DURBAN – DNS Risk Management Framework Working Group
Thursday, July 18, 2013 – 09:00 to 10:00
ICANN – Durban, South Africa

CHAIR: Could everyone please take your seats or take your conversations outside. We are going to start this session for the DNS Risk Management Framework Working Group. All right. Welcome everyone to the meeting of the DNS Risk Management Framework Working Group public comment session. As you will recall, this project has been underway for a little over a year now, I think. Actually, longer than that – almost two years now – and we've now reached a major milestone, which is the delivery of the draft final report from the consultants.

Just a very short reminder: the purpose of this project is to develop a framework for risk management function, which will be internal to ICANN. And the study has been to look at methodologies for doing that and make some recommendations for how to move forward with getting that function up and running. We've been quite careful to keep our eyes focused on things within the span of ICANN's immediate control, which is difficult with a system as dispersed as the DNS.

But I think we've succeeded at that. And as the report has presented, I'd like you to keep that restriction in mind because it is quite critical. That said, I guess we should go around the table and ask people to introduce themselves. I'd invite anybody interested to come up to the table instead of sitting back. It's your choice of course. Then I'll introduce the consultants and we can get going. Patrick, do you want to start?

PATRICK JONES: Patrick Jones, ICANN Staff.

RICK KELLER: Rick Keller, CIRA. Member of the DSSA Working Group.

JIM GALVIN: Jim Galvin, Vice-Chair of SSAC.

JULIE HAMMER: Julie Hammer, SSAC and Member of the DSSA Working Group.

SUZANNE WOOLF: Suzanne Woolf, SSAC and ICANN Board.

RAM MOHAN: Ram Mohan, SSAC and ICANN Board. I'm also a Member of this Working Group.

BILL GRAHAM: [? Suzanne? 00:05:42]. Bill Graham, Chair of the Working Group and ICANN Board.

RICHARD WESTLAKE: I'm Richard Westlake from Westlake Governance.

COLIN JACKSON: Colin Jackson, Westlake Governance.

MAYA REYNOLDS: Maya Reynolds from ICANN. I'm taking care of remote participation.

DON BLUMENTHAL: Don Blumenthal, Public Interest Registry, SSAC and DSSA Working Group.

JACQUES LATOUR: Jacques Latour, CIRA. DSSA.

CHAIR: Okay. Thank you. I guess then we can turn this over to Richard and co. to present their work as it is now. Thanks.

RICHARD WESTLAKE: Thank you Mr. Chairman. Ladies and gentlemen, welcome. Many of you will have been in Beijing when we first tabled the framework as we had developed it. Today's purpose is to seek your feedback and briefly run you through the draft final report that I hope you've had a chance to take a look at. If I could just introduce ourselves first for those who weren't in Beijing.

My colleague, Colin Jackson, and I, and another colleague back in New Zealand have been working on this now for about one year. Colin and my colleague Vaughn went to Toronto, spoke to a large number of stakeholders, involved members, to understand the issues, to understand the scope and to really start to pull the issues together; what it is that people were looking for and what ICANN was expecting.

We have subsequently developed a risk management framework, which we spoke about in Beijing and now we have – as Bill says – produced our draft final report. If I could I would like to take us through where we've got to and just give you an outline, rather than running through the report. I'll take you through how we put it together, how we built it and what the basic outline of it is, and then seek your further questions and discussions.

We've had some feedback so far, some written feedback, and we'd welcome any further before we finalize the report. Just to refresh, what we have developed is the risk management framework for the DNS, and this is not an assessment of the risks or the threats. We do not hold ourselves out to be the technical experts; that is part of the people in this room's job. But what we have developed is the framework to put the assessment into to help ICANN and the community to manage risks and prioritize in order to mitigate or treat them.

Again, just a quick refresher of where we've gone to. Toronto, through Beijing and now here in Durban. And I'll ask Colin now to take over and discuss a little bit more in detail how the report has come together.

COLIN JACKSON: Thank you Richard. Thank you Working Group Members. Before I start showing what we have here, what I'm of necessity going to show you are some high-level slides. There is also a 60/70-odd page report as well. You'll be delighted to hear that I don't intend to work through that word-for-word because we'd be here all morning. It definitely won't fit on the slide.

So this, if you like, is an apology for having elided a great deal of detail. All I can do here is show you the highlights. This diagram is indicating that you have multiple levels of influence and control. At the core, ICANN controls what ICANN controls, which is a relatively small slice of the domain name system as a whole. There is a DNS community, many of whom frequent these meetings. Most people here today might be regarded part of it. And then of course there's the wider Internet.

And ICANN has different levels of influence at these different levels of remoteness from its core. Within itself, ICANN can make direct decisions about things that are totally within its control – like, say, L-root or something. Within the community ICANN tends to seek consensus. These meetings are part of that. Within the wider Internet there is not much. You certainly cannot direct. The best you can do is communicate it in some fashion, if that's what's needed.

There was another dimension that we felt that the particular risks to the DNS should be analyzed under, and this is due to Professor Kaplan and another, I think, writing in the Harvard Business Review a few years ago. They took a view that classic risk management really just looks at things that you can control the probability of. So we can control the probability of, say, a server falling over, by duplicating it, by protecting it, by putting in a maintenance contract – giving you an example.

There are many things we can't control the probability of such as natural disasters, or such as people on the Internet coming up with DDoS attacks – it's pretty hard to do anything about the probability of that. And those things Kaplan regards as external events. The crucial thing about those

is you have no influence over the probability of them, all you can do is mitigate their impact.

And the third category of risks that Kaplan parsed are what he calls strategic risks. They're what I might call risks of doing business. A strategic risk is something that you incur because you're making a change; you are doing an initiative. There are obvious examples in the DNS space. As soon as you start changing things you have to consider what risks will be involved in that change. What are the risks inherent in making some change to the way the DNS operates? And those require a different approach to manage.

Moving on from that, we were invited to build a framework and this framework is from ISO 31000, which is the international standard for risk management. Again, this is one of the inputs that we've put into the overall framework. And this is a very classic risk management cycle. As you can see, you have a contact step, which effectively establishes what you're trying to protect and what the constraints are on you to do so.

It has a step of identifying risks. There are various ways you can do that. It has analysis and evaluation steps and of course a treatment step. And then it cycles back through monitor and review to see whether further work is required. And I expect most people in this room have seen a diagram like this many times. But again, it is an input into what we've built. So, the three of these different analyses have informed what we've put together for the DNS Risk Management Framework.

Before I go through that, there is one point I'd like to make, which is that ICANN and the community talk a lot about SSR – and that's entirely

appropriate. Security, stability and resiliency are all greatly desired – , however, I'm just going to assert that those things are inputs. The output that we really want is a DNS that does what we expect it to do at all times.

So we expect a DNS to be available, we expect it to be consistent within certain parameters – you get the same answers whenever and wherever you ask, within certain parameters –, and that the integrity is maintained so that those who enter records into the DNS, the DNS presents those in the appropriate fashion so that the desired effect is produced when look-ups are done.

From an external perspective of the DNS, if you ask the man on the Clapham omnibus, as they used to say in London, what the DNS should do, that person might say: "These are the things I expect from it." To make that happen of course, ICANN and the community focus on security, stability and resiliency. The reason I've flipped it around into that form was to say that we're actually trying to protect these things as an asset. And that's risk management jargon – we're trying to protect the availability, consistency and integrity.

And our report goes into this at some detail. What follows now is a section of three flowcharts. This is the first one. This is going back to the parsing of the risk into three different categories. We have set out these boxes. Now, this is one area in which I have summarized fairly ruthlessly to get it into a slide, and it's still a very busy slide. There is much more information available.

The format of each of these three things is to show you a classic risk management flowchart under the broad headings of assess, treat and monitor, which again are from the ISO framework. And the table in the bottom section of this diagram is who does what. Now, some of these I'm afraid have slightly fallen off the edge of the screen. I don't know whether it's possible to remove the curtain in the corner there, which seems to be hiding part of it? Apologies, I was really trying to squeeze something onto a small space here.

Thank you Patrick. So, those headings read "ICANN Board", "ICANN Staff", "Experts Panel" – and I'll talk more about that in a moment –, "SSAC and RSAC", "DNS Community", and "The Wider Internet". Now, each of these bodies has different levels of involvement. And again, because I'm ruthlessly simplifying to get it into a single diagram, to some extent who does what varies on how far the management risk is from the core of ICANN's control; back to my concentric circles diagram earlier.

To look at this one – I'll march through this one in a bit of detail – this is the controllable risks flowchart. Now, controllable risks, as you recall, are things that we can minimize the probability of as well as mitigating the impact of, if we so choose. And so we would see this as being done by the… The ICANN Board has an oversight role and probably the Board Risk Committee would be the one most involved in that. ICANN Staff would lead the approach of dealing with the risk but the Experts' Panel would very much participate in that.

The other bodies would be consulted. The extent to which they'd be consulted depends obviously on the specific character of the risk we're

dealing with and the ramifications, and the extent that one has to go to to treat that risk, whether the treatment is something that ICANN can undertake on its own or whether it's something to be undertaken within the DNS community or whether it would require a full-blown communications campaign to get everybody to change something.

Now, the next step in here is a decision point to say, is this in fact a controllable risk once it's been identified? And that's a jumping off point that goes to the external events if it's determined that the risk is in fact something that you can't manage the probability of. The third box along is "Analyze" and then "Evaluate". And again, we see the Experts' Panel playing a considerable role here.

Then the "Treatment" involves setting up options. And this is nothing unusual, I might say. And then "Implementation"… You can't really say who is required in implementation without understanding the specific risk involved. Then there is a Staff function, primarily, to monitor the resolution of that risk and whether there is a residual risk remaining, whether the treatment is working.

As a general observation I'm going to say here that operating this framework does involve a reasonable amount of Staff input. That's something we've discussed with ICANN already. The external events slide looks quite similar, although some of the people who do what changes and some of the detail that I've had to chop out of some of those boxes changes. So I'd refer you to the actual report for more information about the differences between these two approaches.

Again, you get the classic risk management cycle with people, primarily the Experts' Panel, led by the Staff, doing the identification, assessment, etc. The strategic risks one is a bit different. Recalling that the strategic risk is something that you knowingly undertake as a result of an activity where you want to achieve some other outcome. So we're recommending that all Board papers or all initiatives that ICANN might take that could conceivably have a DNS impact, or DNS operational impact, must be analyzed as such before the decision is made.

In other words, some form of risk analysis around the impact on the DNS must be formally undertaken and should be presented to the Board as part of its decision-making process to go ahead on something that potentially has an impact. So this could almost be a standard heading in a Board paper. The experts panel are heavily involved in this.

Another major difference between this and the previous two flowcharts is that there's no loop back on this because once you've decided to undertake a strategic risk it then becomes one of the other kind, because it's no longer a risk of doing business, it's already happened and you then have to manage it going forward. I'll pass over to Richard now.

RICHARD WESTLAKE: This is really trying to address the division of roles and responsibilities and explain where we've come to in our report on recommending the establishment of what in the report we've referred to as "Risk advisory group", what I think subsequent further discussion we have rechristened as a DNS Risk Experts' Panel, to try and be much more focused about

what it is it's actually trying to do and who is likely to be Members of that panel.

The Board's Risk Committee, a typical standard process will oversee the risk management process and make recommendations to the Board for decisions. ICANN Staff have the execution and management functions; administering, and reporting and as Colin pointed out, monitoring and reviewing the residual risks after they have been treated.

And then we have recommended, in order to avoid some of the internal perils of standard risk management processes, the inability to raise a risk through an organization to the highest levels or to see ourselves as we are seen or to address sometimes cultural taboos, an Experts' Panel consisting of outsiders who would be there, able to advise without fear or favor, will be consulted through these processes and will also act in identifying and analyzing risk.

And in the most extreme cases we believe that their terms of reference should allow them to approach the Board Risk Committee direct. When you look at a lot of organizational [inaudible 00:24:05] through [faders? 00:24:06] of their risk management processes, a lot of these are nothing to do with identifying risk but the internal processes for escalation, for willingness to deal with it, for addressing cultural issues or management issues within an organization.

And that is where so many of them fall down, despite having the best risk registers and the best risk processes and procedures, which is why we have suggested this as an extra link in the chain.

COLIN JACKSON: Can I just comment as well? I'd just like to note that we would see the Experts' Panel as being persons who are invited to cover specific areas of expertise. As we all know, it's a highly technical area. We're hardly the smartest guys in the room as regards to DNS technology but the smartest people in it probably are involved in the ICANN community at one level or another.

So we would see the Experts' Panel being chosen to ensure that you have somebody who understood, say, the name server software down to its very last nuts and bolts, somebody who understood all the different areas.

PATRICK JONES: I just wanted to note a time check that we have 30 minutes left in the session and you may want to allow for discussion of the Working Group.

RICHARD WESTLAKE: Patrick, thank you for that. Essentially what that does is bring us to our concluding point, which is to say that having presented this, the aim now following this workshop is to finalized and then the organization will move into the process of implementing, executing and putting in place all the processes.

CHAIR: Thank you very much for that. That's good; we've got a reasonable amount of time for comments. I'd just say that there are a couple of other internal steps that will be going on as well as those listed there. Because this is a fairly substandard and important report, obviously we'll

want to post it for an ICANN comments period. We're planning to do that because there are some significant recommendations here that we'd like to hear from the community about…

There are some other things that are fairly standard risk management work and we believe those can believe to ramp up at the Staff level while the comments period is running. Once we have the comments in and analyzed, this Working Group will prepare a report for the Board, making whatever recommendations are required – for example the formation of the Experts' Group, if that does go ahead.

The report will go to the Board as soon as we can make that happen. I do expect we'll recommend the ongoing oversight will go to the Board Risk Committee. So those are the internal steps internal to the Board process and the ICANN process that you should be aware of. And with that I open the floor for comments. Danny?

DANNY MCPHERSON: I did read this. I read it a couple of years ago and I think it's important work. On page 13 in the version I read it talks about how an advisory group or an advisory committee is most effective; you need some autonomy. Then you also tie that back to the closed loop system. I think that's a gap that currently exists. It's actually something… I saw you guys in the other room earlier.

`I think it's actually something Patrick was touching on during the SSAC discussion, where recommendations are made and it's not clear today what actions were taken as a result of those or if any action… Where someone may say: "We've given due consideration to this and we don't

think those are important issues," or, "We haven't addressed it," or, "We've mitigated those risks." Because there are a lot of things where risks have been mitigated but it hasn't been effectively communicated to the community.

And an example… Well, one of the things I know is… In my day job as a CSO for a public company is that the absolute worst place to be is with recommendations or policies that haven't been effectuated or put into place when a problem occurs. In other words, you put a policy in place and then some incident occurs and you weren't enforcing your policy and the controls that would have helped bring your residual risk to an acceptable level aren't mitigated and that was exploited.

And now you're much more responsible than if you didn't know about those things in the first place. That's the one thing that our lawyers absolutely harp on about. And I think that we certainly have some examples of this expressly in ICANN where, for example, SSAC 59 talks about inadequately addressed and lingering issues and recommendations being made related to security and stability issues in the New gTLD Program.

And I'm just wondering what drove that paragraph into the report and then two, how would you envision closing that loop to make sure…? I mean, certainly, things like gap analysis from ICANN Staff about recommendations and that kind of thing need to be put in place.

But I think that there are a lot of outstanding recommendations and I think some folks that are aware of VeriSign's role in a root zone publication provision process can appreciate this – we're talking about

New gTLDs and you see a lot of outstanding issues and recommendations that have not been effectuated or put into place and that makes us really nervous from a liability perspective and so forth.

So I was just wondering from your perspective, in compiling this and in the work you've been doing for a couple of years now, how you think we can best deal with those sorts of issues.

COLIN JACKSON: Thank you Danny. The Experts' Panel operates in our model here with Staff leadership and administration support, but the Experts' Panel is a Panel and will be regularly reviewing the register of risks. It will be in a position to keep highlighting things that are not being done and as Richard said, it can go directly to the Board Risk Committee if it feels that it is not succeeding in getting the action that it believes is appropriate, performed.

I hear what you're saying about identifying risks and then those messages getting lost in the chain. Whist I've no evidence that this happens here I've certainly seen it happen in corporations, in government bodies in other countries and yes, whilst I hear what you're saying about liability as well… Liability is a proxy for doing the right thing and that's what we need to do here – do the right thing, and that's keep the DNS running.

So from my perspective we do need to ensure that the feedback mechanisms are there so that the people with the greatest extent of authority are motivated to do what they can to keep the DNS running.

MIKEY O'CONNOR: My name's Mikey O'Connor, I'm in the ISP Constituency and a Member of the DSSA Working Group. Could you flip the slides all the way to the very first slide, that title slide, please? I want to point out a change in scope on this slide. Scope of the DNS Board Management Risk Framework Committee, as Bill mentioned at the beginning of this talk, was a Risk Management Framework for ICANN. This says, "A Risk Management Framework for the DNS." My question is, which is it?

RICHARD WESTLAKE: It's for ICANN. The title is incorrect.

MIKEY O'CONNOR: I think I'm going to hold the rest of the DSSA comments for our meeting, which is coming up in a bit. I would really like to hear from the Board Risk Management Framework Committee their reactions to this so far, because what we're trying to do in the DSSA is figure out whether we just stop.

CHAIR: I'll lead off on this and then I'll turn to other Members of the Working Group. I've read the report through a couple of times. My reaction is that this is a workable approach that they're recommending. I think it's a good start; Staff will be able to take this and move forward. There are some questions that I hope we'll see addressed in the public comment period, such as comments on the Experts' Panel or Advisory Group – I do prefer the phrase "Experts' Panel" –; comments on other aspects of the methodology.

But I think in general – and no disrespect intended here – it's a fairly standard approach that I think Staff should be able to work with this and start making some progress fairly quickly. And I'll leave it there. Ram or Suzanne, do you want to speak?

RAM MOHAN: Thank you Bill. [inaudible 00:35:00] question. I echo Bill's comments. I think this is a good start and it provides the basis for a roadmap for what Staff can do. We, inside of the Working Group and certain from a Board perspective, have tried to be clear that the focus is on what ICANN can do; what's within its remit, what's within its scope, and not try to boil the ocean here. That's really not the intent. And we've been trying pretty hard to keep that in that way.

And if you take that as the framing context then the ideas presented here and the direction being suggested, I think are very implementable. They start with small steps and they ought to lead up in the next few years to something that is… To accumulate a body of work and to accumulate a set of practices that become standard for the organization when it comes to risk management framework. Once you get there then I think there's an opportunity to engage again and to say, is this too much? Is this just right? Or, is this too little? And then to go further.

But from a Board perspective, my own exaltation to both Staff as well as to the consultants has been to keep the scope within the realm of feasibility and within the realm of something that can actually be acted upon with concrete, small steps, rather than trying to take such a broad

vision at the start that by the time you start to move forward your energies are dispersed. Thank you.

CHAIR: Thanks Ram. Suzanne, please?

SUZANNE WOOLF: Sure, thank you. I think this point bears [inaudible 00:37:30] because it's actually something very tricky that we work very hard to capture in the Terms of Reference for this, that the outcome of this activity has to be, as Ram says, implementable. It has to reflect the fact that action will be taken by ICANN Staff with respect to a certain, fairly specific set of things.

But also we needed this work to capture the context that, for example, ICANN is not – with respect to the DNS – simply an enterprise, where there's a relatively clear line and a relatively small zone between that which you control and that which you don't. The interactions that ICANN has to be able to take into account are actually rather more complex than that.

The scope of ICANN's ability to implement specific recommendations as actions for ICANN Staff to take is in fact relatively narrow and constrained. That's actually a tricky situation to work with and for the Board we were trying to set up a situation where it would be possible to exercise proper oversight that this was being done in the way that's most effective for ICANN and the larger community.

And this is actually a very tricky thing that, as Ram says, will have to be worked out in detail over time. But I do think that this work captures at least some of the dynamic there, which was very, very important to us. Maybe the most important single aspect of it. And I think we've gotten to a good place to start but there will be some refinement required over time.

CHAIR: Thanks Suzanne. The other Member of the Working Group with us here is Patrick Fälstrom. Patrick, do you want to make any comments?

PATRICK FÄLSTROM: I don't think I have much to add, given what the others have stated. I've also gone through the report and I think this can be [inaudible 00:39:22] for future work. My own personal experience from doing similar kinds of mapping out exercises, say that the really interesting part is when you actually take, for example, any kind of framework and you actually [inaudible 00:39:37] the map into whatever kind of processes that you would like to run, control or audit under those processes.

So to some degree I don't think the rubber has hit the road yet. So there are still… There are some mapping exercises here that are not done and that I think need to be done before it's really possible to evaluate how successful this [inaudible 00:40:03] is.

CHAIR: Thank you Patrick. Other comments or questions? Please?

SPEAKER: Could you flip to the slide that is your next steps? Thank you. Picking up on what Patrick was just saying, I'm curious where the work happens to actually dig deeper to develop the methodology deeper with risks, ails, risk assessment definition, that type of stuff. Is there an existing risk management methodology in ICANN that this is going to interact with or utilize, or are you building from the ground up? If so, it's not reflected here and maybe that's not a Westlake activity but I'm just curious.

CHAIR: Can I ask Patrick Jones to respond to that please?

PATRICK JONES: This is Patrick Jones from ICANN's Security Team. There is an existing risk management function that has been working through the Board Risk Committee. We are in the process of… We recently hired an Enterprise Risk Management Director, who will be taking a look at the work that Westlake has produced, as well as looking at other well-known international standards and seeing if it's time to augment or update the processes that we've been using.

SPEAKER: The thing I would add to that of course is the work of the DSSA, which has looked at this problem but in a broader context. So on that we really need to do some more work; in the next phase analyzing both the Westlake work and what's come out of the DSSA to make sure that we've got all the bases covered within the ICANN context.

DON BLUMENTHAL: Hi, it's Don Blumenthal. I was going to back off saying anything because you may have just covered the issue. I think this report is very good for putting together a framework for ICANN looking at risk issues within its purview and direct control, given some of the issues flying now with respect to New gTLDs, it would have been great if some of this stuff had been in place a couple of years ago.

I guess my concern is, does [inaudible 00:43:06] DSSA is that maybe this is my misunderstanding but there seems to be a disconnect in what I had thought was going to be addressed, because it is so much narrower than what we were looking at in DSSA. But it sounds like that's already being looked at so I'll leave it at that.

CHAIR: Good, thank you. Yes, please?

JÖRG SCHWEIGER: My name is Jörg Schweiger, I'm the ccNSO Co-Chair for the DSSA. My question would be… I would like to get an impression and a better understanding for what the Board's Group feels it is heading for. What is your vision of where we are heading in implementing this kind of framework? If it were just a framework to deal with security problems that might occur and ICANN's mission to run some of the infrastructure assets like root zone, I can easily understand how the framework could be applied to that part of ICANN's mission.

But I wonder if we do envision that, we once again set out to discuss what I would call an operational arm of ICANN into security and to

dealing with security issues that are not under ICANN's operational arm. And I think it's crucial that we do address any issue that might occur with any DNS operator out there in the wild.

So are these risks tackled by the framework as well? Is the group that is supposed to analyze the threats located somewhere within ICANN? Is it a group that is just put together as needed or is there an organization that needs to be founded and within the permit of ICANN? I just want to get a vision of how you really handle the issues about DNS security that might come up.

CHAIR: Well, I'll take a first shot at that and then again I'll invite the other Members of the Working Group… This Working Group has quite a narrow mandate in that we were charged with getting a framework for managing risk within ICANN to the point where it can be handed off to the Risk Committee for follow-up work. And we're talking not only about security risks but enterprise risks more broadly.

So from the perspective of this Working Group, it is true that we'll be looking pretty closely at the ICANN side and not beyond that. That is not to say that risk management can be accomplished in that way. I think the recommendation to create the Experts' Panel is intended to bring a broader view into the work that the Staff does so that it's not operating entirely in isolation.

And I would assume that as the Board Risk Committee picks this up, it will continue to be in touch with the broader community and get a sense of the appropriateness of its work and reach out where necessary. But

at this point, the findings that led to the creation of this Working Group suggested that we didn't have adequate risk management functions at the Staff level and that's the problem we're setting to address here very specifically. Ram, Suzanne or Patrick?

RAM MOHAN: Thank you Bill. To add to what you're saying, I would not be surprised that in the months and years to come ICANN adds a different Staff function or a separate Staff function that's going to focus on enterprise risk that goes beyond just security. In the past, risk has been considered the equivalent of security or something that has been subsumed inside of the security function.

And we think it's beyond just security. Security is a very important component of managing risk but there are other pieces as well and the desire is for a sustained function within ICANN as an organization to have a consistent look and to create a risk management plan within a framework.

And that's really what we have been chartered to do; to help kick that process off, build a foundation and then hand it off to the Risk Committee for continued oversight, understanding that Staff are going to have to build out this function in a way beyond just the security-oriented, historical method that has been followed so far.

CHAIR: Other comments?

SPEAKER: May I answer that one? Once again, I feel that the question of scope would come up once again. I think that it's clearly within the remit of ICANN to foster security and I always understood that this effort is not only centered on dealing with ICANN security issues but addressing how to foster security within the whole ICANN community. So I just want to try and make clear how this work is addressing fostering security as well. Is it within the scope of your work or is it out of scope?

PATRICK JONES: In the materials that our Team uses to describe the different functions of security in ICANN, organizational risk management is one of the four key areas and we do talk about that in our annual security, stability and resiliency framework.

SPEAKER: Richard, I'd be happy to let you take a run at this. I think if we look at those flowcharts for the three different types of risk you will see that both the DNS community and the wider Internet are identified as being integral here, but because ICANN does not have the leverage to control what they do the interaction is described as being "consulting". In the report it's also "communication".

So that is the kind of fostering of fostering of security in the wider community that I think is envisaged here; through consultation process and communication. Obviously, if a risk is identified that is not exclusive or not even within the ICANN remit at all, that would not be tossed in the garbage – it would be communicated out in an attempt to foster security. Does that help?

RICHARD WESTLAKE: Thank you. Coming back to your question exactly, the question you framed was exactly the way we approached our assignment. There is breadth and depth in what we've tried to do in terms of – with apologies to Mikey for the title – we were asked to develop a DNS Risk Management Framework for ICANN, specifically for what is in ICANN's remit.

But recognizing that what we're putting forward to the Board Risk Committee in the end – what one assumes will go to the Board Risk Committee in the end – their remit is not just the DNS Risk Management Framework. It is risk management for the whole of ICANN. But there is an expression we use which is "if you're going to eat an elephant you do it one bite at a time".

So it starts with the DNS Risk Management Framework. If ICANN can then extrapolate – and part of our thinking about the whole framework we've developed is something that could be developed consistently –; not just related to the DNS, not just specialized but much more organization-wide, then we've tried to do that as well.

CHAIR: Mikey, I see you're approaching the microphone. You may be intending to speak?

MIKEY O'CONNOR: I just want to read from the R of P, because the words you said are different from what's in the R of P. "Develop the ongoing methodological framework that ICANN will use to manage DNS security risk..." "*DNS* security risk." Enterprise security risk? What's all that stuff? "…Within the technical mission specified by its bylaws." This is

like a moving target. I've been sitting here all day trying to nail this jelly to the wall. I can't figure out what on earth you're doing.

RICHARD WESTLAKE: I'm sorry Mikey, no. We have, as I just said, developed a DNS Risk Management Framework. Our background thinking in doing so was to make something that potentially – but not as part of the scope of this assignment – could be extended more broadly.

SPEAKER: I'll just add to that if I may. We've used generic risk management methodologies and we've adapted those to suit the DNS and specifically ICANN's role in it. Now, the generic methodologies come from an enterprise risk background, but that doesn't mean that that's what we've supplied here.

MIKEY O'CONNOR: Sorry. I've told myself all week I wouldn't do this. You didn't use generic methodologies – you used proprietary… You've used ISO 31000, which is Copyright. So it's not something that we can go out into the world with if we want to use it anywhere else. We can't take ISO 31000 in the DSSA context, splash it out on a public email list and start drafting changes to it. They'll come and whack us with a Copyright violation.

CHAIR: Do you want to respond Richard?

RICHARD WESTLAKE: I will, briefly, thank you, because I'm absolutely clear on this one. Having had quite a lot of involvement in the whole area – and I have in fact consulted with people who are directly involved with this. The Copyright protection around ISO relates to photocopying and reproducing of the document "ISO 31000.2009".

The point of an international standard is that it is adopted and distributed widely. So if ICANN puts together a risk management framework based on ISO 31000 it has unlimited ability to disseminate, distribute and implement. The only thing you can't distribute is the document "ISO 31000.2009".

Any risk management framework developed from that, such as the diagrams we've included, is absolutely clear and free for ICANN to use exactly as they wish. There is no proprietary protection on the Risk Management Framework that we've developed.

CHAIR: Thank you. There is time for one last comment of question.

SPEAKER: Bill, can I ask one?

CHAIR: Yeah.

SPEAKER: I heard you say something a few minutes ago. You said that the findings that you identified… What was it? Findings suggest ICANN does not have adequate risk management functions at the Staff level. Can you expand upon that?

RICHARD WESTLAKE: My understanding is that both the Security and Stability Review Team and the ATRT 1 had found that there was a need to improve our risk management functions, which included or would include strengthening of the Staff-level. Yeah. That's about the depth of my understanding of it.

CHAIR: Okay. Thank you very much. This is not the end of your opportunity to comment and provide us advice on this report. As I said, it will be posted for comment and a response period. I would invite and encourage you to make use of that. And with that I thank you for being here today and look forward to hearing from you.

And also thanks to Westlake Governance for their work. And Patrick Jones for shepherding us through.

[END OF AUDIO]