
ABU DHABI – ALAC and Regional Leaders Working Session Part 4

Saturday, October 28, 2017 – 15:15 to 16:45 GST

ICANN60 | Abu Dhabi, United Arab Emirates

UNIDENTIFIED MALE: It's Saturday, October 28th, 2017 in Hall B, Section A, ALAC for the ALAC and Regional Leaders Working Session part 4, 15:15 to 16:45.

ALAN GREENBERG: Folks, can you please take your chairs? I see nobody sitting at the table hardly at all. Thank you, Alberto, for being here.

UNIDENTIFIED MALE: I'm here as well.

ALAN GREENBERG: Can people please take their seats? We have three sets of visitors coming in, and we really have to be a little bit respectful of their time. If I could ask everyone to either take their seats, or if you want to have a conversation, we have a door over there. All right, if everyone can please be seated and not have private conversations – thank you – we have a series of three visits from various groups within ICANN. The first is the SSR review, Security, Stability and Resiliency review. We have Geoff Huston and Denise Michel at the table.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

UNIDENTIFIED FEMALE: And Eric [Osterweil] right here.

ALAN GREENBERG: Oh. He's not at the table. I didn't lie. I was going to ask, would anyone else on the review please stand up, identify yourself? And if you can just run over to the microphone and give your name so we all know who you are.

RAMKRISHNA PARIYAR: Good afternoon, this is Ramkrishna from Nepal.

NOORUL AMEEN: I'm Noorul Ameen [inaudible]

BOBAN KRSIC: Hi. Boban Krsic from DENIC appointed by ccNSO Europe, Germany.

NORM RITCHIE: Norm Ritchie.

ZARKO KECIC: Zarko Kecic, .rs.

ERIC OSTERWEIL: Eric Osterweil, Verisign.

GEOFF HUSTON: Geoff Huston, APNIC.

DENISE MICHEL: Denise Michel.

ALAN GREENBERG: Are we done?

UNIDENTIFIED MALE: Yes, I think.

ALAN GREENBERG: Thank you. Just to note, when we finally get to the point of questions, unless you're fluent in French, Spanish, and Arabic, you may want to find a pair of earphones to don at the appropriate time. And I'm going to turn it over to – Geoff? Denise? – Geoff to give us first a little bit of an idea of why you have a Review Team and what the current status is.

GEOFF HUSTON:

Good afternoon, ALAC. I am Geoff Huston, I am one of the members of the SSR2 Team, and you've heard from the others who are present here at this ICANN meeting as well. What I will do is run through a relatively quick summary of what we're doing and where we are, and then I'm actually going to turn it over to you, ALAC, because the real essence of what we're doing here this afternoon is to actually gather input from the various constituencies within ICANN and gather up your concerns, your questions, and your suggestions to help us with this work.

So who's driving the slides here? Thank you. Next one. ICANN drives the domain name system, and the users of that system are you and I as users of the Internet. If the domain name system is compromised through security issues, if it's unstable, if it starts giving the wrong answers, if it's not resilient in the face of attack, then we as users suffer. There is no more Internet because the domain name system lies at the heart of almost every transaction.

So if you look at what ICANN does in its broad reach of what it does, the issues of security, stability, and resiliency are at the heart of everything ICANN does. The real question from time to time, to both ICANN the organization and us the broader constituencies, how are we doing? Are we being appropriately mindful? Are we being effective in looking at its issues in amongst all the other things we do?

So in the Bylaws, there is a provision every five years for a Review Team gathered up from the various constituencies within ICANN to look at our activities and look at our effectiveness in addressing these common concerns we all have as users over the security and stability of the things that we do in ICANN. This is one of four community reviews that occur from time to time within the structure of ICANN. Next slide, please.

Here are a lot of words about the mandate. I believe you can all read, so please, we'll leave it up there for a second or two, but I don't want to waste your time reading them. This is the mandate for the Review Team, and those are the four major bullet points in terms of what we are trying to do here. That's actually a summarization – I think it's a summarization, it's not a direct quote?

DENISE MICHEL: It's a summarization.

GEOFF HUSTON: It's a summarization of the Bylaws, Section 4.6, Subsection C, which you all know of by heart. So it says that. Thank you very much. Next slide.

These are big topics. It's an enormous amount of breadth because security, stability, and resiliency is really part of

everything we do. So if you're trying to review that, that is a huge amount of work. We've already had to review a very large set of material to try and pick out the context from the initial team that did this a little over five years ago, I believe, and also understand where we are right now as a broad community with this common interest.

The team itself has been called upon with a very diverse set of skills and experience to match that against our agenda. We don't want to do a bad job. We want to do a good job. We want to be thorough, and we want to be thoughtful. We're not just filling in a report, we actually want the report to be helpful to ICANN and the constituencies. So necessarily, this takes time. It's not a one-week exercise, it's not a one-month exercise. It takes time. And so time is being taken to try and do this in a way that is thorough, thoughtful, and helpful. Next slide.

Here's the larger set. Not all of these individuals can be here at ICANN 60, but as you see, we are drawn from all over the larger world of the Internet and various constituencies and affiliations as we work through this. Two team members, Emily Taylor and Cathy Handley, have had to drop off the team for various pressures. Norm Ritchie has been nominated to replace Emily, and I think we're waiting for the RSSAC to nominate someone to replace Cathy in their own time. Next slide, please. Thank you.

Here are those five areas of review that we're trying to structure our work around. The first was 28 recommendations from the initial Review Team work in 2012. We've also been looking at ICANN's key, the major areas of stability, security, and resiliency and their activities in that area. We've been looking very closely at the domain name system where ICANN has a direct role or facilitates activities in the domain name system, and that in essence does concentrate particularly in the root zone of the domain name system.

The next one is a broader scope because ICANN does have a responsibility across the entire identifier system of the Internet, and we are looking at more general challenges to that secure and resilient operation. And lastly, the particular thing that's happened in the last five years, the transition of the IANA function into ICANN itself, and we're looking at the impact of that transition on stability and security. So those are the five major areas that we are structuring our work around. Next slide.

The timeline. As I said before, this is not a rushed exercise. It will take some time. I'm not sure I knew how much work this was when I signed up for it. I'm not sure anyone did. Maybe someone did, but they didn't tell me. We're certainly around nine to ten months into this where we're in the process of analyzing and collecting data. And in the coming months, we will start formulating our thoughts about the data we have collected

[inaudible] some of more recent developments that have happened with the Board of ICANN. This is certainly drafted before that, so these were are expectations of timeline. They might be changed in the near future, but that's not really up to me. Next slide.

And just to give you some insight here – and this is the kind of detail that covers a lot of the work, and as I said, this is merely just one aspect, but looking at these particular activities and how we went about it, and there has been an awful lot of work done with briefings from various people, particularly in the ICANN staff. We've set up an RFP for external consultancy to do some gap analysis for us, and this week we are doing a range of consultation, and you're part of it. Lucky you. And over the coming months, we'll be looking at drafting the first draft of the report based on what we hear.

So this week (next slide, please) we're meeting with almost everyone, really, aren't we? Top to bottom.

DENISE MICHELE: [We certainly are.]

GEOFF HUSTON: We certainly are. So as I said, lucky first you are. And we're going to take an extra day at the end of the week because who cares

about home. We'll sit down and analyze what we've actually learned this week and make sense of some of these inputs. So we're keen to continue this conversation. This is not just a fly-in visit. We'll certainly try and keep in touch with you as we progress from here on. In the slides that you will have as a record of this meeting, there's some material about how we intend to do that and how you can get in touch with us.

But right now (next slide), I've talked for slightly longer than I've wanted to. We only had half an hour, so I'm going to stop and you're going to talk. So to get you going, here's a question: if you just had one thing that relates to the security and the stability of the identifier space, just one thing that you think we should be looking at, we're keen to hear it. What's important to you? Because if it's important to you, maybe it should be important to us too. So with that, Alan, I'm going to hand it over, and put on the headphones. Thank you.

ALAN GREENBERG:

Thank you. I have a number of questions, and I have an answer, but I'd like to give other people an opportunity first. Sébastien, go ahead.

SÉBASTIEN BACHOLLET: [inaudible] hear from our two colleagues from ALAC who are members of this group because I think it's important to know how it's happened, what is happening, and what is their feeling as they are representing or the liaison, or whatever the name, between ALAC and the SSR.

GEOFF HUSTON: One of them is here. The other unfortunately [isn't.]

ALAN GREENBERG: Yes, please go ahead.

RAMKRISHNA PARIYAR: I am representing the ALAC community.

GEOFF HUSTON: If you want to say something, whatever you want to say, you are free.

ALAN GREENBERG: If you can give us some idea perhaps on to what extent is this what you think you applied for when you applied and any perspective you have of how things are going at this point.

RAMKRISHNA PARIYAR: Basically, we have two members from At-Large community, and we are focused about the end user customers' perspective also and the interest of the Internet users who are there facing the problem, and [what their view in the] community to make security, the stability, and the resiliency for the DNS stuff. Thank you.

ALAN GREENBERG: Thank you. Anyone else? Well, then I'll do my first one, and I'll answer the question. We hear on an almost daily basis about how various organizations, computer systems have been penetrated and all of our data stolen. It happens with big organizations, it happens with small ones, it happens with ones that we would have thought were doing a really great job and cared and some who obviously aren't. Are you trying to look at to what extent the systems that support the DNS structure have been penetrated? You're looking at obviously, "Are they well built?" But are you also looking at any historical data of, "Have there been any problems in this area that people have been willing to admit to?" I'm not asking for the details, obviously. Are we really at this point in good shape or not, or is there evidence that we do have operational problems?

GEOFF HUSTON:

In the particular area of looking at the procedures relating to the maintenance of the root zone of the DNS, we've questioned closely the staff in PTI as to the overall information process flow of requests for change in the root zone, the way in which the authenticity of that request is made, the use of data to validate that request, and then the handling of that in terms of its process from request to change of the root zone and subsequent publication.

There is a lot of reliance on the admin and technical contacts listed in the root zone WHOIS section of the database. As far as we are aware, that is not private data. It is normal, published data, and the reliance on that, there's not that much that leaks in terms of, "This was private data and it's leaked forward." Your question though about the larger aspect of, "Are all those systems locked down? Is appropriate IT management in place?" Is a fine question, and we should note it. Thank you.

ALAN GREENBERG:

To be clear, I wasn't worried about data being stolen in this case. I was worried about systems being penetrated and perhaps corrupted in some way. Sébastien?

SÉBASTIEN BACHOLLET: I will speak French so if you wear your headset, it's going to be easier for you to understand. I have a question on whether you're looking at something because it would seem that we're starting to perform some tests to replace the WHOIS system with the RDS system or whatever it's called, and there are two important registries that have begun to perform these tests. So I wanted to know whether that was within your scope and whether that could have any consequences on security and specifically on the use that users make of the Internet. And whether it would have an impact on those who purchase domain names in terms of the information they're providing like who can access that data? So is this within the scope of your assessment, or is it not part of your prerogative? Thank you.

ALAN GREENBERG: Denise?

DENISE MICHEL: As you can see by the Bylaw mandate, the language in the Bylaws for the Security, Stability, and Resiliency of the DNS Review is rather general and could conceivably cover quite a large space. We've identified our scope and terms of reference more narrowly than what could have been done in the Bylaws, and it's on our wiki. But to answer your question specifically, no, the Review Team is not looking at RDAP and is not specifically

looking at the WHOIS system. Since the RDS Review Team has just kicked off, we are assuming that since the purpose of that review is the WHOIS system, that that Review Team will be looking specifically at the WHOIS databases, RDAP and those types of issues.

SEUN OJEDEJI:

I just wanted to ask a question, but I was also [considering whether it's necessary.] But let me just ask it anyway. One of the action items you listed among the five was to look at the impact of IANA stewardship transition on SSR. What I wanted to understand by that is, does it mean that this could be recommendations that will come out to [inaudible] recommend some changes or something? What is the goal of that particular item? Is it to actually say, "Okay, what we have decided on may not be the right way" and so you recommend something different? What is the goal of that particular point? That's basically the question. Thank you.

ERIC OSTERWEIL:

The subteam that focused on the IANA transition was mostly looking at the procedures in place, the documentation, and basically just the resilience of the process that's there to ensure that it's visible, it's being adhered to, it makes sense. So it wasn't

really to repave any roads or anything like that. It was just to do some inspection and make sure that it's operating properly.

ALAN GREENBERG: Thank you. Ricardo is next, and I've asked for a 90-second timer for interventions. Thank you.

RICARDO HOLMQUIST: I will speak in Spanish. I don't know if this touches this Review Team directly. Once we received the rollover of the key signing key, and I understand that one of the main reasons was the limited amount of websites that were using DNSSEC. So what are you doing or what is RSSAC doing to try to boost the adoption of DNSSEC so that we can implement a rollover at some time next year? Thank you.

GEOFF HUSTON: I also happen to be a member of SSAC and happen to have some experience in this, but I suppose at the outset, let me say that the postponement of the scheduled roll of the KSK was something that was not known to any of us until it happened, and so this was not part of the SSR review as a generic area of study because we didn't really think that it was going to come out the way it has.

It might be the case that we could include some observations as to what has happened, but it also might be a little premature to start performing a postmortem of this in this particular incarnation of the SSR review process. And it might be useful to allow these procedures, which appear to be well managed and competently managed, to run their course and allow SSR3 to perform a more full and adequate post mortem of what are we doing, why are we doing it, how are we doing it, is it stable, is it robust, does it work properly? So at the moment, it's not on our radar as SSR2 at this point, and it's an option as to whether it should be or whether it should simply be deferred for the next review.

ALAN GREENBERG:

I think there's a general wisdom that you should let history happen before you evaluate it, and at this point it's an interesting question whether they mismanaged the process and therefore had to delay or they did it properly but the world unfolds as it does and they made a prudent decision because of it. It's certainly not clear to me. Anyone else? I don't see any other hands.

DENISE MICHEL:

[I have a –]

ALAN GREENBERG: Sorry?

DENISE MICHEL: I have a closing remark.

ALAN GREENBERG: Oh, you have a closing remark. We are almost closing, aren't we?
I have more questions, but I'll –

DENISE MICHEL: [inaudible] No, please ask more questions. If you have time, we
do.

ALAN GREENBERG: Well, we don't. We're almost on to the next group. But one of my
questions was going to be – and I should tell you, I'm Chair of the
RDS Review Team, and therefore I look for similarities and
differences. And I noticed effectively you're trying to outsource –
I noticed that you haven't yet – essentially the first item in your
review, to look at the first SSR review. And I would have thought
that was within your skillset and, moreover, an important thing
for you to do yourself if you're going to be capable of doing the
other parts. You should be both capable of doing it, and it's a

mandatory step for you to have gone through the experience. And I'm just curious how that decision was made.

DENISE MICHEL: Sure. We spent over six months reviewing the implementation and resulting related material from the 28 recommendations of the first review that was adopted in 2012. So we've done quite a bit of research and review, have asked for substantial amount of material, and in addition to all the other activities, some members of the team felt it was prudent to get a professional gap analysis done as another point of information into the Review Team's ultimate assessment and recommendations on SSR1.

GEOFF HUSTON: I have to say, Alan, I have certainly read better stability reports and security reports than the SSR1 report. Literally, many of these recommendations – they weren't ephemeral – but they were extremely vague in general. The whole issue of whether the implementation had proceeded on a recommendation that was remarkably difficult to interpret I think has been a challenge to everyone. It is not the clearest report in terms of its recommendations and the implementation thereof. And certainly, some members were really confused with the staff report kind of going, "What did it really mean?" Which is why it

has gone for a gap analysis or a request for external help with gap analysis because it's a difficult report the way it was structured. They did a lot of work, and congratulations to them but, gee whiz, I wish it was clearer. Thank you.

ALAN GREENBERG: I did happen to review that report in some detail as part of ATRT2, so noted.

GEOFF HUSTON: Noted.

ALAN GREENBERG: Denise for closing remarks?

DENISE MICHEL: Just to reinforce how we got to this point, way back when ICANN sought to not be on a one-year renewal with its contract and oversight of the U.S. government, they agreed to an MoU in order to help ensure the accountability of ICANN in its commitment to some key areas. Four reviews were mandated, and then the community as part of its accountability and transparency work, as part of the IANA transition, put these four independent community reviews into the Bylaws.

During the course of our work, we received recently a letter – no, actually we didn't receive a letter – SSAC sent a letter to the Board disagreeing with the scope or direction of this review and asking that it be suspended, which was quite a surprise to many of us. And then today, just an hour ago or less, we received a letter from the Board saying that, “SSAC sent us this letter, so we’re going to suspend the review and you should talk to the community, and then we’ll decide what is going to happen.”

Again, we have very little information about the impetus for this or how this is going to play out, but we have a lot of questions, and hopefully they will be answered since we've never talked to the Board about this. We've actually never talked to the SSAC about this either. But I have I think more of a meta concern. If the community included these four reviews as a core way of keeping ICANN accountable and of having an independent community assessment of some key activities under ICANN, and [then in independence] of the first review to be carried out under the Bylaws is unilaterally suspended by the Board, what does that say for our independent community review process and a lynchpin of the accountability in the Bylaws?

So you have ALAC and all the other SOs and ACs have appointed a group of volunteers who have spent their vacations and weekends and a lot of unpaid time as you know how you do that in ICANN working on a very challenging review. We’re in the

information gathering and research phase, and we're not quite sure what the status of this review is.

But you should be aware of that because as is part of the community that called for the continuation of independent community reviews, how independent these reviews are, what the Board's role in allowing them to go forward – of course, the WHOIS RDS review has just started, the CCT review hasn't been completed yet – is an important issue that goes beyond simply the SSR review. So this is something that the community should have a dialog about this week.

We'll continue to meet with other stakeholder groups and SOs and ACs that have time on their schedules, but it is uncertain whether and how this so called independent community security review will move forward. Thanks.

ALAN GREENBERG: Thank you, Denise. I don't have any comment on that. The world is unfolding.

DENISE MICHEL: It sure is.

ALAN GREENBERG: Seun – those were closing comments, and we’re five minutes into the – I think CCT is next. Jonathan, will you give us another two minutes? 30 seconds. Seun has yielded his time. Eduardo?

EDUARDO DIAZ: I have only 20 seconds, mine. So if this happens and stays like that, will that become a precedent for other organizations to say, “I oppose my review?”

ALAN GREENBERG: I’m not sure the Board is “other organizations,” but nevertheless.

DENISE MICHEL: I have no answer to your question. I do not know.

UNIDENTIFIED MALE I bet the ALAC is wishing they had thrown that lever at some point.

GEOFF HUSTON: I should stress that this has happened after the Review Team has met. Denise’s comments are Denise’s comments, they’re not the comments of the Review Team as a whole. There are various opinions on the Review Team necessarily, it’s a very big team.

DENISE MICHEL: Yes.

GEOFF HUSTON: And certainly, these are your views and we respect that, but it's not necessarily the views of the entire team. We are in the middle of a situation, not at the end of it.

DENISE MICHEL: Yes. Thank you, Geoff. I should clarify that. We literally just got a letter from the Board. No one has had time to discuss it or process it. But since we're meeting here and clearly we're giving you the implications that we're moving forward, I thought it only fair to share with you the letter that we just received. And of course, I am speaking in my personal capacity. Thanks.

ALAN GREENBERG: It's always fun watching history unfold, and sometimes a little bit scary, as we know from the real world. Thank you very much.

UNIDENTIFIED FEMALE: [inaudible]

SÉBASTIEN BACHOLLET: Sometime, we use tools or we don't use tools, and I was the first one to raise my hand. That's okay. I'm sorry to interrupt you, but I would like to be sure. Is it SSAC or RSSAC? You know here, we are different language speaking, and I would like to be sure which group asked for the review to be stopped. I am not sure that I have understood.

ALAN GREENBERG It is a letter from SSAC.

SÉBASTIEN BACHOLLET: Okay, then it's one where our liaison will become Chair at the end of this meeting.

ALAN GREENBERG: Vice Chair.

SÉBASTIEN BACHOLLET: Vice Chair, sorry. Okay, is one of those two letters already public somewhere in ICANN website? I know that it's not – sorry, Denise, to ask you this question. It's maybe to staff, but if you have any idea....

ALAN GREENBERG: ICANN correspondence page.

DENISE MICHEL: Depending on the content of the correspondence, apparently it can be quick or it can take a long time to be posted. But I'll forward the letter that we just received to Alan since ours is a publicly archived e-mail list.

ALAN GREENBERG: Yes. Sorry, I was talking about the SSAC letter. I thought that's what he was asking.

DENISE MICHEL: Yes, so the SSAC sent a letter to the Board, and then the Board sent a letter to us. So there are actually two letters. I'll forward them.

ALAN GREENBERG: Both of those are I believe on the correspondence page. I've seen one of them, and I think the other one is as well, but I haven't checked that. Thank you very much.

DENISE MICHEL: Thank you.

GEOFF HUSTON: Thank you.

ALAN GREENBERG: Jonathan, are you going to work from there? That's fine with us, I think.

JONATHAN ZUCK: I think we have some slides someplace. In the meantime, I'm really excited about the newly formed Review Team review process Review Team that's going to be forming shortly.

UNIDENTIFIED FEMALE: [Rude.]

JONATHAN ZUCK: My colleagues I think will probably sit down there. So just because we're short on time, I'll just start talking while we find the slides. If you recall, the last time we spoke, we had just submitted for public comment a draft report form the CCT. My name is Jonathan Zuck, by the way, the Chair of the CCT Review Team. And we had just submitted that report for public comment, and we received a number of very useful comments as a result, and we're beginning the process of digesting and incorporating those thoughts into our final draft.

What was happening simultaneously though were there different sets of analyses that were going on that would

ultimately find their way into the report, and it occurred to the Review Team that those additional sections of the report wouldn't have gone before the public unless we had another little mini public review process. So that's what we'll be starting here very shortly after the meeting, is a 30-day process to go over some addendums to the draft report, if you will, that are specific to three areas.

One is parking, one is DNS abuse, and one is rights protection mechanisms, specifically a survey that was fielded by INTA to its members about some of the costs incurred by trademark owners because of the new gTLD program and a little bit of how those costs have been reallocated to different types of activities instead of just purely defensive registrations and things like that. And so we have those three sets of analyses. We've made some adjustments and additions to the report because of them, and so that's what we want to talk to you about today. Then we will put those new sections up for public comment for a truncated 30-day review, incorporate those things and pull it all together into a final report, hopefully before too long.

I'm pretty sure that we typed out the draft charter for this Review Team on a manual typewriter before the Internet was invented. I don't see slides yet. Are those our slides? Maybe?

UNIDENTIFIED FEMALE: Yes.

JONATHAN ZUCK: Oh, cool. Excellent. So maybe we just jump down to the first parking slide, and we can deal with the timeline at the end, I think. Basically, the parking issue is something with which everyone is familiar and everyone has an opinion about. In their head, sometimes it's not an opinion, it's a fact, and we're trying very hard to do research on this. One of the first things you notice is that the majority of domains sold, both in legacy and new gTLDs, are parked if you give a pretty broad interpretation of what that means. In other words, if they're not the primary identifier for a particular website, then they're parked in the broadest possible [thing.] Somewhat more of them are parked in the new gTLDs than they are in the legacies, but the truth is it's the majority in both cases.

One of the things that our team struggled with is that our mandate is specifically about the impact felt as a result of the new gTLD program. In other words, what changes to competition, consumer choice, and consumer trust came about as a result of the new gTLD program? It's clear that parking is something that, while wildly interesting, is not new and even the fact that it's most website registrations is not new either. But

there was slightly more of them, about 20% more parking, if you will, in the new gTLDs.

There's a lot of potential explanation for that in terms of speculation or something like that. So we did take a look at this in a very cursory way just to see if there was anything that jumped out at us from the standpoint of some correlations to lack of renewals or something like that that might affect our analysis about competition and consumer choice.

What we did find is a lot of different hypotheses about whether parking is actually good or bad for competition, and we didn't immediately see support or data jump out at us to support any of them. So after all of that is said and done, we don't have a big conclusion about parking, except that it's a big, interesting thing, but that even if we looked at the worst case and excluded all parked domains, we still would draw the same kind of conclusions about the increase in competition associated with the new gTLD program.

So from that standpoint, it made sense not to fall on our sword about parking in particular because while it is an interesting topic to the community as a whole, it's difficult to identify the specific interaction of the new gTLD program to parking. There are somewhat higher rates, and then also malware, we found in the DNS abuse survey, is marginally more likely to occur in zones

with higher parking rates. So there is this correlation between the two, but it's fairly slight. It's not a deep correlation. And so there's still a lot more thought and work that needs to go into parking, and it's something the community might want to take up, and maybe even a future CCT Review Team, but it didn't seem like there was enough to this issue that we could tie directly to this new gTLD program.

So if we go to the next slide, you can see that our recommendation is really to collect ongoing data with respect to different parking rates so that analysis can be done with data as it's collected and that it doesn't require trying to recreate the past, which is some of what we had to do to come up with the legacy numbers. And so there's good consensus on the team, but basically, it's an ongoing data collection exercise. We didn't reach any conclusions about parking specifically as it related to an impact felt as a result of the new gTLD program.

To talk about DNS abuse, I'm going to hand it over to my esteemed colleague, Laureen Kapin from the Federal Trade Commission.

LAUREEN KAPIN:

Hi, folks. I'm going to try and shorten things a little bit on the fly since I know we're a little bit short on time. So you can progress to the DNS abuse section. I'm channeling my colleague, Drew

Bagley, who actually was very focused on this issue. I was focused too, but not as much as Drew.

Basically though, we were looking at the question of, were new gTLD safeguards effective in mitigating and preventing DNS abuse? And by way of context, there were a number of additional safeguards baked into the contracts for new gTLDs, and we were really wanting to look at those to see if they made a difference in the levels of DNS abuse that were present in new gTLDs as compared to legacy gTLDs. Next slide.

In terms of DNS abuse, there is no one universal definition, but DNS abuse does capture the use of unique identifiers for cybercrime infrastructure. That includes directing users to websites that enable certain types of crime. The crimes can be varied, everything from fraud, IP infringement, child exploitation, etc. Next slide.

The Review Team focused particularly on types of technical DNS abuse. Those actually have a fairly agreed upon definition, they're measurable, and in many instances the contracts themselves prohibit these activities, and certain jurisdictions also prohibit them as well. These three big buckets that the DNS abuse study focused on in terms of measuring DNS abuse were phishing, malware, and spam. Next slide, please.

The DNS abuse study was published in August. It's a very dense and fact- and analysis-filled study, and I urge you all to look at it firsthand, but the analysis included absolute counts of abusive domains per domain and registrar abuse rates. It also looked at the issue of whether there was a correlation between abuse rates and privacy proxy services – there was not – looked at geographic locations and also looked at two different types of DNS abuse depending on the way the DNS abuse operates, malicious registrations – so those are domains registered for bad purposes, that's the intent in registering the domain – and then compromised domains, legitimate domains that are attacked and then used for illegitimate purposes. Next slide, please.

In terms of findings, the findings were actually very interesting. The good news is that DNS abuse did not increase overall. Even though there was a huge increase in the number of gTLDs, the amount of abuse did not increase. I guess the corollary here is perhaps not so good news is that we didn't actually see a decrease in abuse in the new gTLDs despite the fact that they had additional safeguards. But we leave open the question of different ways to measure that and further increase, so it's not a comment on the efficacy of the safeguards, and we're still in early stages. But that is the headline here, that abuse did not increase for all gTLDs as a result of the new gTLD program.

In terms of what happened in legacy gTLDs, the number of abused domains remains constant. But in terms of the amount of abuse that's going on in new gTLDs, we do see upward trends in phishing and malware domains. In terms of spam, we also see some interesting things. There's a relationship with the new gTLD program and spam and legacy gTLDs. So we see as spam decreased in legacy gTLDs, it actually moved into new gTLDs. And in terms of spam in new gTLDs, we see the absolute number of spam domains in new gTLDs is actually higher by the end of 2016.

In terms of legacy versus new gTLDs, we see that malicious registrations are more common in new gTLDs, we see that the number of compromised domains is higher for legacy gTLDs than new gTLDs. And in terms of overall rates of abuse, so when you take into account the number of domains overall and specific gTLDs, we see that abuse rates are pretty similar between legacy gTLDs and new gTLDs.

Here are some highlights of factors that correlate to DNS abuse. Next slide. These are some of the most interesting findings in the study because these really focus on takeaways in terms of potential future policies. These are things that did have a correlation to actually impacting DNS abuse. So we see that registration restrictions actually correlate with lower levels of

abuse. The stricter the registration policies, the lower the level of abuse, so correlation there.

Price matters. Operators associated with highest rates of abuse often offered low prices. And then we also see trademarks being used as bait, so maliciously registered domains often contained strings related to trademarked terms. So these were factors that appeared to correlate to DNS abuse. Next slide, please.

Based on the results of the DNS abuse study, one of the concerns that we identified in particular – and this is called out in the study – is not all gTLDs have abuse. And in fact, there's a significant percentage of gTLDs that don't have any abuse. But on the other hand, there are high levels of DNS abuse concentrated in a relatively small number of registries and registrars, and sometimes that DNS abuse despite being much higher than the rest of the DNS appears to go unremedied. So many of our recommendations really focused on trying to get at this issue.

Our recommendations really want to encourage proactive abuse measures; introduce measures to prevent DNS abuse; and ensure that data is collected, published, and, importantly, acted upon. And then also, we have one recommendation that considers an additional means to deal with registry operators or

registrars who haven't effectively mitigated DNS abuse. So now I'll turn to our recommendations briefly. Next slide.

We want to encourage proactive anti-abuse measures. We want to figure out how ICANN in discussions with registries and registrars can negotiate provisions that actually create incentives to include proactive anti-abuse measures. That could include financial incentives.

We also really want to prevent systemic use of contracted parties for abuse. If there is information that specific registries or registrars are havens for bad behavior, we want to make sure there are provisions in the contract that actually allow ICANN to get at that behavior through its compliance process and hopefully stop it. Next slide, please.

The issue of information and data is of course really important. We want to make sure that ICANN is collecting information and publishing information that actually shows which are the registrars and registries that may be havens for bad behavior. So one, collect the information; two, publish it; and then three, again, make sure that this information is acted on by ICANN Compliance.

And then finally, we have consideration of an alternative mechanism to combat excessive levels of abuse. So a DNS abuse dispute resolution policy could be considered by the community

to deal with registry operators and registrars that are identified as having excessive levels of abuse. This would be an alternative mechanism to combat this abuse and, again, this is a recommendation that really puts this out to the community to debate and consider this.

So that's in a nutshell the recommendations and information that are present in our next version of the CCT report dealing with DNS abuse. Folks, I don't know if we're doing questions at the end.

JONATHAN ZUCK:

We can have it however you want. I guess I'll also just draw attention to this DADRP recommendation, that it's the first time that we didn't reach complete, unanimous consent about something. So there may be division in the community about whether it's a good idea, and I really want to draw people's attention to it because David originally drafted it, but it's kind of a Hail Mary because of something that's observed, such high abuse in certain TLDs, and it might be time to get creative and step outside our comfort zone to try and solve it. And then David Taylor from Hogan Lovells and the IPC is going to work on the rights protection area, unless you want to do questions as we go. Up to you. Okay.

[DAVID TAYLOR:]

I've also run out of time before I started, I guess. So yes, rights protection mechanisms. The CCT Review Team was looking whether the rights protection mechanisms that exist or were newly created are encouraging a safe environment and promoting consumer trust and also looked to measure the costs on trademark and intellectual property owners.

How did we go about doing this? We looked at the CCT metrics reporting, the INTA impact study which has already been mentioned which was long awaited, a previous ICANN RPM review, and then the reviews we've seen on the Clearinghouse already. And there's also the parallel working group with the RPM Working Group, so we're trying to keep an eye on that as we go. Next slide, please. Thanks.

On the INTA survey, this came about because there was concern on many occasions about the costs of this expansion of the new gTLDs, etc., and really looking to assess whether those concerns were real or not real and look at the additional costs and efforts which have been required. So INTA members were surveyed as to capture all their costs over the last two years. It was a very complex questionnaire, and 33 responded in total so we're low on response rate, which is why this is something which we've put in as an indicator of trends. There's not really enough data there to say this is the absolute way things are, but it certainly

does indicate. And some of the key takeaways are in the draft report on that.

The main reason for brand owners is certainly defensive purposes. No brand owners were saying, “Yes, this is great, it’s another option, it’s more choice.” The finding there of commonly parked, a large number of the domain names [aren’t] exactly saying the same as we found with the parking study. Increase the overall costs of trademark defense. Interestingly, 75% of cases brought involving privacy proxy services, that’s certainly something we’re seeing more and more. It’s way different to what it was five years ago, for sure. And RPMs generally considered to have been helpful in mitigating, so a positive side of that at least, that the RPMs that are in place are helping. Next slide, please.

Looking at some of the ICANN metrics, a number of cases filed looking at the UDRP and the URS, in the year before, there were only cases filed. In 2013, there were 3371 filed, and then the cases have gone up in total. You can see on the right the total cases combined have been going up fairly considerably. Year on year it’s going up, that’s the main thing. Depending where you take the baseline, if you compare 2016, we’re at 36% increase over the year before new gTLDs. If you look at a mixture of 2012-2013 figures, it’s 25% over. No doubt that it’s going higher, but

that's normal because the number of domain names in the root are going up, so there's no real surprise there.

The question is really, is there proportionally more trademark infringement in new gTLDs than old legacy TLDs? That's something which the ICANN data doesn't give us, but we've drilled down into WIPO data which is available publicly. If you look at the WIPO case load, in 2016, 18.6% of their case load involved new gTLDs, and at that same time period at the end of 2016, 14% of the gTLDs were new gTLDs. So we do have proportionally more trademark infringement. It's not massive, but it's significant. It's certainly not going down. So you take away what you want from that.

One of the key things I think is that the UDRP and URS are only part of the costs to brand owners, so it is a measurement, but that's something that the INTA impact study was trying to get you because you can do a lot of other things apart from file a UDRP and the URS. And certainly, in conclusion the URS doesn't seem to be popular. It's pretty flat, 5% of cases, so it's not on the rise or doing anything which many thought it would. Next slide, please.

On the conclusions, increasing numbers of disputes since the introduction of the new gTLDs, trademark owners are using a variety of different things, more trademark infringement

generally. The impact study was good, needs to be more sure friendly. URS is questionable, and the Trademark Clearinghouse, we think there needs to be a cost-benefit analysis on that to see really on its usefulness.

On the next slide, if we can, I'll just highlight the recommendations. These are the recommendations. The first one is to repeat the impact study and do that regularly every 18-24 months. Go to the next slide. And then Recommendation 41 is a full review of the URS, so we're looking at that and also how it interacts with the UDRP. That's to the GNSO. The next slide, please. The last recommendation is the cost-benefit analysis of the Trademark Clearinghouse. So I'll be brief and we can all read those, but I'm happy to take any questions or continue the route.

ALAN GREENBERG:

Thank you. We started a few minutes late and we'll go for another five minutes at this point, and we're going to run badly into the break after our next speaker. So that just gives the At-Large folks a notice that we'll have a five-minute break instead of 15. I have one very brief question, and I really just want a yes or no answer. There's a fellow named John McCormick who's collected a huge amount of statistics, including on new gTLDs. Have you interacted with him at all?

[DAVID TAYLOR:] Yes.

ALAN GREENBERG: Okay. Thank you. That's a good thing, rather than not being aware of it. Dev?

DEVANAND TEELUCKSINGH: Thanks. Thanks for the presentation. I guess I have three questions on all three things. Regarding the rights protection mechanisms, URS versus UDRP, I thought the URS was meant to be a quicker, less expensive method of dealing with trademark disputes versus the UDRP. Has there been any analysis as to why that has not turned out to be the case?

The question regarding the DNS abuse, there was mention that a small number of registrars are responsible for a high level of abuse. Do you have a metric? Like 99% is caused by only three registrars or something like that, some idea of that imbalance.

And the first part regarding parked domains, I saw the use cases mentioned on the slide. I thought one legitimate use of parked domains is that when a company or organization rebrands and therefore they're changing their name or they want to use a new domain name to focus that they're now part of – be it a new

gTLD or they want to be more associated with a ccTLD. So they may register a gTLD for example and decide to want to use a new gTLD because it more goes with their brand or whatever. Therefore, they switch to the new domain and then keep that domain basically as a reserve to ensure that their URLs don't break and so forth. Isn't that a legitimate use of parked domains? Thanks.

JONATHAN ZUCK:

Thanks for your questions. I guess there are a couple of questions about URS and UDRP. I'll just very briefly say that there are all kinds of legitimate uses of parked domains. There are people who are just using them for e-mail for example, and therefore it's not pointed to a site. There are people who are using it as a new brand and they're waiting for the rest of the site to catch up because there's no cost essentially of keeping their old domain. Those are the things that complicate that analysis, and so parking is in and of itself sort of a complicated term that's difficult to define.

Some people would say that it's just the use of monetized parking sites is all that you should consider when treating parking. It's difficult to nail down a definition that everyone can agree with, but there are lots of legitimate uses for parked domains. That was the whole point, that we came away without

a value judgment about it because there wasn't anything particularly bad about them and they didn't have a huge impact on our competitive analyses which we were trying to figure out.

LAUREEN KAPIN:

Quickly an answer to your question about DNS abuse. The study is your best source. I can quote you some general statistics, but there are all sorts of very specific charts that drill down, and that's what I would say would be your best source. But for example, five new gTLDs suffering from the highest concentration of phishing attacks also owned 58% of all blacklisted domains in new gTLDs. So you see a commonality of bad behavior there.

Spamhaus blacklisted at least 10% of all domains registered in as many as 15 new gTLDs at the end of 2016. That's another concentration. And then some new gTLDs on the good side, about a third, didn't experience any levels of abuse. Those are just some very high-level figures, but the study itself does actually name names about certain problematic registries and registrars.

ALAN GREENBERG:

We have time for one very short question and answer.

[DAVID TAYLOR]: [I haven't answered my question yet.] I've got my last bit on the URS.

ALAN GREENBERG: Oh, sorry. Then very quickly, please.

UNIDENTIFIED MALE: So yes, on URS, there's no study per se on that. That's what needs to be looked at as to why. There's a lot of anecdotal evidence coming from brand owners and general use. I mean, it's many reasons. It is supposed to be shorter, quicker, and cheaper, which it is, but it's more complicated. There's an appeal process, there's no transfer at the end of the day. Those are all issue with it. And it's just less well known as well. The UDRP is known, tried and tested, and the URS has come along and it's very similar, but has issues.

ALAN GREENBERG: Any further question? Thank you then.

JONATHAN ZUCK: Thanks. Please take a look at the addendum when it comes out and provide public comment.

ALAN GREENBERG: Our next speaker is Bryan Schilling, Consumer Safeguards Director, and I will give you a few minutes. We do have....

UNIDENTIFIED FEMALE: Excuse me, Alan, we have one question in the chat, if I could read it off.

ALAN GREENBERG: I'm sorry.

UNIDENTIFIED FEMALE: It says, "Do you recommend that domain name costs should be higher as an alternative to address domain name abuse?"

ALAN GREENBERG: I'm afraid it's a bit too late at this point. And again, I'll introduce Bryan Schilling. We have about 20 minutes until the official break, a 15-minute break, and we do have to start the next meeting pretty much on time. I don't mind going into the break. We may find that some people are leaving partway into it. I'll turn it over to you to let us know what's new in your area. Last time we spoke to you, you were effectively brand new here, so now we want to hear the long list of great things you've done, or whatever.

BRYAN SCHILLING:

Thank you, Alan. I think the first thing I'll attempt to do today consistent with my title is to safeguard your full 15-minute break. I actually don't think we'll take the full time. It will depend on your questions and feedback because that's really what we've been seeking, is community input into really how should the consumer safeguards role – which is new to ICANN, and as I understand it largely driven by the ALAC and the GAC – really what should we focus on?

It's separate from the Contractual Compliance department, so we don't see it as having any real connection there in terms of enforcement powers. We're not there to go out and actually go after registrars or registrants but really to facilitate a community-wide discussion about gaps or other areas to focus on to enhance consumer trust in the DNS and unique identifier system.

So with that, since I've had the opportunity to speak with you in Johannesburg, we did a compilation or a summary of the current safeguards that are within ICANN's remit, and we published that. We looked at the articles of incorporation, the ICANN Bylaws, as well as the contracts and produced a summary of what we thought are safeguards that are currently in place. The objective behind that task was to then move to a discussion forum which we held on 25 September.

Backing up a bit, we were talking about having a working group, but we stepped back from that to start off with a bit more of an informal, more of a relaxed discussion forum to encourage participation and not have it be so structured, and moving forward to something with the thought of if organically the discussion moves into a consensus within the community about having to have more formal conversations and more of a movement to a policy PDP, then that would just happen organically.

So on 25 September, we did have the webinar. We had a good turnout, I think around 100 participants, but what we still are seeking is direct input on the safeguards and some of the questions that we raised during that webinar, which were around what are the thoughts of this summary that we've put together? Are there gaps within the safeguards that we should be discussing within the community? And what are some of the other expectations or thoughts that the community has in respect to this role?

And then we also put out there that this role is one of a research assistant. If there are facts that need to be gathered for the community to further discussion in this space, we view the consumer safeguards department as being a place where we can go out and conduct that research to generate the facts to move towards facts-based policymaking.

So really, what would be fantastic is to hear from the ALAC in terms of any thoughts that have been had about what we've done so far or what we haven't done so far if there are things that were expectations that we haven't met, would be fantastic. I think the webinar maybe was too large of a group to get that direct comment and feedback. So with that, Alan, I would open it up to questions and comments.

ALAN GREENBERG:

And I open the floor. You've either done a great job, or you've completely baffled them. I'm not sure which. I'll put a different question to the group: did any of you participate in the webinar? Would you like one of our own? Would you participate in it if we asked Bryan to do something tailored for us?

Now, I will tell you a fair number of the people in the room are relatively new, so may not even have known about it. What would you like? We're supposed to be here to protect consumers and users. Bryan was hired partly at a demand from us that ICANN pay attention to things like that. Maybe we don't really need you.

I personally think that this is a really important area for ICANN to take ownership on, and although I don't know the specific targets we should be looking at because that is something we need to investigate, I don't think it's something we want to walk

away from. Am I hearing that we would like at least a tailored webinar for Bryan to present the kinds of things he's been talking about and for us to further pursue them? Will you actually attend it? I see one or two heads shaking. All right, so we have a to-do list. We have an action item staff will note, and specifically to schedule a webinar at an appropriately suitable time for everyone, which is impossible.

BRYAN SCHILLING:

I'd be happy to [do it to] accommodate different time zones. I know that was one of the – we just held one, we missed out on the APAC region but we did record the last webinar which is available. We did a follow-up blog in preparation for a future discussion if you want to go back and take a listen to that.

I think one of the things that – certainly ICANN has a limited remit, and we are obligated to stay within that remit. It's still good to hear if there are thoughts out there about other things on the fringes that are impacting the Internet communications and technology community that ICANN should at least make sure we're aware of and observing because as we have all seen in many areas, sometimes there's a slippery slope side effect, or as we are kind of seeing now with GDPR and the impact there, trying to just make sure we stay on top of things so that as a

community, we're not necessarily in another rush or concern situation.

So that's something that we'd throw out there. Our Bylaws keep us focused on our remit and our mission, and that's where we will stay. That being said, as part of an overall community, if there are things to be aware of, please bring that to the discussion or raise them now.

ALAN GREENBERG:

I think one of the relevant things is, yes, we have a limited remit, but as we've just heard from our previous speakers, spam and phishing may be out of our domain, but domain names are used heavily to enable this kind of thing. Domain names are used heavily to enable botnets and a variety of other malicious things that go on, and I don't think we can afford – I don't think we should ignore the fact that we are complicit in it. And can we do anything which would impact this in a positive way? Sébastien, please.

SÉBASTIEN BACHOLLET:

Thank you. I'm annoyed about the fact that we don't have anything to discuss right now, but perhaps we could take the chance to consider how we prepare this kind of meeting. Perhaps we should have organized a specific webinar on these

issues before coming here, and it would have been a bit simpler to exchange with you right now had we done so. I think your work is absolutely essential. It is crucial to us, and what end users have to say on this matter I think is extremely important.

So we're not discussing or bringing new ideas to the table here, which is a shame, but it's not because we're not interested in this issue. It's rather because we're not sufficiently prepared and given that we've started early in the morning and we're down to the 10th or 12th subject and we're not knowledgeable about everything, so that complicates matters a bit. Thank you.

ALAN GREENBERG: Indeed, correct. Anyone else like any input or thoughts on how to proceed? Otherwise, we will have a longer break. Nobody? Narelle?

NARELLE CLARK: I'm just thinking now about the review of consumer safeguards that's happening within the Australian context, so I'm here with that shopping list in mind. Where can I go to look for good reference material on this particular topic across the rest of the world? Where do I look for good models? What's robust? Where do I look for numbers, statistics? What's effective, what doesn't

work? What could work, what might not work? What's been thought of but not tried? Etc.

BRYAN SCHILLING:

I think I have some homework. I think to the point of Alan [bringing up] the CCTRT [just here,] we now have this role and this department starting within ICANN. We also have OCTO developing their DAAR tool, which I know they're presenting it a bit. So I think there are a number of efforts underway across the community to start focusing in on abuse and the DNS role in that space. I'm a little bit personally more familiar with my background with some of the other efforts in the ICT. If you look at some of the big players and looking at transparency reports and looking at EFF's "Who's got your back?" ratings, some of their efforts to push this discussion earlier in the ICT space – I don't want to name anyone in particular – but a number of companies and entities now have these transparency reports and efforts are underway.

Some of it more recently seems to be in response to potential government regulatory activity to regulate content, in particular hate speech and terrorism-related, but we've seen that in the past. I know Australia in particular has been looking at efforts over the years in terms of data retention and cross-border warrants, but again, that's a different topic. But still, at the end

of the day I think it comes back down to what is safeguarding, how big does that go?

But that's a really good research assignment, and I appreciate that suggestion, and we'll get back to the community in respect to that.

ALAN GREENBERG: Sébastien?

SÉBASTIEN BACHOLLET: Thank you. I'd like to suggest that we consider the matter inversely. What do you expect from us as representatives of end users, and how can we interact in a way that is effective, useful, smart, with the work that you do for ICANN?

BRYAN SCHILLING: Thank you, Sébastien, and for your comments earlier too about this being important. I know it's important to the organization and all of us as being end users, it is important to us and future generations being able to be safe on the Internet. I think I said it in Johannesburg: some of this is trying to figure out how we avoid boiling the ocean here and focus in on some aspects so that we can collectively have some measurable results.

Some of it is, what is the most important to the end user? Is it focusing in on malware and botnets? Is it having a discussion about content regulation and spam? Because there are certainly some very important interests across the community that are concerned about content regulation, and that is a gray area and a fine line that I think we do need to certainly be aware of and cognizant of, and have a community-wide discussion on that area.

So figuring out how to have that dialog so that the consumer safeguards department within ICANN is working for the community to facilitate those discussions and focus in on what's most important to the community is very important. And perhaps other suggestions, I'm open to that.

ALAN GREENBERG: Anything further? Go ahead.

SÉBASTIEN BACHOLLET: I will say it in English this time because it's need to some diversity. I was wondering if it could be useful – and I am talking more to Alan and to ALAC – if we have what I will call a point of contact about this subject within our part of the organization. Is it something that could be helpful for your work, or is it a bad idea? Thank you.

ALAN GREENBERG:

For clarity, are you meaning someone on the ALAC or whatever who's sort of on a regular contact with him? In theory, I do that, except I've been too busy on other things in the last couple of months. But if there's anyone else certainly with an interest, we can share the load. We will be going into a new ALAC at the end of this week, and that's certainly something we can look at.

The subject actually will come up in our discussion on working groups. And if you've read the briefing paper, you've seen it already did come up in the concept of subject matter experts. So I think we may have an appropriate way of doing that, and I think that's probably a good idea. Anything further? Go ahead, Bryan.

BRYAN SCHILLING:

No, I think that's a good idea as well, so long as within the other representative groups, we could also maybe get more of a focused area so that we've got transparency and uniformity across the groups. That would be fantastic. So as I'm speaking to other groups, if it's all right with you, Sébastien, I'll raise that idea as well.

ALAN GREENBERG: You had said you were originally thinking of some sort of small think tank working group. Are you thinking about reviving that concept as we go forward?

BRYAN SCHILLING: I think we'd certainly be open to that. The large webinar that we had was great to have the participation. Maybe it was too big of an environment for such a large number to feel comfortable speaking up, so if we have consensus across the various constituencies that a smaller think tank would be ideal, then I would certainly be open to that as well.

ALAN GREENBERG: Thank you very much. With that, I'll close this session. We reconvene in a little over 15 minutes. We are looking at essentially a review of the CCWG Accountability Work Stream 2 subjects and a few related things. There is also a public session, but I think this one is really important because it will give the At-Large perspective on a lot of these things, and I think will be a good primer for going into the public session. So I encourage everyone to be here. Participation at this table is a little bit sparse, and I think Sébastien is right, it has been a long day. I don't know how to make them shorter however, but try to get things accomplished. So I close this session. We reconvene in about 15 minutes. Thank you, Bryan.

[END OF TRANSCRIPTION]