PANAMA – Tech Day (1 of 3)
Monday, June 25, 2018 – 13:30 to 15:00 EST
ICANN62 | Panama City, Panama

UNKNOWN SPEAKER: The sponsor for Barcelona lunch, we will talk about it next time if it materialize, but it sounds like very promising. As usual, my name is [inaudible], I'm the ccTLD manager of dot NA, and I think this is now the 35th of the 37th, I am not sure. I think it's the 37th tech day that we're doing, so I think that number speaks for itself. Doing this, at the policy forum is always a problem because we rely on speakers that either come there already, or are willing to come specifically and on a policy forum it's often not so easy. [inaudible] for example, was very keen on coming but said we're not doing a presentation that I wanted them to do, but they are not coming because it's a policy forum so they're not sending their technical people and they are busy with the transition of [inaudible]. So, [inaudible], initially made a request but then later for reasons I don't know, but so it's sometimes difficult. I hope we've still got a reasonably good mix, we have a few round tables and I hope it'll work out. First we have a presentation about another of these European directives, then we will have a presentation about the data security measures. I don't know the presenter from... there you go. OK. I do know the presenter, but I couldn't put faces to names, then

we have a round table of around 30-35 minutes about considerations for disaster recovery or business continuity planning, as we all know we had this problem in Puerto Rico and in Saint Martin when the hurricane struck them, in my own situation my business partner died and for such a small operation and with 2 and a half people doing the work the was quite devastating. Fortunately, we had thought about it from a year about and started to document our processes, so we were not really effected, but it's something that has not been taken serious, especially in smaller operations, but even bigger operations need to consider things like allowing certain people with the same knowledge to travel with the same planes, and silly things like this. Then [inaudible] will talk about what they're doing on the registry with regards to crime prevention, then [inaudible] is going to... holding the place for the emergency security working party, they will give us two or three topics. [inaudible] collaborated or communicated with me, I don't really know what the presentations are, it's the round table, I will leave it to them... I will just mention it. Then we have a few minutes of the CSC review, Martin [inaudible] is another person that Bart suggested to... I don't remember so I put Martin [inaudible] on. We usually have a host presentation but the host fell ill so we had to cancel this, unfortunately on short notice. Then we have a round table about the GDPR, but don't worry it's not about anything political or anything, we just are all affected

in one way or the other, and we would like to know what technical consequences the GDPR has on registries. What have we done as the dot NA registry to cope with this. Then as usual we have some closing remarks, this time it will be [inaudible]. If we run early, if it's shorter than we expected, we will adjust the timetable accordingly. OK. Without further ado, Jim Reed will be the first person. Will present from this, the clicker is working, the reason why we present it is because the more audience reads this and sees this, and we want to have the same presentation for the local and the remote audience. After each presentation there is enough time for question and answers, however, the remote audience if there is questions, has priority or precedence.

JIM REED: Good afternoon everybody, before I start I'd just like to say thank you very much to [inaudible] for rejigging the agenda to accommodate some last minute changes to my schedule this week because I think I was due to be speaking a little bit later on in the day today. What I am going to be talking about is the EU NIS directive, and I am speaking here purely in a personal capacity, I don't represent any other organization or entity and I speak purely for myself and I'm making my own mistakes. So... what's this all about? Well, the title of this slide is oh dear, another one, and this is actually reminds me of a joke a long

long time ago. In the days of the music hall theatres in Scotland, English comedians were not very well liked when they toured up and tried to perform in Glasgow, and one particular English comedians was a double act of two brothers and one day, when they started their act, one brother came onto the stage, told a few jokes, didn't go down very well with the audience and then his brother joins him on stage, half way through the act and a voice from the hall said, oh dear, there's another one. In actual case, they didn't say oh dear, they said something a little bit stronger than that. In actual fact, we have a similar situation here, there's a lot of discussion in ICANN as we know, about GDPR. Which is one of these evil EU directives that is going to have a major impact on the DNS industry and also some other areas of enterprise activities. BUt, there's also another one which is the NIS directive, so I'm going to talk a little bit about what this is, why do we have it, what's it likely to mean, and who's going to be affected by it and in what ways? Some of this stuff is a little bit an early stage just now because of where we are in the process, but this is going to have a significant impact on the domain name industry, not just in Europe. So, it's the directive on security of network and information systems, and it was passed by the European parliament two years ago. The object is to improve cyber security across the EU and this has been enacted into national law by May of this year, which is pretty much what's happened, we then have a stage now of

moving towards now into the implementation phase of that and the next stage of this timetable is by the end of this year, operators of essential services have to be identified to be told that this directive is then going to apply to them. The directive doesn't just apply to the internet industry it also applies to a bunch of other sectors too. The basic principles here are essentially stuff like motherhood and apple pie, nobody could reasonably object to this kind of thing in principle, the idea there's going to be a competent network and information security authority, or authorities. Maybe we'll have independent authorities or competent authorities for each of the sectors which is going to be affected by the directive, or maybe there's one all encompassing one, that's an implementation issue for each member state to decide for itself. There then has to be incident response teams which are going to share information about risk threats, maybe do some fact finding after the root cause analysis, exchange of information after attacks have taken place, about how they were dealt with, exchange that kind of information and so on. There's also going to be reporting regimes, so that whenever an incident has taken place, there's covered by the directive will then be required to report to the competent authority to say, we were affected by incident X, this was the impact on our community, this was the impact on the end users, or whatever, and of course, there's going to be fines for non compliance or for any serious network outages. This was

be the usual EU approach of fines of up to 20 million Euro or 4% of your turnover, whichever is the greatest. That will be the discretion of the prosecution authorities of each member state when they decide they want to go and implement that.

Next slide, so the general idea is to have a fairly light touch approach to this, and it's not going to be, if you like, an aggressive approach to try and figure what's going on. It's essentially, the competent authorities are going to respond to the information they're given, they're not going to be going out, hopefully, and banging people's doors. There's also going to be the [inaudible] cooperation of law enforcement and other kind of agencies that may be affected, both internally within the member states and across the EU. At the EU level that coordination will be facilitated by [inaudible], the European network and information systems agency, and the European cybercrime centre, EC3. The question of jurisdiction of entities that are going to be affected by this directive is where those European organizations have their main place of business, or their headquarters. This may be interesting for companies, like for example, just saying Google or Amazon, who I think have their headquarters based in the Irish Republic for tax reasons. Clearly, then the Irish authorities are going to be the ones that are going to be deciding what happens to these companies with respect to this directive. There's also going to be a single point of

contact and that will typically rest with a government ministry, but again the government will get to decide that for itself. The single point authority is going to be getting the reports that are coming in from these competent authorities that might be coming, say from a regulator or from an incident response team, and they will also be interacting with a cooperation group which will consist of members of [inaudible], member states, and the European commission to exchange information at a pan European level. Certainly the way that this is planned to unfold for the UK, that single point of contact will rest with the department of business, government ministry. I should also point out, in case anyone really cares about this, is that the UK government has said that they're going to implement this directive even though they are not going to be in the EU, probably because of the Brexit referendum campaign. The UK government is broadly saying we're going to following all of the EU directives for the foreseeable future with respect to whether they are in or out of the EU. If you want to talk about that particular issue, we will have a discussion about that later.

What are the essential services that are going to be covered by the directive? Well, it's the usual suspects that you would imagine, it's going to be things like the transport sector, railways, airports, roads, the utilities services, electricity, gas, oil pipelines, healthcare, banking, [inaudible] services, but there's

also this thing now called digital infrastructure. Within that context, we're talking about important internet exchange points, important TLD registries, important DNS providers. It's also talking about application to cloud computing providers, search engines, and online marketplaces, so presumably things like eBay and Amazon, and stuff of that nature. Small and micro enterprises will be exempt, so if an organization has fewer than 50 staff, or a turnover of less than 10 million Euro a year, they should be exempt from the directive. The sort of incidents that will be required for digital infrastructure that have to be reported will relate to things that cause a significant risk to public safety or security, or even loss of life. If there's a major surface outage which results in more than 5 million user hours of downtime, that would be covered. Let's say for example, there were 5 million users in the UK using Google's 888 services, and Google's 888 service went out for one hour, that would be an incident that would have to be reported because that was more than 5 million user hours of downtime. If there's a data loss or breach that affects more than 100,000 uses, that also has to be part of these reporting requirements, or if damage costing more than 1 million Euro, applies to any one individual, that has to be reported too.

So, what happened about this? Well, various European administrations are deciding about how they're going to be

about approaching this, and this is the description of where we;ve got to with things in the United Kingdom at the moment. The government ran a consultation on what they planned to do about the directive last year, and they defined certain thresholds in the context of what was had applied for ISPs and DNS servers, essentially traffic rates for the internet exchanges, DNS query rates for the DNS providers. They decided there was going to be a split between the DNS component and the ISP component, and responsibility for that would rest with Ofcom, the telecommunications regulator, whereas the cloud computing, search, and online market stuff would be passed across to the information commissioner's office, the data protection authority in the UK. So, the internet is not regulated in the UK, there's nothing about tariff rates or [inaudible] policies, or pricing [inaudible], it's left purely to market forces, so the government in the last communications act that was passed about 5-7 years ago explicitly says that the internet is not regulated, full stop. So, we've seen that breakdown just a little bit here. Ofcom in the context of these critical services from a DNS and internet exchange point, Ofcom, the telecoms regulator gets to decide, who are the operators of the essential services. So, in the DNS context, the thresholds that were decided by her majesty's government were top level domain registries that average 2 billions DNS queries per day or more. Notice again the directive said top level domains, it didn't talk about root servers which I

think is rather interesting. They also said it applies to authoritative DNS providers that host more than a quarter of a million domains. If you are a recursive DNS service provider and you handle more than 2 million queries a day from UK IP addresses, for some definition of UK IP addresses, you are covered. But, the plan that was set forward by the government is that Ofcom has got to some flexibility to define other operators of essential services that it might reasonably think that this reporting regime and requirement should apply. I think Ofcom will probably have to use those discretionary powers in one way or another. So, there are a number of issues about the idea of using these thresholds of absolute numbers of queries, if we talk about the traffic levels from a TLD perspective, pretty much the only UK base level domain that would be within scope would be [inaudible]. I don't know for certain, but I would imagine [inaudible] DNS infrastructure gets more than 2 billion queries per day.

However, how can we measure that accurately? That's difficult, the only way to do that would be to knock on the door at [inaudible] and say, tell us how much traffic you get. [inaudible] are good corporate citizens and I am sure they would be happy to provide that kind of information. Other registries would perhaps maybe be less inclined to cooperate. Even if you could measure those kind of rates by look at say things that have little

traffic, that's not going to give you a good indication either because, well behaving resolving servers only talk to the root servers once or twice a day, if that, and as you get referral sponsors, you've got caching, lots of that traffic is going further down the tree inside the DNS name space. So, looking at the [inaudible] data sets which are held at DNS [inaudible] as a way of trying to compute traffic is not going to give you meaningful data. Likewise, if you look at any caching statistics that becomes much harder to measure, because those providers might not be able to provide statistics about everything they do so in a consistent manner. Then, how can you get access to the query streams, and then if you apply that in the context of resolving servers it gets much harder again. So, to pick a large ISP at random, British Telecom, if Ofcom was to come along to British Telecom and says, tell us how many queries you get so that we can decide whether you should be regulated or not, I think we could be reasonably cynical and guess what BT's response would be. Yes, we get less than that query threshold, of course we do. So, relying purely on numbers is perhaps an unsatisfactory way to go about this, and some of the qualitative assessments that might need to take place here can be quite interesting. The new top level domain dot Scot is probably tiny in terms of the amount of DNS traffic it gets, quite frankly who cares? I am a Scottish nationalist so I don't think dot Scot is a good idea, I want Scotland to have a country code not a gTLD.

Not that politics... so, the issue there is the Scottish government has decided to anchor all of the websites under gov dot Scot. So, from that point of view, Scot might become important because if that goes down, it could have a substantial impact potentially on the population of Scotland. Likewise, dot London might have a significant impact, I am sure the mayor's office in London would be very upset if dot London went away for a great length of time, so maybe they want thet regulated, I don't know if Ofcom are going to do this or not, but that's the sort of thing that Ofcom is having to think about right now. Likewise, we've got one or two people hosting important domains but only have a small number of domains that they manage, and the best example of that I can give is the BBC. The BBC has probably got about 100 domain names under management, but two of them in particular are very very important, BBC.co.uk, and BBC.com. All of their new stuff, of the BBC content is accessible through those two domain names, so those two domain names if they fail for any reason is going to have a significant impact. So, maybe then the BBC has to come under the remit of this directive because of the fact they've got these very significant domain names. So, other issues that Ofcom is currently trying to figure out what they're going to do about is, are things like are other overseas important top level domains going to be in scope or out of scope? For example, should they apply this to dot com.

A lot of people in the UK will find that rather than inconvenient if dot com went away, or had a failure.

Here's another interesting question if you look at this from an EU perspective is, suppose every EU regulator or competent authority decided that Verisign has to become under the scope of this regulation because of the fact that dot com matters to all of these member states, then that's going to place a potentially intolerable burden on Verisign as an organization. So, what's going to be the jurisdictional aspect of that? Don't know. What do we do about the any cast providers? So, we're talking about companies like Ultra DNS, or CloudFlare, [inaudible], and people like that. Again, do they matter or not in terms of query rates they get, possibly, maybe they don't. In other cases, they do matter, for example, I think it's [inaudible] provide DNS servers for dot co dot uk. Maybe that matter because all of the government stuff sits under dot co dot uk, so maybe the regulations should apply to them too, purely because of the fact they host that too. Likewise, the academic community, [inaudible] manage [inaudible] almost like a [inaudible] for the UK government, so maybe they have to brought within the fold, but that introduces other problems as well as there is no contractual arrangement between the UK government and [inaudible] over the operation of gov dot uk. At the moment that's done in a volunteer best efforts basis, so if this thing gets

brought within the directive, I'm pretty certain [inaudible] is going to say we need a contract that involves money from the UK government to operate this domain name. Likewise, if you've got registers that park zillions of domain names that nobody actually uses, they're just essentially there to trade or to warehouse, do we really care about them, do they matter, should they be covered by the directive or not? Well, maybe, maybe they don't. Maybe we'll have to look to see if there's any meaningful content that each of these domains [inaudible] to see if they should fall within the directive or not. I spoke before about the issue with BBC, we've got similar situations with other small kind of like, almost boutique registrars who host domain names that matter largely because they're a Fortune 500 companies, or for like top 100 websites, or top 500 websites or whatever. So maybe, whoever is doing the DNS for Google.com, or Amazon.co.uk might have to come within the scope of this regulation requirement because of the fact that those domains are significantly important in terms of the overall digital infrastructure that applies inside the UK, and in fact pretty much every country in the world.

The next question that Ofcom has to figure out is how we're going to do this but from a monitoring point of view. Should they be passive and just wait for reports to come in after an incident has taken place, or should they have some kind of machinery

out there to go and monitor what is happening and be able to know that for example, there's been a failure that's caused certain websites to disappear, or certain pieces of DNS infrastructure fall offline for a while. Maybe, they need to know that there's an outage, at let's say for argument's sake, at CloudFlare DNS hosting nodes in London for an hour or two, how are they going to measure that? How are they going to effectively measure it? And if it's [inaudible] how can you really measure it anyway, because the [inaudible] would automatically pop up somewhere else in the network, say in Amsterdam or Frankfurt, or whatever, so who cares if the London site really goes down? Maybe it does matter, maybe it doesn't. How is it going to be measured? Likewise, if you apply this to the large resolver operators, you only way you could really measure the uptime of those resolver operators DNS services by querying from inside the network because those resolving servers are not going to be answering queries from the general public internet, they're just going to be answering queries inside the network so how can you measure the uptime or not? That'll be an interesting issue to sort out. Elsewhere, the EU, well similar things are happening. I'm just saying this is how things are apparently appear to be panning out inside the UK at the moment, and broadly speaking, a similar kind of framework appears to be emerging elsewhere. It looks as if the communications regulator is going to have responsibility for this

DNS stuff, and maybe they'll have oversight for the ISP stuff, but that's not necessarily the case, I know there's another member state where the ISP in that country already under regulation under the communications directive which has been out a few years before now, so they're not making the case to authorities that the ISPs shouldn't fall under the remit of the NIS directive because they're already covered by the communications directive which has been in place now for a number of years before. There might also be a role for any national cyber security organizations, if a country has one, or maybe it's going to be set up, and then the role of that national cyber security organizations might still need to be clarified or teased out about. In some cases they may have a hands on role, or they might just be providing some advice, and of course, that advice will not be just for the internet sector but it will also be for the utility companies and for the transport companies, healthcare, banking, and all the rest of it.

So, there's legislation pending in certain countries, some consultations are still under way in other countries, and other countries once they get that kind of legal framework sorted out through consultations or secondary legislation, or primary legislation they then have to get, let's say the communications regulator or some other body to then figure out how they're going to implement this. So at the moment, we're at the stage

now where the legislation has pretty much been passed, the regulators or competent authorities have identified and have been tasked with the job of finding out who are going to be operators of essential services, and those competent authorities are now figuring out how we're going to make those operators of essential services comply with this directive, what sort of reporting measures are going to be put in place, what procedures do we have in place for dealing with this, and how do we then deal with this afterwards? So, maybe I would say one year, possibly two years away before we start to see this thing really begin to bite, and how soon after that we see it really has teeth, is still unclear to me. It might well be for the first few years once everything's all in place and the dust has kind of settled, there might not be a mindset to go for prosecution, they might go for a lightweight touch, that certainly was the case when the data protection legislation kicked in the UK many many years ago, the informations and commissioners office would say, register if you're processing personal data, we're not interested in prosecutions at this stage, but over the last few years they've changed their tune and they've started prosecuting people for violations of the data protection legislation and of course, the GDPR that's becoming much more significant. With that, I am done and I am ready to take questions and comments from the floor.

UNKNOWN SPEAKER: Thank you very much for a relatively dry topic, reasonably well presented. I remember that two or three years ago I was asked by one of the registrars about the GDPR or something similar and that we told them to go away and to bother us with this nonsense, maybe it's time to start looking at these things when they can, because eventually they will come and bite you. Maybe also thinking about legislation of... to legislate essential databases. I don't know how they're going to legislate this but they will approve certain minimum standards for encryption, minimum standard for security and they will have an authority where few people get jobs to go and look at this. In the long run, I think there's nothing wrong with doing this, but for our side, the implementers, we should look at it from an early time.

JIM REED: Thank you. I would just say there's one other thing here, I am not a lawyer, and a legislator and a politician. I would say however, that whenever the EU started doing data protection legislation which is almost 20 years ago now, the model that was applied for that initial data protection legislation was picked up and adopted by other countries for their own data protection regimes in places like Singapore and Canada, Australia, New Zealand, and so on. So, it would be not unreasonable to we

expect that if the NIS directive gets traction and say the EU which is almost certainly is going to, that similar kind of mechanisms might then be enacted in national legislation outside the EU, so if you're not one of these European's thinking this stuff is not going to affect me, well, think again, and also if you're dealing with important DNS services, or important internet exchanges, say for example, you're an [inaudible] who runs internet exchanges all over the world, or data centers that host internet exchanges, maybe this is going to affect you anyway even though you are not an EU based company, just a thought.

UNKNOWN SPEAKER: Alwin.

ALWIN: Thanks Jim, Alwin [inaudible]. Interested in how dot co dot uk went to [inaudible] we had several discussion in Denmark, especially to scoping and who is in the scope of regulation, sorry directive, and who is not. So, as a data point in Denmark, did not use the number of [inaudible], but the number of registered domain names, which is set at half a million which conveniently enough is also just a ccTLD dot dk and not of the other ones, for ISPs on the [inaudible] that's number of subscribers. The other point is, to some of the other services you mentioned because of

how in Denmark the regulations is implemented, per sector, it meant that Danish [inaudible] is only responsible DNS, then again, how do you scope DNS and when is DNS by itself an essential service. So, when you get into is it a hospital that is important or the mayor's office? They might still be regulated under the NIS directive, indirectly through the other sector that would not be Ofcom, of the [inaudible] business authority.

UNKNOWN SPEAKER: Any other questions? OK, thank you very much. OK, next presentation will be [inaudible]. I hope I say it correctly.

UNKNOWN SPEAKER: Yeah. Hello everybody, my name is [inaudible] and I am CTO at Serbian TLD registry. We are... actually Serbia adopted new information security law in 2016 which is based on NIS, and our registry is picked as essentially service for Serbia. Not only in the part of DNS, but our registry system is also picked as essential service. So, we have new registry software which is, developed not under that law but under our needs and it is introduced in July 2016. We have two ways of access which is web application, with responsive design so you can use smartphone, tablets, PCs, and all other devices which can access applications, and also extended DVP with some minor changes to have our internal roles up and running with EPP. That's mostly standard just few

more fields. The new system is pretty much reliable on our ability system, with modern modular design and it is very easy to maintain, and also introduce plenty of new features that I am not going to talk about today but if somebody is interested I could show him. We thought about security from the beginning, when we started designing our software and we did static [inaudible] testing, aggressive stress and penetration tests during the inception period, and also we got automated testing tools for both web and EPP. System security is divided into a couple of fields, and that's application and data security, access control with edge security and I would like to emphasize about security a little bit more at the end of the presentation and also this reliable availability system, and so far we have 100% uptime.

This is our availability registry system so we have two points where we have automatic failover within one data center, and also we have active active availability cluster between data centers. So, everything is done through a series of firewalls and load balances, so if something happened to one data center, the other one will continue working and our operations will not stop. If we talk about data security, we have three entire data processing system, the highest level which is presentation layer, we have request processing, both seperated, [inaudible] requests and EPP requests. Then, another layer is registry logic

where all that stuff is done, and the final one is data processing and database access. All network communication is encrypted so from that side, we are pretty much safe. If we talk about application security, it is as I mentioned secured by multiple firewall instances and there is no direct access from the internet to any of applications. We introduced IP filtering for both web and EPP, web also has [inaudible] communication with our clients, and EPP encryption is done through pre shared key that we share with our registrars. It is pretty much to control access to our systems because we are talking about known system users and IP filtering is done in dynamically, os first IP address is set up by registry operator, by us, under the time of registry set up, and everything else can be done by registrar itself, actually by administrators of registrar and they can add IP address is couple of seconds. Because we still some discrepancies and some registrars didn't use that feature as they should, we're limited number of IP addresses for registrars to 10 for web application access and for EPP access. If they ask, we can relax that but there were no questions about that until today. Also, as I mentioned we have a [inaudible] using pre shared key for EPP access, and we have introduced two-factor identification for web application.

If we talk about security, so, if we look what I already said, we have a series of firewalls, we have IP filtering, we have pre

shared key for EPP access, and that's because we wanted to be sure that nobody who doesn't have right to access our application can even come close to it. But, sometimes it is not that easy, we have pretty much secure application on registry side, we have registrars that are using EPP service, and they are allowing their customers to use their platforms and connect through EPP sent request to our systems. Even before the new law come and make us essential services for Serbia, we have some security request for registrars but only some of them introduced that. There are some of registrars that are using us a [inaudible] communication with their customers on their portals, none of them have introduced two factor authentication on their portal, some of them are using firewalls. Some of them are introducing and imposing strong password requirements for their customers, and also some of them doesn't have separate appliance machines for customer portal and registrar operation systems. So, there number of registrars which are not that secure, that we would like. So, there is the weakest part of chain in this key. Having that in mind, we introduce a couple of security issues, of our customers, and most of our registrars have registry lock and plant side lock. But, some... only some registrars have implemented plant side lock correctly. What I mean correctly? It is the allowed on their customer portals to switch on plant side lock, but they do the same to switch off, it is hitting very more than key lock and leaving keys inside. So,

that's one part of the game, and another thing that we introduced and I believe that we are the only registry that has that, maybe now it is changed, that [inaudible]. It is very light security issue which requires registrant or admin contact to approve critical operation. What does it mean? When secure mod is on, we sent email with certain code and customers... actually registrant or admin contact, or whatever, they pick to do this operation just approve that operation.

Why is that? We had a few situations and I know that some other registries has similar situations that registrars were broken in and a lot of name servers actually a number of name servers for thousands of domain names were changed. With secure mod, it is easy, it is fast, so if it is on any unwanted change wouldn't be confirmed unless attacker can attacker also controls email access of registrant or admin contact. At the beginning the idea was to have secure mod on by default, but management decided not to do that, actually registrars complained that it is unknown, it will confuse their customers so it is an option. It is free of charge and I believe that in the future we'll have much more domain names with secure mode up and running. That is it, I hope we are going to have some questions and my strongest question is, do anybody has some way, how to pursue registrars to complain with rules that are imposed but not having some tough punishments.

UNKNOWN SPEAKER: Thank you very much from the chair, I on a regular basis encounter registrars who either can not read of think that paper... it means nothing if it is printed on paper and they have signed it. We have 70 registrars, 35 outside, 35 in the country, and we encounter both overseas and local registrars not abiding by policy. If it's in our agreement, for example, WHOIS requirements, we enforce them and we have un accredited in ten years, one registrar who did not listen to us. In the same place with 4,500 domain names, it's different than in a place that has 500,000 or 5,000,000 domain names, and if you have got 700 registrars who have a large turnover, it's difficult but we tell them very clearly if they don't abide by the agreement and they don't follow our instructions we will give them notice, and that usually works. If word gets around that we are actually enforcing the policies, at least in our country, they talk to each other and they stop trying to see how far they go, it's a matter of cost for them to do something, they look what's cheaper, not doing anything or doing what the registry says. When the cost benefit analysis goes in the favor of the registry they do what you say, if it doesn't, they won't. So, it's then a decision within a registry or the management company of whether you are willing to make an example of a registrar. But, if you use the smallest registrar,

or a small one to make an example of to encourage the others that obviously will work.

UNKNOWN SPEAKER: Yes, I understand that and it is a little bit strange for you hearing that we allowed registrars to somehow break rules and contracts, so that's our problem.

UNKNOWN SPEAKER: Well, enforce your contract. Any questions from the floor, or from the remote audience? OK, thank you very much. Now I can hand the floor over to Jack for the round table.

JACK: Good afternoon, so... right now we have the TLD op standing committee members here, so me, Erwin, [inaudible], and Fred, we're on the TLD ops committee. We also have Warren who is on the SSAC liaison to TLD ops, so what we're going to do today is talk about TLD ops, what it is, because I don't think we've ever done a presentation on tech day about what we do. Then the goal of this session is to determine if yes or no, the TLD ops committee and the community are going to work together to build disaster recovery and business continuity playbook or collateral for ccTLDs to enhance the security and stability of ccTLDs. That's the goal of the workshop, is to determine that,

and then we need to determine also to what extent the community is willing to work with us, and that's going to determine, yes or no, we're going to work on this topic. So, there's hopefully going to be a collaborative session for the next 30 or so minutes. So quickly, TLD ops was created 3 years ago, I think, or 4, following the secure working group which made a recommendation that all ccTLDs, we should create a contact repository of all the security contacts for all the ccTLD, and make that available to all. So, TLD ops, that's what we did, we created a mailing list with over 360 people on the list today, we have 166 countries represented on the TLD ops mailing list, and it's growing. The goal is there's two goals, one is to create the repository of contacts, so to have an ability to see who's the contact at other ccTLD, and also to create a media, a mailing list where ccTLD can share security incident or security notification to all other ccTLD to be more better to react to security. So to create a mailing list, the intent is to... TLD ops is not an extension of the security group, you can't use TLD ops to expect TLD ops to respond to your incident and work with you, so it's there as a repository and a media to share information. There's, today we have 6... in the end I have the list of the SSAC, the TLD ops committee member, but we have representation from SSAC, IANA, and ICANN security team.

We meet on a regular basis and determine what the future of TLD ops is. I've covered that... not the replacement. Right now we've... the example of exchange of security alert that happened, we get one or two exchange on a regular basis between our meetings, examples of those are... wrong presentation... but we had a website that had stolen password, that was shared on the list and a bunch of ccTLDs got feedback in working together to determine if that was impact them or not. So, that's the... now the goal of TLD ops is to create value to the community, so on the mailing list, and one thing we did at the Copenhagen ICANN meeting and following at the Abu Dhabi meeting is we had workshops, two series of workshop on the DDoS mitigation. So, to develop something for ccTLDs to respond to DDoS attack and the outcome of the workshop was building a DDoS mitigation playbook. That was developed, it was completed work that we've done, and it was shared to all the security contact on the mailing list. The reason for today's presentation is to determine if we're going to do workshops for TLD ops, for disaster recovery and business continuity. So, the example of the outcome is we built a DDoS mitigation playbook, we had two workshops. The workshop was successful in that we got a bunch of people in the room and collaborated together on flipchart and build the content for mitigating DDoS. The second session, we refine the first session content and built the layout of a playbook that could be used by ccTLD. This experience turned

out to be successful and we had a playbook written and available to all and it was translated in 6 language. The challenge is that the standing committee members ended up doing most of the work, well some... well most, a lot... not all. A few typos were corrected by other people. This is what we're trying to avoid is for the next following workshop, we don't want us, the standing committee to do all the work, it's got to be done by the community. We can do some work, that's OK, but not all of it. I will pass it to.

UNKNOWN SPEAKER: Thank you Jack, so as we said the [inaudible] group is here to... the main goal is to help the community by providing advices, sharing information between the community on security aspects and on security issues. After the result of the first delivery, and during the last ICANN meeting in Puerto Rico, especially after the host presentation and host actions described when hurricane passed on the island, we had the idea to working on the next topic, and next subject who is disaster recovery and business continuity plan, especially on natural disasters. We have a thing that everyone tried to work on this kind of subjects, on the TLD ops point of view, we have to focus it on security and technical aspects, because it's the parts that we know well as security experts and we want to extend the general disaster recovery and business continuity planning on focused, on this

kind of natural disaster all over the world, because we know that natural disaster are different from which part of the world you live in. One objective of the workshop today is to define if there's an interest in this topic for the community and where to start, where to focus on, and getting feedback and experience from the community. On the technical community plans we are working on several domain names, DNS, registry systems, and IT systems, I will explain that later, and on the business continuity plan we will focus on planning, testing, document making... writing procedures, and simulate the [inaudible]. So, if we focus on the TLD ops community, because the community is made of technical and security experts of DNS and registries, we will ask ourselves if we need something on the DNS resolution infrastructures, of is it important to have that on the registry systems, SRS, RDDS, [inaudible] systems, on IT infrastructures, network, hardware, servers, softwares, and first parts that we can share together is about emergency communication, because as Jack said, one of the goal of TLD ops is to share information and to communicate inside the community when there is issues and technical issues and security issues. We have to ask ourselves about these four topics, it's not when we say business continuity plan, it's not necessarily customers, it's not necessarily financial parts, we will focus with TLD ops on technical aspects.

So, what we need now is feedback from the community, we do a presentation today a tech day, we will do another presentation at the CCNSO meeting a day after tomorrow, to fill and to collect data from the community to see if the community needs this work, and if we have to work on this subject in the next ICANN meetings. So, what would the community needs, perhaps a playbook with advices, perhaps sentences of feedback. As Jack said at the beginning of the presentation, we are not here to work, you've got your security team in your registry and we just can add advices and share experience from the current team. So we need past experience from the ccTLDs that's important, and we will define and collate feedbacks from different team of actions depending of geographical area. I think it's important because I think in the Africa, in Caribbean, in other parts of the world the issues are not the same so the plans are not the same. We can make, if we are going in this way, a presentation, different types of technical continuity plans in the playbook to give advice, I think to small ccTLDs that perhaps doesn;t have at the moment for [inaudible] not... didn't make some test to test the continuity plans and it will be a way to provide help to these ccTLDs. So, what is the roadmap of what we think about it? To make some presentation here at the ICANN 62, at the tech day presentation is today, at the CCNSO meeting two days ago and having in Barcelona one workshop, I think, to collect and work together as we did for the first delivery, for the first playbook.

Working with the community the TLD ops community to collect work and create the contents of the playbook to deliver it to the community after.

UNKNOWN SPEAKER: Thanks [inaudible]. So, you can see here the members of the standing committee, so go back one slide, alright... just one. So, the goal is to determine if we want to have a workshop at the Barcelona meeting and what's the scope of the workshop. The reason we're here is that at the last meeting there was an interest from the community for TLD ops to do something and now we're asking you what is something. To be honest with the answer, if you don't want anything then we'll skip the workshop for ICANN 63. There's no... maybe disaster recovery BCP is not the right topic, maybe you want to have TLD ops to focus on something different so now is your time to tell us what you think of this, what we should focus on, and if we should focus on this at all. Doing nothing is an option, we take that. OK, so let's go... I guess the main components for technical disaster recovery would be in the DNS infrastructure, so have a playbook, how to recover your DNS infrastructure, another example is, a playbook for your registry, but since everybody asked us [inaudible] that could be a bit difficult. Standard baseline for IT infrastructure for the operation, for BCP, or I just thought of something that I forgot to say... registry network... anyway. So, is anybody

interested in building a playbook for DNS resolution, like DNS infrastructure? Is that something that we need? Because we go back, last summer, center like TLD, all the ccTLD organizations, they ran a survey with all the ccTLDs to determine if there was a gap in disaster recovery BCP, and most of the smaller ccTLD in the survey stated that they're not ready to handle a disaster recovery scenario so, there was a need for something there. Warren?

WARREN: Warren [inaudible], Google. I think that this would be really useful. Shockingly I said that a number of times on calls, largely because, you often don't realize that you need this until it's too late and if you start trying to figure out where to do this, it's just so much documentation and a lot of it is written with sort of regulation in place and laws you have to comply with that it's really hard to figure out where to start. So, to answer your question, yes.

UNKNOWN SPEAKER: OK. So, the other option, I think the one thing we're missing here for what I thought about is... based on the survey the majority of the disaster was cyber attacks, cyber security attacks that caused, maybe that's another slice we should had had in here...

it's not necessarily a DDoS but a different kind of disaster. We're here to help, but you need to tell us what to help with.

UNKNOWN SPEAKER: We have a remote comment from [inaudible], says that, all registries may use different software, custom registries, but the problems associated with recovering them will be similar, so he says that he thinks this effort is valuable.

UNKNOWN SPEAKER: A comment from our esteemed committee member doesn't count. Sorry, no. The challenge is very broad, so disaster recovery, business continuity is a super broad topic, we can focus on building a playbook for something very specific, start small, grow big. If there's a common area where we should focus on...

UNKNOWN SPEAKER: Thank you. The other way to look at it is just because it's so broad, you might develop a more generic response playbook that just has all the things in it that you need to remember if you are in a crisis that you might remember if there's a crisis, and have those in place. Then built underneath those, the scenarios where you want to have more specific, well response or playbook for those exact scenarios. But, at least you can have

the generic one for when it is a crisis, when it is not a crisis, what's your crisis response team etc.

UNKNOWN SPEAKER: The other idea I had was, maybe the first workshop is we typically, the TLD ops workshop is on the Sunday, it's a couple of hours in the afternoon, like from 1 till 5 or something, so maybe the first... an example of a scenario is we do a tabletop exercise, all of us, we simulate a disaster and then collectively we figure out where the gap is and then we move forward on addressing some of these gaps. So, anything.... yeah, Christian.

CHRISTIAN: Maybe a suggestion would be to start with our colleagues in Puerto Rico and ask them what they learned from their experiences.

UNKNOWN SPEAKER: That's on Wednesday at the CCNSO meeting, yes. Sorry about that.

UNKNOWN SPEAKER: Yeah, I just wanted to mention, this is a little bit different than DNS... DDoS attack playbook, because having disaster recovery and business continuity, there are certain differences in risk that

we have, you have... or other registries. So having one playbook that fits everybody, it will be difficult. So, we have to discuss how deep we want to go to be really helpful for everybody there.

UNKNOWN SPEAKER: Yes, I agree. There is also standards like, ISO, that defines how to do disaster recovery, BCP in great detail. If we take what is... so there's something special for ccTLDs, so maybe we write a playbook, or that you need to follow these standards and guidelines, and there's a high level plan of what you need to do to address disaster recovery, so... think about.

JIM REED: Thanks Jack, Jim Reed here. The thing about the ISO standards are, they shouldn't be seen as an end in themselves. Where I think the ISO standards and things like business continuity and disaster recovery kick in, is they can help an organization figure out how to do a proper risk assessment and risk analysis, figure all that kind of stuff out, but actually having the certification, the compliance certificate, in my mind, is completely and utterly pointless. It's the actual how you... the mechanism behind that, how you deal with these, how you identify what the risks and threats are, and what sort of scenarios you do to test these things and try them out, really is the thing that's important. I know there's certainly one registry has actually got these kind of

mechanisms in place and is quite proud of the fact that they've got that done already, but to try to do disaster recovery can be very very hard, and some people take it to great extremes, but certainly in other sectors, there could be lessons that we could learn, for example from banking and other things of that nature where if there is significant downtime in their infrastructure, there's a massive disruptive effect plus a reputational impact. I know from my own personal experience before I got involved in all this DNS business for a while, I worked for an organization where their approach to disaster recovery was quite morbid. One of the scenarios they had was, the building has gone up in fire, everybody inside the building is dead, the servers are down, how do we get the servers back in an hour.

UNKNOWN SPEAKER: Yes, to get there you need to start the maturity from a very basic step and move your way up from a certain maturity model, right?

JIM REED: Yeah, that's definitely the case, you obviously cannot go to those kind of extremes, certainly not as a first base but what I would suggest if people are thinking about doing this is to try to get some information, either from others who have done this before or from other business sectors who have applied those kinds of

technologies and approaches. Telephone companies might be a good case in point, the banking sector is obviously a good case in point as well. Maybe say the electricity production, those kind of things. They will have fairly mature procedures in place to deal with these kinds of incidents, and from time to time they happen and lessons can be learned, so I think it's important to try to do this from a DNS perspective, from a registry perspective, that you don't try to reinvent the wheel from scratch, try to learn from other people's experiences.

UNKNOWN SPEAKER: OK. I have three questions, we'll finish this with this so... first question is, should we do something, so raise your hand if we... you agree generally that TLD ops should do something disaster recovery related. OK, raise your hand if you think we should not work on this topic.

UNKNOWN SPEAKER: The ayes have it.

UNKNOWN SPEAKER: Yes. The ayes have it, the yes have it.

UNKNOWN SPEAKER: Then to the third question is, would you be willing to volunteer sometime to work with us? OK, let's write the name down. That's good enough, so that's the next step. The CCNSO workshop on Wednesday at 2 o'clock, 9 o'clock. On Wednesday we have a 40 minute, we're going to cover this in more detail and ask the same question again, kind of. Alright, that's it.

UNKNOWN SPEAKER: OK, thank you very much, any questions from the audience or the remote audience? Somebody is rising?

MARK SIDEN: Hello, Mark Siden from the SSAC. I just have a little suggestion, which is that you might end up with pairs of TLDs that have similar technology stacks but are in different places and might want to be willing to spare each other cooperatively and back each other up. That might be a good way to, a good central community building feature of ccTLD ops.

UNKNOWN SPEAKER: My question is actually, also do we just restrict this to ccTLDs? Because, small TLDs have the same problems whether they are G or C, ccTLDs have the advantage of disadvantage that they don't have contractual requirements in this regard, so we have to basically roll our own, but we should maybe try to get

experience off others involved, and as you said, I am also willing to give it some play time in tech day, because we want to be just not ccTLD focused, that said, I remember that in Mexico many years back, we had such a presentation of risk management company. So I am wondering whether we should not maybe get some professionals also involved if we can, it's a cost issue of course. To get the ball rolling in the form of maybe like a moderator or something.

UNKNOWN SPEAKER: Who here was at the Mexico emergency preparedness workshop, [inaudible] just two right? So, you know who organized that, we can take it offline... but...

UNKNOWN SPEAKER: We have got this all on the... all the agenda's are online, I've got this still somewhere, even on my laptop, I can give it to you.

UNKNOWN SPEAKER: Any other questions, feedback?

UNKNOWN SPEAKER: The same line as what [inaudible] was saying of involving some people outside our community. [inaudible] we take direct registrations and probably, you do that in Brazil too, besides

having registrars, so some of the problems that we face from the business continuity point of view, are those of registrars also, like contact with end customers, allowing them to continue registering and updating domains, and billing them and so on. Do you think you could involve some registrars in this work too, or do we leave that just to gTLDs? That is my question, and I have a half serious question, have you updated your privacy policy because of GDPR.

UNKNOWN SPEAKER: [inaudible].

UNKNOWN SPEAKER: OK. We'll talk about GDPR later this afternoon. No, registrar is a good point, maybe the secret sauce is the science of doing disaster recovery BCP, is well documented everywhere but keeping domain alive, keeping your partners relationship alive in the domain business is maybe something we should focus on which is more the secret sauce for us, versus the standard practice of doing disaster recovery so, OK.

UNKNOWN SPEAKER: I would just like to add something. We have to remember the TLD ops list is made with ccTLDs, security contact. It's hard for the moment to make the trust between security contact in the

ccTLDs to share each other the information about security. If we extend, we already have the question of gTLDs, new gTLDs, and registrars. If we extend too quickly the scope of contact who can work on security issues, I think there may be a risk is that no one wants to share with the community, we have just to think about that.

UNKNOWN SPEAKER: Alright, so we're out of time so thank you. Join us at the CCNSO workshop Wednesday.

UNKNOWN SPEAKER: OK, without further ado, Alvin [inaudible] gets the clicker.

UNKNOWN SPEAKER: I guess I am the one standing between you and coffee so I will be quick, 10 minutes. I am not sure how things are in your registries, but over the last few years we've seen a development of [inaudible] looking for fighting crime by going after the middle man, we've seen DNS blocking and now we're also seeing going after to the registry as a way to get domains offline, rather than going after the hosting company or the one actually creating the domain name. That's not to say there is not a problem. For this graph shows the number of domains that were seized by the Danish police over the last couple of years. 2016, there was

about 700, in 2017 we closed 1000, and already in March this year we saw a number of 800, which if we extend that to the rest of the year we would almost reach 4000 domains that would be seized by the national police. It clearly is a trend that is not looking good for our TLD in the number of bad things happening. The question is then, can we as a registry do something about that? Before we did something about this as a registry last year, the model was, someone sees a problem on the internet on a Danish domain name, they report that to the police, and the police is actually not on this slide, but there in the white space over there they do some secret things because they are not there, but they do investigate and when they find something is very wrong about this domain name they go to the courts, get a court order and the court then comes to us and has the domain seized and we transfer the domain to the police. Of course, this is a very slow process so can we do something that's quicker and an we do that at the registry level? Last year we had a public hearing to the Danish internet society, the internet community and hear what should the role be of us as a registry. Can we do something or should we stick to not doing anything and just be a boring database administrator? The conclusion was yes, we can do something, there is a clear requirement in the Danish domain act that the registrant has to give his real name, address, and phone number. Which means if they don't give us, we can actually take it away from them. What we do not

want to do is look at the content, it's a very slippery slope of looking at the content and say oh, this is looking bad, this is IPR, this is a rights infringement, this is filesharing and there might be some bad files in there or movies that you're not allowed to... we as a registry cannot look into that, it's just impossible to do so, we should leave that up to the courts. But, the identity of the registrant is clearly within our domain. So, we took two initiatives, for the Danish registrants we now require them to log in with our national EID called [inaudible], it's very widely used by the banks and all government institutions so we assumed that most registrants would have access to it and could use it for getting a domain name as well, and for the foreign registrants of course, we can't do this, so we do a risk assessment of their identity and if we have some suspicion that they don't give us their real name, and address we send them a request for additional documentation. The risk assessment is, comes up [inaudible], scoring algorithm, if you're below a certain limit, nothing happens and you're green, you just go through the system like you've always done. If it's a very high score, we stop your registration, your domain does not get into the zone, we require you to send in some documentation. After you do so, and we approve of the documentation, we let the domain go into the zone, and as the middle ground in the middle, we do let the registration go through but if you do not send in your extra

documentation without 30 days we take the domain out of the zone again.

What are we looking at? I am not going to tell you, because they might be listening, but of course, looking at those seizes for the last couple of years there was some clear patterns that we just coded into an algorithm. Before we did that we had an external company do a crawl of the Danish websites and they found some numbers, this was actually done for EUIPO, the EU rights organization, and the number they found of the number of websites that had intellectual property rights infringement was below 0.3%. That doesn't sound like too much, is it really a problem? Well, if you compare it to the number of websites that have a web shop, then the number of web shops that look fishy are almost 7%, which means that out of every 14 web shops, one is selling you fake goods. This is a real problem, so we should do something about it. Here are some more numbers, you can look at that later on the slides that will be online, but it ended with that we took down almost 4000 domains when we measured it a couple of months ago. Then the number looked much better, now the number of web shops that are fake are just above 1%. As the final remark, what can we do as a TLD operator? As a TLD operator we provide the infrastructure, we can look at identity of the registrant and take down the domain if they do not tell us who they are, but we cannot really solve the real problem is that

people manufacturing and buying fake or otherwise counterfeit products. That's what I have to say about this. Any questions?

UNKNOWN SPEAKER: Yes, one question from chair. This 30 day removal, is this an automated process or do you do it manually?

UNKNOWN SPEAKER: It's an automated process, so when they send in the documentation.

UNKNOWN SPEAKER: It's validated and approval is ticked.

UNKNOWN SPEAKER: Then it's approved and then the lock or status is removed. If they don't send in their documentation it's automatically removed.

UNKNOWN SPEAKER: OK.

UNKNOWN SPEAKER: Hi, I was just wondering what kind of safeguards you might have... yeah sure... my name is [inaudible]. I was wondering, especially if this is an automated process, what kind of

opportunities you might provide for recourse or remedy if people feel that their content has been taken down without just cause?

UNKNOWN SPEAKER: Sure, so first of all, the first thing we do is just require extra documentation, if you send that in, and we don't approve, then of course there is the normal procedure of the complaints board, which is independent institution outside of the registry, where you can complain within, 30 days or so. Of course, they can then tell us if we made the wrong decision.

UNKNOWN SPEAKER: Sorry, if I didn't catch this... but you... for this automated process, in order for the content to be removed and the domain to be seized, do you require a warrant or some sort of court issue...

UNKNOWN SPEAKER: Yes for the seizures, that's by court order. That's the police going to the court and getting a court order.

UNKNOWN SPEAKER: That's not what he said, he said... Danish citizens must identify themselves to the authority with... they have a little thing with

serial numbers on cards, it's very sophisticated on plastic, and foreigners do not have the ID, this is government issued. So, foreigners cannot identify themselves in an automated manner to the registry, so they use a [inaudible] method to assess the risks, under the Danish law, if I am not mistaken, they can require any foreign applicant to provide identification, [inaudible]. That's the reason why they try to automate it with the risk assessment that only the ones who trigger the yellow light must send it in, and the ones who don't send it in don't get a domain name. The seizure is the policing that if you don't want your domain seized you fight this in court.

UNKNOWN SPEAKER: Exactly, it's two different things. The seizure is a completely manual process done by the police and the courts outside of the registry. Identity control is an automated process done by the registry, again we don't look at the content but the police does.

UNKNOWN SPEAKER: Thanks.

WARREN: So, Warren [inaudible], Google. So for [inaudible] ID thing, for the Danish citizens, how do people generally feel about that when you started requiring them to prove that sort of level of,

this is who I am? Many countries people would be very twitchy about doing that.

UNKNOWN SPEAKER: I have to find a politically correct answer to that, we can talk about it moreover beer after. My impression is, that for the general population is that they're so used to it already because they're already require it at the bank, the government requires it for all interaction with government institutions, so for the 90 something percent it's perfectly alright as they're already used to it from the last couple of years. Of course there are the tech nerds, the privacy nerds, and a small group of people that are quite noisy, and they really are upset about this, of course. I don't think that's a problem for the registry to solve. We do have an option to go outside of it, if you really have to.

UNKNOWN SPEAKER: Warren, you must not forget this is a legal requirement by the domain act in Denmark. In the Netherlands, if you communicate with the government you have a [inaudible] ID, it's your [inaudible] and then you can identify yourself. In Germany, you have an electronic pass that you put this ID card, you put this in a reader, so I assume if the legislation in Denmark is, and the people are used to it, the Danish people are not bothering much

about it. It's either using it or not getting a domain name probably.

UNKNOWN SPEAKER: Yeah, there's just a big difference between having to prove your identity to get a bank account or interact with the government, versus what many people would view as sort of a non-government organization.

UNKNOWN SPEAKER: It's not... they're a government organization. It's the domain act requiring this.

UNKNOWN SPEAKER: Anyway, we must break now. It's 3 o'clock and we want to break for lunch, for second lunch, coffee, and when are we going to be here again, 3:15 plus minus.

[END OF TRANSCRIPTION]