

Adigo
nashtonhart _ 2009-06-10 0700 APT _ 1008538 _ 230218

Conference Participants listed alphabetically:

.....

Adigo operator
Cheryl Langdon-Orr
Darlene Thompson
French Channel
Garth Bruen
Gisella Gruber-White
Greg Ratray
Marika Konings
Matthias Langenegger
Sebastien Bachollet
Spanish Channel

.....

Greg: I'm ready, if you think we have the people that are likely to be here.

Cheryl: Ah, well -- that's one of the greater mysteries of life, I'm afraid.

Greg: [laughter]

Cheryl: Okay. The meeting is being recorded in the Adobe Connect Room. Of course, the audio channels in French, English and Spanish are also recorded.

Greg? The floor is all yours.

Greg: Thank you. I appreciate the opportunity to make this presentation to the committee. I look forward to hopefully more dialogue in Sydney regarding the plan that we're about to talk about, today.

I did want to start a little bit with maybe the genesis of the plan, quickly. Where it stands in the ICANN processes.

The ICANN strategic plan -- and this year's operational plan -- have called for the establishment of a plan. Really, in my mind, to create a foundation for the community about what ICANN both sees as its role in securing the stability...

[Garth joins call]

...and resiliency. We can talk some about the addition of the word, "Resiliency," to the normal terminology of security and stability. As well as giving the community transparency into the specific activities -- and even the resources invested -- in this area of ICANN activity.

The board had seen it a couple of times, and at the April meeting, they reviewed it. We made a focused set of tweaks about DNS at the May retreat. They approved it to be posted for public comment on the 21st of May. Or it was posted on the 21st of May. It's open for public comment through the 19th of June.

The SSAC has the plan and I've had some interactions. I've briefed the SSAC on the plan. I got some feedback that was incorporated in the draft. That is publicly posted. I believe they plan on additional comment.

As well, I've briefed the GAC a couple of weeks back -- really, for information. There will be another session where I talk to the GAC about this plan at the Sydney meeting.

Finally, there's a session scheduled for Wednesday afternoon at the Sydney meeting. Specifically, again, to present the plan and take public comment on it. Within the ICANN processes, that's where the plan is.

As I'll brief, the plan is really considered to be part of our overall strategic and operational planning processes. Assuming that the community is comfortable, adjustments will be made. The plan would be for the board to approve this, and then this plan would be developed annually -- along with our other planning documents.

I've not done a presentation. I've done them on Adobe Connect, before -- but not one that has been subject to translation while I do it -- and recording. So I'm going to try to keep my pace fairly slow. For me, sometimes that's difficult. If somebody believes I've started to speed up to a distracting degree -- including the interpreters -- please let me know, and I'll try to bring it back in line.

Also, normally, I'm a person that likes to take questions during the flow of the presentation. I think -- in this case -- it might be more effective to just let me go through the presentation and hold questions 'til the end. I've got a feeling that the dialogue might make the translation task a little more difficult.

But if anybody feels an imperative need to interrupt me, please feel free to do so.

Because of the nature of the presentation, I'm also going to pretty closely go over each of the bullets that are on these Power Point slides. This will ensure that if the Spanish version had not gotten translated, we'd ensure that all the material on the slides had been briefed during the course of the session.

Does that sound like about the right approach?

Cheryl: That sounds excellent, Greg. Cheryl, here. I really appreciate that.

There is a question, I suspect, will be on some of our language-channel minds. That is asking whether or not the draft [inaudible]

Greg: That was cut off at the end, but I think the question was going to be whether the draft plan had been translated.

Did I get cut off? No?

French Channel: I can hear you. The French Interpreter, Tisha.

Greg: Good. Cheryl?

Gisella: I can hear you. Gisella.

Greg: Okay.

French Channel: And the Spanish interpreter can hear you.

Greg: Cheryl, was it you that...?

French Channel: We can't hear Cheryl. We don't hear Cheryl.

Greg: I think we may have lost her. Shall we give her a moment to return?

Gisella: Yes.

Sebastian: It's Sebastien on my mobile. Sorry to interrupt. But you can go ahead. I think that Cheryl's got trouble, sometimes. She can still hear, but she can't be heard, any more.

Go ahead and she will join us back as soon as she can, I guess. Thank you.

Greg: Thank you, Sebastian, for the recommendation.

I believe Cheryl was asking whether the plan has been translated.

Sebastian: Yes. I think it was a question from Cheryl.

Greg: It was submitted for translation. I'll have to be honest... I haven't had a chance to check in the last week whether the translations have been accomplished. But the intent was or is to have it translated and get them posted.

I will check into that and we'll make sure that you guys get an update on the status of the translated version of the plan.

With that, I'm going to proceed into the briefing. At each stage, I'll say which slide I'm on. I'm going to advance from the first slide to the second slide -- which is entitled, "Principles Guiding Drafting."

In some ways, I think that this is maybe the most-important slide in the briefing, if only because the plan is very much a document that tries to establish what ICANN does, and does in cooperation with others. But also, what ICANN sees as not in its core responsibilities.

I think a major challenge in this realm is to be clear about what you do and what you don't do.

I've briefed the board twice on these principles, and I'm confident that they believe that this is the right kind of foundational approach for this first version of the plan. It's intended as a foundation, again, focused on role-definition and the framework for delineating what could be interpreted in very different ways. Delineating what we do in programs, activities and resources related to security, stability and resiliency.

It's not meant to table new initiatives. It really describes programs and activities already part of ICANN's strategic and operational plans. My rationale there is that while ICANN has long done a series of security-and-stability related functions, they have not been articulated in one single place. In that we need the community's buy-in on a starting point, as we talk about our role in this regard.

In the recent drafting... And this is kind of a legacy bullet... The last bullet on this slide, for the board, on streamlining the document flow...

The subject matter -- like many, in ICANN -- is pretty complicated. So hopefully, the draft that's now out for public comment is a relatively readable document, even for the layman. I probably should have said this upfront, but I certainly encourage feedback from people that get the opportunity to read the plan, and provide comment.

I'm going to move to the next slide.

Most of the remainder of the briefing really parallels, section-by-section, the content of the plan, itself. The first section of the plan is the plan's purpose. It says that the purpose is to delineate the role -- to overview existing programs and activities.

The last portion of the plan, and the appendix that exists in the plan, provides detail on the specific activities and resource commitments that we undertake in FY'10. We'll go into each of those major areas on more depth.

The purpose, also, highlights that integrated is part of our strategic and operational planning.

I've now moved to the next slide, which is, "Challenges and Opportunities." That's Section II of the plan.

This is a relatively brief section. We made the decision that it really wasn't a place where we were going to try to overview the full set of threats to the Internet security and how the unique identifier systems -- the domain-name system[s] -- might be subject to abuse and misconduct.

There are some broad outlines of why that's significant, and becoming more significant in the plan. But it's not a big threat section, in terms of challenges. It does highlight that there is growing misuse of the Internet. That does often leverage unique identifier systems.

It highlights that ICANN has a longstanding commitment to ensure the "stable and secure operation of the Internet's unique identifier systems." And that this plan is intended to provide the community a roadmap for ICANN's efforts in this area.

I will say that -- with much consideration -- we've decided to add the word, "resiliency," to

"security-and-stability," in the plan. The focus there is -- increasingly -- we see disruptive activity, both conducted through the unique identifier systems in the DNS, as well as directed at the domain-name system. In addition to being secure and stable, we need to make sure that system is available, if it comes under attack. We believe that the word, "resiliency," captures that.

With that, I'm going to move to the next slide. ICANN's Role -- Section III of the document. There are five bullets on this side, which I'll basically read.

The first is, "ICANN focuses on its core missions, related to the Internet's unique identifier system." There's more language in the plan. But the focus here is that ICANN's making clear that the scope of its activities need to remain focused. By its legitimacy, they're limited to where its mission area is -- which is the coordination of the unique identifier systems -- with a strong focus on the domain name system.

In terms of where it plays in the broader Internet security realm -- it's not a policeman in operationally combating criminal behavior. It does not have a role, regarding the use of the Internet for cyber-espionage and cyber-war. It does not have a role in what constitutes illicit content on the Internet.

A strong portion of this section is trying to make clear some boundaries around where we're focused, and what activities we're not responsible for leading. Probably a grey area.

There is a grey area, certainly, when abuse of DNS is contributing to criminal behavior, and that abusive behavior needs to be responded to. That's addressed -- to some degree -- later in the plan, here.

Really, in the last bullet, it says, "ICANN will continue to participate in activities with a broader Internet community, to combat abuse of the unique identifier systems that enable malicious activity."

A primary example of that -- and I think the best case study of my couple of years' experience with the organization -- is the activities that undertake dealing with the Conflickr Worm that's still out there on the Internet.

Moving from the slide on ICANN's Role -- Section III -- to the slide entitled, "ICANN's Contributors -- Section IV." This is a pretty short slide. It's actually a short section of the document.

Our principle purpose here was to point out... I do have a small, 4-person staff within the ICANN staff, that's focused on security activities; both internally and in coordination with the supporting organizations and the advisory committees. A lot of work with SSAC and then participate in broader sets of activities, external to the organization, as appropriate within our role.

However, this section basically illuminates the roles of most of the rest of the staff. From the IANA staff to the policy staff that supports the [SOs and ACs] to the compliance staff and services staff. All of these portions of the ICANN staff -- and the supporting organizations and advisory committees -- really play active roles in what ICANN does for secretary and stability.

We serve as an orchestrator and a security staff, for both planning purposes -- and, hopefully, a place where if security concerns are arising, that somebody on the staff is responsible for bringing the whole organization to focus as necessary and useful on those things.

With regard to the supporting committees or the supporting organizations and advisory committees... In this portion of the document, SSAC and RSAC are identified, explicitly. It's acknowledged that all of the SOs and ACs play a role. Some of that is detailed more fully in Sections V and VI of the document.

Is the pace about right? Taking a brief break on the substance? Can everybody understand? Or maybe more easily, does anybody think I need to slow down or conduct this in any different fashion?

French Channel: French, here -- Tisha. It's all right.

Spanish Channel: Spanish is fine, too.

Cheryl: That's just a wonderful reflection on the quality of our interpretation service. I thought you'd be challenged with all the alphabet soup. But, well done, girls!

French Channel: Well, he's also speaking very clearly. We really appreciate that. Thank you, Cheryl.

Cheryl: Well done, Greg, as well.

Greg: Thank you!

I will try to -- on some of the letter-soup acronyms -- be a little bit more fulsome in the development of what I'm talking about, there.

Moving from this slide to the slide entitled, "ICANN Programs," which is Section V of the document. Sections V and VI of the document are the lengthy portions, in terms of the document. Section V really reviews -- to a small degree -- what we've done, but certainly what we are currently doing, in terms of different sorts of programs.

The bullets on this slide don't hit everything in the section. This slide really shows the high points of our program activities.

This slide is really intended to show where we're focused, and where we think we have a more contributory role.

The first bullet is, "ICANN is directly responsible for IANA operations as the highest priority." That is very much a board-directed statement about the relative priority of our efforts to ensure the secure and stable operation of the unique identifier systems.

ICANN is an enabler for the DNS and addressing community efforts to strengthen security, stability and resiliency. Including supporting protocol, to authenticate Internet names and numbers.

While that could be considered fairly vague and conceptual, things like pushing for the implementation of DNSSEC -- or Domain Name Secure Extensions -- at the root level. And making efforts to educate the community about the value of the implementation of that technology and that protocol. In order to help with the security of the DNS, and combat things like cache-poisoning and misdirection of domain-name resolution. That would fall in this second bullet.

ICANN is an enabler and facilitator of the security, stability and resiliency activities conducted by the registry and registrars. This is a collaborative activity in name. Though, with the generic top-level domain operators, there is contractual obligation and compliance aspects to these activities, as well.

ICANN is directly responsible for the secure, stable and resilient operation of its own assets and services. We'll talk a little bit about that further on. We do believe we're a key participant in broader forms and activities related to security, stability and resiliency of the Internet's unique identifier systems.

The main name system, while a fundamental part of the Internet, isn't all that well understood at the technical and operational levels, by many people -- including people in the security community.

We believe it's important to participate in forums. Certainly, the Internet governance forums - like the ITF and the IGF. Also, security forums -- like the Forum on Incident Response Team, and the activities we've conducted related to the Conflickr Worm. In order to make sure that the communities both understand what's going on, as well as provide assistance and technical advice about how the DNS can be secured, and not a place for abuse.

With that, I'm going to move to the next slide -- which is entitled, "Major Program Elements."

This slide isn't really well-designed to be read. It really provides the headings of the different portions of Section V of the document. Without reading each individual numbers, I'm going to try to walk us through what we identify as the "Program Elements."

The first major element is "Core Domain Name System -- Addressing Security, Stability and Resiliency." The two focus areas within that are IANA -- the Internet-Assigned Numbers Authority Operation. And the Root Server Operations.

The second major portion of the program is identified as work with the top-level domain registries and registrars. The major sub-elements are ongoing work with the gTLD registries. The efforts regarding the standup of new generic, top-level domains and internationalized domain names.

The work with the gTLD registries efforts that ICANN has ongoing, related to contractual compliance... This is where issues related to "Whols" are addressed.

Protecting gTLD registrants. The collaborative work we do with the country-code top-level domain operators. The fact that IANA has technical requirements, in terms of being put into the root zone. That adds to security and stability.

The emergent role that we've had in collaborative response to malicious abuse of the DNS -- again -- prompted by some of the recent activity with Conflickr. Then, our role in enabling overall DNS security and resiliency.

I'm going to move to the next slide, which I believe is the remainder. It outlines the remainder of Chapter V. There are four major headings on this slide. The first is "Engaging with the Number Resource Organization." The NRO and the Regional Internet Registries and the Addressing Space.

To be clear here, as we discussed this portion of the plan and what we're doing, really it was identified as an area where we needed to try to reinvigorate this contact with the NROs and the RIRs, related to security and stability. There are not a lot of active efforts in that regard. That's not necessarily a good thing, and we need to at least engage them, to see where collaboration might be initiated.

The next major heading is our "Corporate Security and Continuity of Operations." We do have a director of Security Operations, who is internally focused now for ICANN, [ensuring that we've had security programs]. Like many organizations, they certainly stand to be improved. We're improving those, as well as putting an increased focus on our continuity planning for the operational functions -- like IANA. Particularly, in our roles with Root Zone formation, and potentially, with our roles with DNSSEC operations at the Root Zone.

The next major heading details activities related to supporting organizations and advisory committees. The ALAC is specifically identified there.

The last section of the document is "Global Engagement to Enhance Security, Stability and Resiliency." That really talks to our global partnerships and regional liaisons. The activities conducted through Theresa Swinehart 's team, and working with both organizations like ISOC.

The work that ICANN has long done with regional network operator groups and regional CCTLD associations -- as well as identifying that ICANN does work with governments through the GAC. The security, stability and resiliency of the DNS in particular is a crucial aspect of protecting the Internet as an infrastructure. It's been a rising concern for years. Governments are very attentive to this, globally. We understand that we have responsibilities there, and need to work with governments.

Moving from this slide to looking at the slide entitled, "ICANN Fiscal Year 2010 Plans." "Key initiatives" -- which is Section VI of the document... Another extensive portion of the actual plan. Again, organized around a set of bullets that really try to hit the high points of each major section or each major element of Section VI. I'll probably approach this similarly to the last couple of slides.

Again, in accordance with our priorities, IANA's operations are listed first. The key initiatives include improving root zone management through automation. Improved authentication of communication with TLD managers -- supporting DNSSEC implementation.

The wording in the plan has actually been more prominent, based on discussions with the board over the last month, leading up to the 21 May version that was publicly posted, regarding DNSSEC.

People on the call may or may not be aware there's been a very active phase in our engagement with the US government and Verisign in terms of planning how DNSSEC implementation at the root zone will proceed.

The next section is "DNS Root Server Operations." Here, there's a recognition that we really do need to follow through with the community. It's a loosely-coordinated community. ICANN does not have authorities over the root zone operators. But we are seeking mutual recognition of roles and responsibilities.

As a root zone operator itself, ICANN as the L-Root operator is working on voluntary efforts to conduct contingency planning and exercises.

The next major section are of activities and initiatives related to the generic top-level domain registries. Including establishing processes for applicant evaluation and operation of the new gTLD and IDN applicants. To ensure technically secure operations, and to ensure the protection of registrants. I will say this has become a pretty consuming aspect of both my time and many others on the staff, which we're doing very closely with Kurt Pritz and the Services Staff. The Policy Staff. Much of the staff is very focused on some of the overarching issues related to new gTLD on security and stability. Particularly, how to address the potential for malicious conduct.

Staying in this section of the FY'10 key initiatives... ICANN will mature the gTLD registry continuity plan. We do plan a test of the data escrow system in the upcoming year.

Looking at the next major section, which is the country-code top-level domain registries... ICANN is going to focus its collaboration on maturing a training program that we initiated over the past year on attack and contingency response planning. We've done this really under the purview of the CCNSO, hand-in-hand with the regional TLD associations.

We are working more closely with ISOC on a deeper technical layer. The real focus here is capacity building in the ccTLD that are more resource-constrained. It makes the assurance that those people are giving the training, and hopefully the skills and information necessary, to not make those points of the overall TLD system and DNS weak points, just because of a smaller scale and limits to resources.

Moving to the next slide, which is really entitled the same thing -- with "ICANN FY'10 Plans, Key Initiatives... continued."

[laughter]

There are four bullets on this slide, so I'll just hit those in a similar fashion.

Contractual compliance. ICANN continues to increase the scope of the contractual enforcement activities. The staff has been incremented up of late. I believe the operational plan for FY'10 -- assuming its approval -- calls for at least two additional staff members.

The real focus there is the ability to conduct audits, as part of implementing the recently board-approved, '09 RAA amendments. To really try to identify the potential involvement of contracted parties and malicious activity. And to undertake compliance actions as warranted.

The next major bullet is, "Response to Malicious Abuse of DNS."

As I can talk at-length during the question period, we have conducted a pretty vigorous effort in terms of collaboration with the TLD operators. Particularly the ccTLD operators, in trying to block the use of DNS in both the control and spread of the Conflickr worm. If necessary, I can explain a little bit more about what the Conflickr worm is.

It's become pretty clear that there's a strong call both within the DNS community, as well as security community, wanting the ability to reach across the operators of the DNS. To collaborate when events like the Conflickr worm happen. There have been other worms. One was named [Zurisbi]. Another had to do with the operations of a registrar named [Macolo].

These collaborative responses have proven important portions of the overall Internet security picture. We plan to continue figuring out how we enable collaboration within the DNS.

6.4 is the bullet entitled "Internal ICANN Security and Continuity Operations." This is really the internally focused operations that we've stepped up on. The bullet reads, "ICANN will ensure security programs are conducted within overall corporate risk-management." The board has just [stood up] a risk-management committee, which will have its second meeting at this Sydney session.

Crisis Management and Business Continuity Programs. Our major focus for the coming year is to ensure that we've got a strong set of documented plans and supporting procedures for these sorts of programs.

Then finally, the last bullet on this slide... You can see I'm starting to slow down a little. It's been a long time since I've talked so much in a one-way direction.

[laughter]

Hopefully, I'm still doing okay.

The last bullet on this slide is, "Ensure Global Engagement and Cooperation," which reads...

ICANN will further extend the strong partnerships and engage in global dialogues to foster the understanding of security, stability and resiliency challenges -- and improve response capabilities.

That's all pretty generic language. But in that section of the plan, it identifies the Global Forum for Internet Response Team as a collaborative partner. Regional organizations within the European Community. There's an organization named IMPACT, which is headquartered out in Malaysia. Really, to explore how ICANN enables -- with its expertise in its core areas - - the DNS. Global activity to improve or enhance security, stability and resiliency.

With that, I think I'm getting closer to the end. How are we doing, time-wise? We're doing all right?

Cheryl: Yes. You're doing fine.

Greg: The next slide uses a format that I'd used in previous professional experience, to try to provide a snapshot or overview of different aspects of an operation. To identify objectives, deliverables, key stakeholders and resources.

The last slide here in the brief really shows you an example of what is in Appendix A of the document. For all of the -- I think -- 11 distinct programs, what we've done in the plan is really show you for the FY'10... For those who may or may not know, ICANN runs on a fiscal year that goes from July through June. So, Fiscal Year '10 -- assuming board approval of the operating plan -- would begin in July of '09, and extend through June of 2010.

The appendix of the plan provides detail on what we're doing in each of the programs. To include the resources down at the bottom right corner of the slide that are allocated to different portions of our security activities.

With that, I believe that's the last slide. Yes. That is the last slide.

I'm done with the briefing, and certainly stand ready to answer questions, or engage in a dialogue.

Cheryl: It sounds like we should give you a few moments' deep breathtaking. That was quite a marathon, but I must say, a huge amount of very important information.

Is there anyone who wishes to raise some questions or formulate their questions, or make some comments while Greg catches his breath?

Spanish Channel? French Channel?

Spanish Channel: No one in Spanish.

Cheryl: Okay.

French Channel: No one here on the French, either.

Cheryl: Okay. Thank you.

Greg, how much complexity do you see coming in with the IDN world[s] opening up?

Greg: That's a good question.

Some complexity. I'm going to answer this maybe in a little bit counterintuitive fashion.

In terms of overall complexity -- in terms of degree-of-challenge -- to some of the fundamental problems that we have in Internet security, or even in the limited remit of ICANN in the DNS... I don't think IDNs will prove that difficult.

The challenge is going to be the near-term. I think technically, they'll come in and they won't present major stability challenges. We need to be attentive, there. The real near-term challenge will be the potential for confusion. Particularly, for people to take advantage of confusion, to conduct malicious activity.

I think we are aware of that. I certainly hope that both internally, the ICANN staff -- but that the community -- will be pretty hypersensitive at the initial phase. Watching for that sort of behavior.

As we move forward on the implementation planning, I'm actually the person responsible for the overarching issue on dealing with the potential for increased malicious conduct. I think the strong expectation is we're going to enhance some of the procedures that will allow for some more rapid action in the case of potentially identified malicious behavior.

I'll tell you what my gut feeling is, and this comes from my operational experience in the cyber-security area... If we can refine our procedures pretty rapidly, while people keep trying take advantage of confusion related to IDNs, we should be able to keep a handle on it. If we can develop good response procedures pretty quickly.

Cheryl: That's very heartening to hear, Greg. Thanks for that.

I would like to think that -- of course -- our At-Large structures within the ILS communities... We've got 110 -- 120, soon -- community outreach opportunities. Many of which are within the IDN-focused geographies. Maybe there can be a little bit of mutualism developed there, as well. Consumers also need to be warned.

Greg: Right. This is probably not as well-developed as it should be. But working with you all in the ALAC... If there's an opportunity to do some education and awareness-raising, we'd certainly like to add that to the game plan for ensuring that we keep this under control.

Cheryl: I'm fairly confident that the regional At-Large Organizations would be delighted to hear that.

Sebastien has his hand up. Sebastien? Off mute and go ahead, please.

Sebastian: Thank you, Cheryl. Thank you for the presentation, Greg. I didn't have the loop for the Power Point Presentation because I was not on my computer. I am, now. I would like to have the presentation, because I just have the last slide.

On this slide, what struck me is that you're referring to a lot of people inside the staff, but not very much about people outside the staff. I am worried about the word, "Stakeholder."

If an ICANN stakeholder has one meaning, it's the large meaning. It's not the staff meaning. You may try to -- as you need security for Internet, we need security on word use. And "Stakeholders," is really "us," and not "staff." Staff, maybe... No. It's not staff.

[laughter]

I really think that it's great and an interesting presentation. In addition to just what you say, it's not just to educate our members, if I can say that the [ALSs] and RALO are members of At-Large. But it's also true to take opportunity to have people with knowledge on this issue to participate.

I know some of them. One is representing us, and that's great. In [LSAC]. But I know others who have competency in this field, and could also be interested and therefore very useful to have them participate in this work and discussion.

Thank you.

Greg: Sebastien -- I think two things, in response.

As you look at the last slide... And I may have chosen unwisely... But this is just one example of 11 slides that are at the back of the plan in the appendix. It happens to be the one with the internal ICANN focus. Therefore, the "stakeholders," are identified as being very much the internal stakeholders.

Cheryl: Yes.

Greg: If you look at some of the other slides in the actual document, I think you'll see that there's a much broader, externally focused set of stakeholders identified.

That said, we certainly welcome any feedback on the specifics of who the right stakeholders are, identified in the appendix. But Sebastien -- more broadly -- I'd like to leverage as much expertise as is out there. So individuals in the ALAC that want to comment through the public comment forum -- or if they happen to be present in Sydney -- engage in the forum, there.

Or obviously, if ALAC as a committee wants to provide some overall comment, we are soliciting that. We welcome it and would incorporate it into the next iteration of this.

Cheryl: Thanks, Greg.

Just to draw the public record, because that is what we're doing, here... For those of you wanting to drill down to the particular part of the appendix Greg was referring to... That would be Pages 50 and 51 of the 66-page English-language document.

Anyone else on our Adobe Room wanting to raise a question? Or anyone else on any of the channels? Well, I've left a fashionable silence -- so that's all I'm willing to do.

Greg -- another question from me. I suppose I should declare I'm sort of sticking on my ccTLD hat here for a moment.

A number of ccTLD operators -- and the one I'm a board director of is one of them in dot-AU space -- have been involved in a number of security and stability exercises. Blackboard exercises and other sorts of things. That's all very well and good. But it tends to be "like" going with "like."

I noted in your presentation that you mentioned particularly in reference to engaging with ISOC... Where the plan that you've discussed with us tonight is making a point of not having a status and preparedness. Least-developed versus most-developed economy model differentiation, here.

Is there opportunity for ICANN to perhaps do some like and unlike exercises with ccTLD operators? Perhaps one of the smaller kids in camp playing with the bigger kids in camp on the hypothetical...?

Greg: Cheryl, that's a great comment.

I didn't get into it, but in [attack-and-continue to response] planning and training that we have been conducting... For example, we just did one in center, where we actually had more of the advanced people participating. It helped us understand the content of the course better. But certainly, had some of the opportunity for the more well-resourced and technologically mature TLD operators to interact with some of the less-so. Right?

Cheryl: Yes.

Greg: We agree that leveraging the willing ones... because this is a very voluntary program... Obviously, ICANN and the ccTLD space works collaboratively on these issues... would love to leverage that.

I think maybe the follow-through on that -- Chris Disspain's been very aware of what we've done with this program. We're going to talk with the ccNSO and the regional associations again, in Sydney. Maybe they'll work more strongly on that idea. Maybe even identify some kind of...

What's coming to mind is, those more-developed ccTLD operators that want to become active partners in the program. Maybe there's an opportunity there.

Cheryl: Almost a mentoring model.

Greg: Right.

Cheryl: I think the leverage tools and some of the language -- if I may be so bold to share it with you -- that you might want to utilize is, most of the ccTLD operators have a mandate and requirement to interact, interface and look after their local Internet-using community.

That, of course, brings you squarely into our community, with At-Large, the ALAC and the RALO model. That's a leverage opportunity to encourage all of the links -- including the weakest linked groups -- to work on making sure that "we," the end-user, has a reliable and secure and stable... To the best possible set of protections exercised.

Greg: You're on a good theme. One that may need improvement in the document, as well as action in our work in the upcoming year.

The document does reference a symposium that we cosponsored with Georgia Tech back in February of this past year. One of the four focus areas of the symposium was resource-constrained environments. How to do some of this capacity-building.

I'd welcome -- again -- your input as an individual, or a more formal organizational input. To the language of the plan, but also to our actual practical activities in the upcoming year.

I assume you'll be at Sydney. Right?

Cheryl: [laughter] Yes. Well, it's not too far for me to travel, actually.

Greg: Right. Compared to all the other locations we've had meetings.

Cheryl: Exactly, Greg.

But the language you're using -- Capacity Building -- certainly, "we," as in the At-Large Community, need to recognize that that means different things to different people.

When we're looking at our African regions, and there are Asian regions... Coming back to something that Sebastien said... We need to watch the "language" and to ensure that "intent" is properly being transmitted by the choice of word "tools" we use.

Greg: That's fair. I tend to use those capacity-building words maybe too loosely or too blithely. I certainly seek input by people who've been across the globe. Right?

The strength of your organization is, you can help with the right wording that will resonate globally. Again, I welcome you helping me with that.

Cheryl: Looking forward to it, Greg.

Are there any other questions?

Sebastien -- you still have your hand up. Is that because you can't put your hand down on your connection?

Sebastian: No. I'm sorry. It's just because there are too many screens at the same time. I need to do it. Sorry.

Cheryl: [laughter] That's all right. I've stopped clicking people with their hands up, because I end up giving them the microphone, and then I don't know how to get the microphone back from them. So I have a hands-off policy until I learn more about the care and feeding of the Adobe Connect Room.

Is there anyone on any of the language channels that wishes to raise a question or make a comment to Greg now?

Spanish Channel: No one in Spanish.

French Channel: No one in French.

Cheryl: Thank you very much, Ladies.

Anyone in the Adobe Room or on the Channel Phone Bridge?

Sebastian: I think it's a bother, too, because it would be recorded in French and Spanish. The fact that Matthias gave me the link to the presentation given by Greg in French... I don't know if it's also in Spanish, but...

Part of the answer, Greg, to the question asked by Cheryl at the beginning of this call. There are some materials at least in French and hopefully in Spanish, too... It's your presentation. I don't know for your full document, if it's yet in French and in Spanish. But the pronunciation is -- and that's very important for us to know that. Thank you.

Greg: Cheryl, you had dropped off -- but maybe you were listening or came back on. I will get you an update on where we're at with the translation effort. The document was submitted for translation, and I just did not get the opportunity to check on its status.

French Channel: Thank you, Cheryl. The English presentation today was translated into French.

Cheryl: Thank you so much. In fact, the building of those resources through our At-Large and ALAC requirements -- the multi-lingual effectiveness -- I think is a very useful tool. And they're really one of the reasons why excellent presentations, such as Greg has given us tonight, are so incredibly useful.

Of course, this is recorded both in the Adobe Room and in the Telephone Bridge Network. There will be MP3s of this in the three languages. This is a hugely useful resource.

Greg, please make sure that you let the rest of the ICANN community know that this resource is now available for all of our use. Once Matthias gets it up onto the website, of course.

In the absence of any other questions -- and, coming up to the top of the hour -- I would like to thank you most sincerely for what... Well, it's a subject I'm clearly passionate about, so I'm absolutely biased with it. It was a very informative and very welcomed briefing.

If we can ensure -- and certainly I'll be asking questions -- that the French and Spanish translation of the master draft plan are available well in advance (though there's hardly much time) -- or in advance as much as we can to the Sydney meeting... That would be most welcome. We certainly appreciate your time tonight, Greg. We hope that it's not the last time that we can lure you back to do a briefing on this very important topic.

Greg: Cheryl, I appreciate the opportunity. Please lure me back. I look forward to seeing those who will be there in Sydney in a couple of weeks.

Cheryl: It's been our absolute pleasure. Thank you so much.

Greg: Take care.

Cheryl: Okay.

Thank you all. Good morning -- Good day -- Good evening -- Good night. Depending on what part of the world you're in. Bye for now.

V: Thanks Cheryl.

Cheryl: Thank you.

