because the dealing of a security threat will ordinarily involve the processing of personally identifiable information or data.

There is one more line but I'm going to leave that to Dennis and maybe that will lead to the next part of the conversation.

DENNIS CHANG: Thank you, Alan. So what he was referring to is the future of the document that we will be revising, which we will get to. So let's go back to the slides, if you will. What we will do next is to show you an example of how this framework could be used.

[IRANGA KAHANGAMA]: Very quickly we could go through how this would work. We have, one, law enforcement identifies the botnet [inaudible] so law enforcement could reach out to the [inaudible] point of contact in the registry and they could highlight that this is a severe issue, this may be a high priority issue. Let's say it's a critical issue

because of the way the botnet is created and then give you the information and even give their preferred solution or what they think may happen based on the evidence at hand.

So under this framework, the registry would acknowledge receipt of that. They would take it in, process it and then that's when that 24-hour requirement or suggestion would kick in.

And after acknowledging the receipt, I guess it's really important to note that acknowledgment is really important because with each fair share of different policies in the past, you could either get no response in which case your law enforcement and you're just left hanging and you're not understanding what's happening.

Not all law enforcement understands ticketing systems. It's kind of like getting an answering machine. You're not quite sure if a physical person's actually seeing it or not because the content may be really important or may be minor so having that acknowledgment is actually a really big deal for law enforcement.

And then the registry is the process of kicking in and figuring what they want to do happen so they would do their due diligence to realize is this FBI, is this RCNP or is this someone with an unvalidated claim just trying to take someone's website down or something like that, as well as do their necessary

technical work to identify the security threat to make sure that it is what it is and it's not something that's misinformed or otherwise not as valid.

And then they would decide on the set course of action and then as best as they could within 24 hours acknowledge this receipt and then highlight what their potential course of action would be where there's any of the aforementioned things that Brian had mentioned obviously giving them a wide range of options, which to be fair can include the fact that they may not do anything, which may seem not helpful but at the same time it can inform law enforcement decision making in terms of if they're not going to do anything then we need to elevate it and get a court order basically to make something happen or maybe we misread it or maybe there's a third party or someone else that we can go to. But just having the clarity is obviously very important to law enforcement.

So again these would all include checks and balances to determine the legitimacy of the person and then the threat and then those considerations would be given and then communicated back to a law enforcement agency as appropriate.

DENNIS CHANG: Well done. Thank you very much. Before we go to the next slide, I want to open it up for questions. If there's anybody in the audience who'd like to ask questions or any further comments on this framework, you're invited to ask. Go ahead.

Well then, I will give you another opportunity at the end of the meeting. Let's go to the next slide. Did you have another question?

So next steps, this is, as I said, a voluntary team who came together voluntarily to this work voluntarily to produce a voluntary document so it's only appropriate to decide what we will do in the future for this document.

Now we sort of… I think of it as gave birth to this framework and as parents of the framework we have some responsibility on how this framework will live in the future because, as we all know, Internet changes, security threat changes. It's a constant thing that we can only expect and therefore and during the public comment also, we have received some suggestions, recommendations, do something this way, that way, do more, this was helpful but can you do additional work so I want to ask the Security Framework Drafting Team this question now.

You have delivered what you have committed to do and you've done it, you've done the job. Now, please give us advice, meaning all of us, what should we do next. There are many

options, right? One could be that you'll like each other so much and you like this work so much and you want to keep doing it. That's one option. The other is, "We're done. We're getting out of here," and the other could be that you leave us some ideas about how to proceed, perhaps ideas on how to receive further suggestions and how to act upon them or, as Alan just mentioned, there are other working teams, other groups that we can [inaudible] on the future work too. So these are all options and ideas and there are plenty more, it's unlimited, so I'd like to hear form the Drafting Team. You want to go first Jim?

ALAN WOOD: You gave a very either/or there where I actually believe that it's a bit of a hybrid of what you actually said. I think that for the purposes and for the completeness of this document and this process, I think today is a good day to draw a line under this particular process.

However, noting the fact that the drafting team worked exceptionally well together, I would definitely encourage the people who participated within the drafting team to then consider what else is out there.

And I think the PSWG you've already taken quite a good initiative because I've been involved with the DNS Security, the Cross-

Community Working Group. Thanks to these mechanisms coming up at this meeting.

The next question, as far as I can see it, separate completely to this but hopefully using the same mechanisms and the same goodwill and the same concept of what got everybody talking at the same table about how to then actually report the security threats. So as far as I'm concerned the next thing is finding the evidence, isolating the good evidential sources that we can action and then having good reports and what leads on from that.

But I do genuinely, as much as it pains me to say it, I think that a line does need to be drawn under the response conversation for the moment. But as we say in the last line of the document as per processes in the future, if necessary this can be revisited but I don't think it should be a hang-on of us as a drafting team as we were but that hopefully we would all be happy to put the hat on again if called.

DENNIS CHANG: Okay.

JIM GALVIN: Thank you. I want to agree with Alan. That was quite a pour – that's all I got to say. I do think for the purposes of this

document it is appropriate at this time to draw a line. I think it's important to get some experience with the document and see how well it works.

I know from our point of view, Afilias's point of view, we're already aligned with this and do it. It would be interesting to see others who may come up and want to adopt this and admit that this is what they're using and indicate whether or not it works for them. I think that we need to know whether or not it is the right thing or not based on what people's experiences are.

I would add, though, that it probably is a good thing to make sure to call attention to the Subsequent Procedures Working Group, PDP Working Group because obviously there should probably be a reference to this.

Again let's keep in mind it's voluntary so I don't want to put that out there right up front and not lose track of that but there's still an opportunity and a place for it to be referenced there as a way to approach these kinds of issues.

I'm sure that as they get down the path of getting more specific about what future guidebook might look like and agreements that go with it, there will be opportunities to reference this work and we shouldn't lose track of that and should make sure that it's included in those opportunities. So that's one specific action I would offer. Thanks.

DENNIS CHANG: Thank you, Jim. Is there anyone who is the Subsequent Procedure PDP Working Group member here?

MICHAEL FLEMMING: You're asking for sub pro people? Yes, I'm sub pro track mono Chair for the time being until we can get any co-Chair elected.

DENNIS CHANG: What I was going to ask you is can you please relay the message since you're a member of this team and member of that team? I think the request is to refer this work to that team. Can you do that?

MICHAEL FLEMMING: I will make sure it is referred to.

DENNIS CHANG: Thank you very much, Michael. Iranga, did you have a comment?

IRANGA KAHANGAMA: No, I think those are both really good points and I would agree that we should close this for now. And I would be interested in seeing reviews especially from the registry side. You know the FBI is a federal national law enforcement so we may not even be

seeing this mostly because either we have relationships with a lot of the big companies or just we don't get as many of the localized requests that the smaller police departments may be.

So I think from operational perspective, it would be interesting to get that input from a variety of both domestic, U.S. and international law enforcement sources.

And then to Alan's point, yeah I agree that I don't think the natural evolution of this is to keep opening and closing but rather establish a relationship moving forward and I think the DNS abuse mitigation is kind of a proper evolution. It's almost like with this round we've not concluded but negotiated and identified things that registries can do to help on the DNS abuse front. And now it's almost as if registries and then to the extent registrars, law enforcement can come together and see what ICANN may be willing to do in terms of mitigating or helping to address some of these issues now that we've created this document as a starting point.

DENNIS CHANG: Good point. Thank you. Anybody else have comments? Anybody else? No? Thank you for all of your input –

UNIDENTIFIED MALE: There's an online comment from [Frieda]. [Frieda Talen] says, "Agree with Alan. It is worth drawing the line and when a review is necessary the original team could always be reconvened if available and have it noted in the subsequent procedures.

ALAN WOODS: Everybody loves a sequel. Thank you, [Frieda]. Noted and agreed.

DENNIS CHANG: Yes, thank you. I think we have a good consensus of the team and that is to draw the line as we've heard and declare completion of this project but we are going to hold on to the e-mail group just in case. That's what I've heard also. I hope it's not too soon that I call you next week. No, I'm just kidding.

So with that I think we have made a decision as a team for our future and I'm going to then declare the Security Framework Drafting Team work completed, project completed, and therefore another round for everyone. Thank you very much and we're going to close the meeting. Bye-bye.

[END OF TRANSCRIPTION]