Patrick Jones: Good morning, everyone. Thank you for coming. We're still working to get the slide deck up, but this is our ICANN Security Team briefing. So I'm Patrick Jones with the Security Team. We'll go down the line and introduce ourselves, give you an overview of our main areas of work; also introduce new Chief Security Officer, Jeff Moss and talk about our FY12 Security, Stability and Resiliency framework and comments that were received on that document, as well as our priorities, how we see engaging with the community and hopefully make this more interactive and take some questions. So with that, introduce everybody.

Dave Piscitello: I'm Dave Piscitello, Senior Security Technologist at ICANN.

Jeff Moss: I'm Jeff Moss, the shiny new CSO.

John Crane: I'm John Crane, the not so shiny and old CNA Director of Security, Stability and Resiliency Programs.

Patrick Jones: We're working on getting the slide deck set up, but as we do that, the next section was to introduce you and get a chance for you to talk about background interests and your role with us.

Jeff Moss: Alright, well, good morning, everyone. I'm Jeff Moss and in a previous life I started a business that failed and that forced me to have to get a job which ended up being at Ernst & Young in their Information Security Practice and then from there I went on to a company called – I don't know if you guys remember this – there was a secured computing corporation which was a spin-out of – who is it, Honeywell – it was a spin- off of Honeywell, and then there I built their Professional Services Division and the relevant part of that was that it got me ultimately in charge of the Asian/Pacific region.

So I came to Singapore. I've been coming here since about 1998 and this country is completely different than what it was from '98. It's just evolved so rapidly. But back then they were doing business with us cause it was the only country that decided that they were running IPV6 or going to run IPV6 and they needed a firewall that was certified, and this was in '98.

And then from there I moved on. Most known for a series of information security conferences DEFCON and Black Cat, which is another business I had started that I sold. So now I just remain tentatively connected to Black Cat in the Content Selection side as a contractor, but I don't have any day-to-day operational association really, besides answering phone calls and giving advice.

So when that happened, about that time, Rod started heavily recruiting me to apply for the ICANN position, and I really liked the community because the community in ICANN seems to be similar to the community in the security space where, sort of, the best idea is supposed to win. And it doesn't really matter who you are; it's based on your arguments and the merits of the case and ICANN is neutral or tries to be very neutral; the conferences I started were trying to be very vendor neutral.

So there was this natural affinity between the two – what I have done in the past and what I wanted to do in the future. The other thing about ICANN I found very interesting is there's only one of you. If you talk to your friends, you can say, "Hey, what's it like working at AT&T or T Mobile or Deutsch Telecom or Orange?"

But you can't really ask your friends what's it like working anywhere but ICANN. And it's a unique organization that sometimes gets lost in the mix, I think, in the outside in the wider security world because I feel sometimes it can be a bit insular.

And so I'm hoping to try to bring in a wider audience, a larger attention to the issues. Some of the things I'm worried about – I'll just briefly touch on that since we don't have a presentation up there. I'll just keep talking. Oh you do? So I can stop?

I'm spending more time in Washington, D.C. which is the office I'm working out of. I'm busy trying to buy a place in D.C. right now. And a year and a half ago or two years ago there was no legislation really relating to information security in Washington, D.C. in the United States.

And at the session that just ended, we saw 71 or 73 - depending upon how you count - bills. And to go from zero to 70-something in a year is very frightening because it's not the quantity of legislation; it should be the quality of legislation. So this year I think we already have several Protect IP and some others that are coming along.

And this is very unique in U.S. history. We also had… The United States came out with the National Strategy for Cyberspace, and some other countries are following suit. And so I think in the next couple of years we'll see a lot of countries putting a stake in the ground and saying, "This is what we believe in as a national country."

Well, all this is going to influence our operations and we need to be aware of that. So that's something that's been very interesting to me. I used to always believe that there was a technical solution to a technical problem and the more time I spend in the higher layers, you know, 8 and 9, the more I realize a lot of this stuff is policy-driven and you need to engage at the policy level much more actively.

And that's another growing fascination of mine and has been consuming the last several years of my life, so I'm perfectly happy. My strategy on the Security Team is I want Security to be seen as an enabler of business, an enabler of the community. I don't want

Security to really become a roadblock to anything. And if it does, we need to figure out why and how we can get around it because, while Security presents a unique set of challenges, I don't think any of them are impossible.

There are solutions to these problems. It's just is there enough political will to institute them. And so part of what I'll be trying to do is figure out is there enough will to pursue these or is it a waste of time and we're going to end up burning up good will that we should be better using elsewhere.

So as part of that strategy, I have an open door policy where I'll talk to anybody about anything. My team is available to answer questions or point you in the right resources, in the right directions and really, I think, a lot of this is about information exchange and no one person has the perfect optimal answer. And so I always remind myself of that – there's no perfect solution.

I had a law professor once who – he was a constitutional law professor – but he said, "Politics is the art of what's possible, not what's perfect," and I can't forget that. For some reason I've carried it around for all these years because it's really… I find it really true. And so I want to try to help do what's possible and push those limits and constantly expand what's possible so we can get as close to perfect as reasonable. So that's my little rant and I'll pass it back to Patrick. And we'll be available for questions at the end, so…

Patrick Jones: Thanks, Jeff. We have a slide deck, but if you're in Adobe Connect you'll be able to see it as well as for remote participants. The slide that we have up right now is a description of the ecosystem in ICANN's role and if it's not on the main… Is it not showing up in Adobe?

Male: Everybody has a laptop, just get over it.

Patrick Jones: Don't we have tech support? Alright, well, we'll work through the logistics, but… So one of the things that we tried to do for our FY12 Security framework was to take a step back and make a clear distinction between those areas that are ICANN operational such as LRoot, IT and the DNS Operations, internal ICANN compliance, the string evaluation function for the IDN Fast Track, meeting logistics, administration, finance, that sort of thing.

And separate that or make a distinction between those areas where ICANN acts as a coordinator, collaborator and facilitator with the community and also those areas where ICANN's an observer on the activities of others in the global internet ecosystem.

So that's sort of a, as a baseline, try to make it very clear for the community what things that are internal, collaborative versus observing. And for the Security Team, we had set up before Jeff came on board our team areas into Global Security Outreach, Engagement and Awareness With the Greater Community, our

Security collaborative efforts, such as with the Conficker Working Group, and also the DNS Capability Training Program with partners such as ISOC and the regional Top Level Domain Organizations.

And then our corporate security programs, that include everything from internal IT, meetings-physical, personnel security, as well as business continuity and planning and risk management – those areas across the organization where Security Team supports efforts such as the new gTLD Program, the IDN Variant Work and the Fast Track DNSSEC Implementation, overall policy development, the Compliance activities and work with global partnerships and the Government Affairs Team.

So for last year, the major activities where Security was a contributor included the DNSSEC Implementation in the Root. Several of us were part of the key-signing ceremonies. I think we've now done six key ceremonies. Correct me if I'm wrong on that. But we just did one in Culpepper, Virginia about a month ago and they rotate between Culpepper and the key-signing facility in Los Angeles.

And in addition to that, we conducted an LRoot Continuity exercise and participated with… So, supporting International Cyber Exercises in ISSA, ICANN was also involved in a larger international cyber exercise with some ccTLDs. And then supporting community efforts to look at threats and risks to the DNS such as the DNS Security, Stability Analysis Working Group that's meeting for the first time face-to-face here in Singapore.

And then also building on efforts from the San Francisco meeting, we have greater engagement with law enforcement and the security operations community. We did our first Chief Information Security Officer's round table in San Francisco, so we're working to build on that. And then also supported the DNS OARK to meet at San Francisco and do their joint session with the ccNSO Tech Day.

And then John can also talk about work around DNS measurement and metrics tools like supporting actions like the right RIPE Labs Atlas Program. And then lastly, sort of a brief overview of our FY12 Security, Stability, Resiliency framework.

So this was the document that we published May 2 of this year and we had public comment from May 2 to June 2. I'm really pleased with this document because it was one where as a team we reached out to SSAC At Large and some others pre-publication to conduct some targeted discussions and that really helped shape the revisions that went into publishing it.

I thought this was really useful because this helped make a distinction between ICANN's role in security, the greater ecosystem and try to put some distinction between those areas that are internal ops, collaboration and observation with the community.

So this is the document that is for Board acknowledgement on Friday, and we received quite a bit of positive feedback from the community. There was general support for this new format as well as appreciation for posting it with translations in five U.N. languages. At the same time, the ccNSO and the Registry Stakeholder Group requested some improvement on definitions in the document and precision on describing ICANN's remit.

But there was general support for an environmental scan to assess the current internet security ecosystem and work to involve the broader internet community, including Enterprise users, internet infrastructure entities, government entities in that work as we move forward.

So at this point we'll turn it over… I want to go down the line and have an introduction of what some of your activities are going to be for this next fiscal year and then also open it up for questions too cause we're at a point where before I give an introduction to what some community engagement in security includes the DSSA Working Group. This is a cross-community working group that was endorsed in Cartegena by the ccNSO, the gNSO, At Large, the NRO and also has liaison support from SSAC.

So this is a working group that's going to examine the actual level frequency and severity of threats to the DNS – look at current efforts and activities to mitigate those threats and the gaps, if any, and then hopefully come up with some recommendations.

This group is interesting because it's huge; it's made up of a lot of people in the space and touches on the different actors in the ecosystem and it's working somewhat on a parallel track with the Affirmation Review Team on SSR and that group is going around and meeting with various stakeholders and advisory committees this week here in Singapore.

And I know there's some in this room that participate in the DSSA as well as on the Affirmation Review Team, so I'm hoping that they will get a chance to talk to each other this week and further the greater community discussion around SSR. So with that, I'm going to turn it back down the line to talk about what some of our priorities going forward, you know, training, interest from law enforcement, as well as our role in supporting community initiatives and being open and then take some questions. I'm going down the line, so Policy Development?

Dave Piscitello: I may be talking about activities that we haven't even funded yet. I'm sort of a – if you are familiar with American football – I'm sort of a free-roaming linebacker. I work with the Policy Team, I support SSAC, I work with Compliance and I work with the Security Team.

Part of playing that role is trying to make certain that all the players in ICANN are on the same page with respect to security and respect to the current threat landscape we're paying attention to and accessing risk and trying to understand where best to put our resources.

So some of what I do, and much of what I'll do for the remainder of this year, is work with external security communities like the APWG, the Anti-Phishing Working Group, the Message Anti-

Abuse Working Group and other law enforcement and security OP SEC venues to discuss what are the most pressing problems that law enforcement and the security community face when they're dealing with crimes that either involve or exploit the DNS and registration systems.

So I'll be doing some presentations of some of the work that SSAC has produced over the past six months @nes.net; internet 2; Joint Text Conference. Next month I'll be participating in a [Team Kimri] Underground Information Exchange Meeting. Sometime later in the year I'll be working with some of the people on the panel here on a DNS conference called DNS Easy where I'll be talking quite a bit about DNSSEC and other threats to the DNS later in the year.

As an example, some of the outreach. I'm a member of the APWG Internet Policy Committee. I spend a fair amount of time working with them and we actually do things that are not necessarily directly related to the DNS, but help ICANN contribute with some of its expertise in things like assessing web vulnerabilities, how it would recover from attacks against a website and some other broader security matters.

So with the Security Team, one of the things I hope to be able to do considerably more over the next year is work more in cooperation with and try to assist law enforcement and the security community in having an appropriate voice that ICANN… and also in understanding how ICANN the corporate entity can work more closely with law enforcement on issues that require the kind of urgent attention that we saw was so important in combating the Conficker worm several years ago.

As many of you know, there have been a number of similar sizeable take-downs of botnets, [Rus Dock, Coreflood] and others, and while ICANN hasn't played a direct role in those, it's inevitable that at some point in time, because domain names are involved and because there are going to be contractual issues, or there are going to be other issues in terms of connecting the dots, putting people in touch with the right TLD operators and trying to understand the right way to do a suspension – whether a suspension is appropriate or whether a sink-holing is appropriate – it's a good thing that we have more security expertise and that Jeff is bringing them together to be able to pay attention to these and provide redress and remedy in as many different manners as is necessary to combat crime.

So that's a long-winded way of saying I try to do what is necessary to essentially keep the DNS clean.

Jeff Moss: Since my tenure at ICANN is much shorter, my answer will be much shorter. But on the ICANN the company side, the internal side, I sort of think of it, which I believe will be consuming probably 30% of my time, is sort of an inward-facing role and the rest of my time, I believe, will become an outside or externally facing role.

I want to be spending the immediate future trying to get a better understanding of our risk analysis for our company. You know, what risks we face – update that; better understand what the new gTLD program means to our risk profile changing; DNSSEC adoption as it accelerates and more and more people start putting interesting things inside of DNSSEC responses.

I'm curious what happens to our risk profile there as well. Instead of getting a number back when you ask a query, what if you get a recipe or a picture of a cat? There's all kinds of stuff people are going to be stuffing into DNSSEC that was not envisioned and I'm curious on what that means.

I also in the very near term will be with the Security Team we'll be consolidating some of the Security Team functions. We'll be preparing for additional activities surrounding the gTLD program and so once we have all of our people in place, that will allow us to be very clear moving forward.

And then on the outside-facing a lot of stuff is going on. There's the SSAC that we're trying to support, and SSRT initiatives and the DSSA so I'll be spending my time better understanding those groups and how we can answer any of their questions or support them in their endeavors when they come to us for support.

And as Patrick talked about, I'm too trying to figure out exactly how law enforcement fits in, what our role is because I believe it's important to have their cooperation and involvement in securing security and stability. We need their support to go back to their national governments and say that ICANN actually pays attention to these things and cares about online crime and shares some of our concerns.

I'm just not sure exactly what kind of a role they will play. And so I know there was a meeting, the San Francisco ICANN, where they had one of their first meetings where they all got together and talked about their concerns and I believe they did that again at this meeting. So maybe just having the avenue for them being able to talk to one another is sort of a first for them and that will help inform their own decisions about what it is they're looking for from ICANN. If they can communicate those clearly, it'll be good for all of us.

So I have so much on my plate that I can't see a whole year in my future. I'm lucky if I can see three or four months right now. Thank you.

John Crane: Okay, so I just got off an airplane so excuse me if I'm a little jet-lagged here. One of the main areas that we've been focusing on over the last couple of years is working with ccTLD organizations to help them build their capabilities around operations and security of those operations. We expect to continue working with the Regional ccTLD groups over the next year and continue with those trainings.

There is a question as to whether or not there are other areas where we need to be giving training, not only to the ccTLDs but maybe over parts of the community. These training programs are very much community-driven, so if there are things that need to be done, then we need to hear from the community. What we don't want is ourselves going forward on that.

So we have our discussion about whether or not there needs to be training on IPV6, on DNSSEC, on whether or not law enforcement would be interested in some training and other things in this area. All of this is a little up in the air because we need to get requests from these people who are more forward to us.

The other area that we're working on a lot this year is the definition and measurement of some of the things that we talk about in my title like, what is resiliency, what is stability, what is security when it pertains to the identifier systems. There are lots of different organizations out there in the world now and groups that are looking at such classifications and definitions and how they should be measured.

A lot of this is in relation to what they call CIIP, Critical Information programs, Critical Information and Prescription Protection. So we're seeing a lot of requests for input on those so I suspect that will continue throughout the year and it seems to be building to a crescendo. There's a lot of different groups working on that work. A lot we've heard Dave Piscitello on interacting with some of these groups and probably with Jeff over the next year as he's agreed to join us in doing some of the outreach. And those are some of the main things and I suspect Patrick will want to talk to some of our internal stuff.

Patrick Jones: So we do have some other members of the team who aren't here who cover our internal security meetings, security and will be working quite a bit on continuity and contingency exercises and also testing of systems before any of the launch for new TLDs making sure that its auditing and vulnerability testing and making sure that this won't be loss of confidential data prior to announcement of any strings.

So there's still quite a bit of work to be done there and we look forward to being involved and supporting new gTLD teams in that area and also other continuity and contingency exercises that happen.

I mentioned we did an LRoot exercise. That was, I believe it's the fourth of our annual continuity exercises that we've done as part of the program. So the first was a registry fail over exercise that was internal for ICANN from a few years ago. And then we did an exercise that was with VeriSign and Afilias. And the previous year we did an IANA continuity exercise that was a live rollover of systems from the West Coast to the East Coast of the U.S.

So I would envision that there will be further exercises including work with NTIA and VeriSign in a root zone management system contingency and other things like that.

So at this point we have time for questions if there's any one of you that wants to raise anything or ask something more of Jeff or John or Dave of myself. And I see a question in the audience.

Marilyn Cade: Thanks. And I want to compliment you, Patrick and the rest of the team on the format and content of the materials that you provided. My name is Marilyn Cade. I'm the Chair of the Business Constituency. I think there's some other folks from the Business Constituency here.

Let me also though, ask a question about – you don't need to look at page 20. I'm going to tell you what my question is. We have four strategic objectives that are identified, but in the body of the work product, there are several references to enhancing awareness, building what I would consider more informed user base, including businesses as we all know a vast part of the internet is operated by the ISPs, the web hosting companies, those of us who build and run the internet, not just the DNS providers.

And I'm pleased to see the beginning of the recognition of the implications of the export in/export out nature of the activities that we do here at ICANN.

I would like to propose that we think about a fifth strategic objective and how that would be couched in enhancing the awareness of users. It's sort of embedded in the work product but it's not identified as a strategic objective. I think we need to think about, if we're talking about collaborative activities and outreach, that enhancing awareness is clearly one of our goals. So that's one question.

And then the other point I think I would make is, while we've improved somewhat in the level of detail and the explanation at an extremely high level is clearer, you will continue to hear from the Business Constituency that we feel overall, including in this plan, that ICANN needs to provide deeper levels of detail that can be interactively discussed.

Jeff Moss: What's an example of a more interactive detail?

Marilyn Cade: Jeff, are we gonna spend a lot of money on a DNS form – I can't remember the exact name of it – and whatever the plans are. And they may be perfectly great plans if they are targeted at a particular set of players your plans may be very, very suitable for those. If they are going to be inclusive of the broader business community and the ISP community, then we may have something to offer as the Business Constituency or even other stakeholders from ICANN on how to insure the broadest and most effective participation. And since I don't have any detail, I can't give you any comments. Is that a good…?

Jeff Moss: Yeah, I think Patrick's gonna take this question cause he's got about, what, eight, nine more years of history.

Patrick Jones: So, Marilyn, I think you're referring to a potential and proposed third DNS/SSR symposium? In 2009 we did the first one at Georgia Tech University and then in 2010 there was a follow on symposium at Kyoto University in Japan.

So what you're suggesting and what we actually own the community if there's going to be a third one is to publish a date and information about it and an agenda and note if it's going to be open or closed or targeted to a particular group and provide that level and also when on the calendar so that if people are going to attend…

Marilyn Cade: Thank you for that. But you see, this would be… You're making a point that I should have made more clearly. Actually that isn't what you should do. You should have a draft that you seek input from enough of the community that's relevant to make sure that you end up with support for that and I think that probably is in your plan.

But I'm just suggesting when you come out for consultation, it's extremely difficult and if you feel that you can't take consultation with everyone and that you really want to have targeted consultation, then you do have a community of leaders across the constituencies and in the SOs and ACs to do kind of a "can we test a straw proposal with you."

Dave Piscitello: So, Marilyn, I'm actually on the Steering Committee of this DNS Easy Conference, which I mentioned earlier. One of the hard parts about doing a conference where what you want to try to do is pull the people with the greatest technical expertise to tackle a global technical problem is how do you actually figure out who to invite? And it's like any other academic-driven kind of conference.

We've essentially asked somebody to take over the chairmanship and they ask the community who is the right set of individuals. And so, yeah, there's a certain amount of subjectivity in who gets invited and what gets covered.

And there is a Steering Group of I guess between 12 and 18 people that have been put together in the last six to eight weeks. And we are currently working on the program agenda, the call for papers. And this is the kind of conference similar to something that you might see at Usenix or any other academic conference where people are publishing articles that are literally referee journal quality.

I'm open and certainly willing to carry anything that you might suggest into the Steering Committee and if you want to send some ideas to me, that's a great idea.

Marilyn Cade: I'm not sure that you're hearing me because your answers are not responsive to my question. I like your answers and I might act on them. But I'm saying to you is in material like this, when you're taking comments, you need to get… Dave, you already told me more than anyone in the community probably knows about the organization. That's great and so for anyone who's here, they're reading the transcript, they got it.

But just the level of detail that we'll say the options we're considering are highly refereed conference; we are going to use a steering group; our focus is going to be on option, you know, these three areas. It's not going to be at a level that is suitable for the lay person. Just enough that people can say, "Oh, wow, what a great idea and this is how it fits in."

Or they can say, "Well, in addition to that, you need to add a day for decoding this for governments and lay people." You're shortchanging our ability to support you without a little more detail.

Dave Piscitello: Certainly not by intent. And I take what you say to heart and I think it's a very good idea that we're able to talk more about that.

Patrick Jones: Anyone else in the audience have questions or something that they want to raise with the team? Anyone on the Affirmation Review Team want to raise a question or something or from the DSSA Group? I'm looking at someone in the front row or from Mikey on the other side. This is your opportunity to raise a question. Feel free.

Bill Manning: This is Bill Manning. As a member of the Review Team, last Thursday after a long gestation period, the U.S. Department of Homeland Security released a risk profiling for the Domain Name System. Not sure if you guys have taken a look at that or if you've seen it, but that's something that I suspect we're going to see similar types of things emerge from other sovereign entities about their views about the risks of the Domain Name System.

How are you guys going to accommodate sovereign entities who come up with their own set of risk frameworks for the DNS? Have you thought about that?

Patrick Jones: Well, first off, you acknowledge them, "Thank you for your contribution," and compare them to your own analysis in case they come up with some new novel angle that you haven't considered. The DHS one was interesting at least to me because it gave a very low probability to denial of service attacks against the root operators, the root servers.

I don't know if I would have assigned it that low of a probability. So they might identify risk and we might disagree over the risk probability that might inform later decisions that we make. But I think the more governments consider the risks to the global DNS and unique identifying system, I think the more they'll understand and be socialized to the problems that we face.

I don't see it really as being the negative; I see it as being a positive that these countries are now understanding the value of these systems and therefore they should understand the value of what we've been doing all these years. So I'm not worried about it, I'm just hoping that they don't run off and start legislating.

Bill Manning: I believe that they in fact will run off and start legislating individually in their own sovereign territories and harmonizing, getting to the common subset of risks. Globally I think is going to be a really interesting set of challenges. Is ICANN up to that? Are you guys up to that?

John Crane: So this is already happening, as you're probably well aware. The issue of critical information, infrastructure protection and whether or not DNS is part of that is being raised left, right and center by many governments. I think, not just from ICANN, say ICANN as staff, but ICANN as a community, there is going to be issues of how we give input into this.

I know as a staff member and other staff members, we do get asked by various governments to come and explain to them what the DNS is normally after they decide it's really important. And I suspect that others in the community are getting the same thing.

So I think as a community we do need to work on this and be aware of it. I don't know what the implication is for resources and for how far we get dragged into all of this. We certainly can't ignore it and I think it certainly behooves us as a community to try and make sure that the governments that are doing these kind of things are as well informed as we possibly can. And, yeah, we fully have a lot more work on staff to do in this area.

Patrick Jones: The DHS risk strategy that you're referring to is interesting because, as you're well aware, we were an invited subject matter expert into that as well as some of you that are here in this room. And I know you were, Suzanne was and there were some from industry.

The problem… One of the issues with that report though is that it was completed over a year ago and it's been sort of going through the approval process for posting. And so interesting to see if it's stale or how much has changed and that's natural with any document. But this is one that's been quite a bit of rapid change and already there's been some things happen.

So that's just one aspect. I believe there was also an [AENISIS] study that was 250-some pages, incredibly detailed on risk profile and stuff and…

Male: They don't overlap. That's part of the problem.

Patrick Jones: Marilyn.

Marilyn Cade: I have a question that's sort of related to that. In your non-contracted parties partners list, one thing that really stands out to me is who's not there. And I know you're just beginning to build those sets of relationships. But I might note that some of the regional multilateral groups are picking up as much interest in this set of issues and in addition to the IGOs, the Inter-Governmental Organizations.

And there are many, not only technical experts in ICANN, but many geopolitical experts in ICANN that have very strong relationships at the geopolitical level. And you, I think, are really going to need to be inclusive of that input into your outreach to them and it's going to be really important to reach into some of those regional groups. They probably have a very direct ability to help you to interact with groups of governments.

John Crane: Yes, and can I ask you to help us with that kind of thing because we do as staff, also get asked from who else should be involved in this and we don't always know, so you want to get together and have coffee at some point and… or anybody else who wants to talk about how we can reach out to these people in better manners is always good. We can always improve in that area.

Male: In light of recent changes or proposed changes by the U.S. Government and other bodies for blocking portions and lists and the DNS, we as an organization, have side-stepped the issue of organized blocking for a fair number of years, I would say, and I was curious as to what within the SSAC seems to be rising up as a political issue more and more. Are there any plans for addressing blocking within DNS? It seems to break DNSSEC pretty badly.

Jeff Moss: So actually it's… we actually published a paper on Saturday and apologies for SSAC publishing a paper in the midst of an ICANN meeting, but it was sort of important to try to respond to a request from the Government Advisory Council. And the paper is on the ICANN SSAC pages. It's SSAC 050 and I also wrote a little blog article that sort of gives an overview of it. If you want me to give you that later, I can.

But basically, SSAC's position at this point in sort of a 10-word sound bite is first do no harm. And so the principles in the paper identify the need for any organization, whether it be a private enterprise or a home, a family or organization, or sovereignty to understand the parties that are going to be affected by the policy to anticipate and try to consider the collateral effects of blocking and their set of missives and guidelines which is essentially a two-page high-level description of the consequences.

So, unlike the Protect IP paper that Dr. Crocker and Danny McPherson and several others wrote where they essentially identified and enumerated some of the technical issues and problems associated with this, this is more of a meta-look at the issue and a call to the attention of governments to the fact that understand what you're doing is not simply going to affect only people that you believe are under your sovereign administration.

And when we talked to the GAC yesterday about it, there was a significant amount of nodding of heads and that this was important for them to understand from the meta-level. But still some curiosity about some of the harder things to wrap your head around. Like if one government does it, what are the effects? If 14 governments do it, what are the effects?

There are probably some successive issues about legitimizing this as a reason to do blocking and then suddenly thinking, "Well, if it's right for anti-piracy and it's right for morality and public order, maybe it's right for phishing or maybe it's right for whatever – embargoes.

If you look at the number of different things you can now use in the [Maslow] Hammer manner, this can get quite a bit out of hand, simply at the administrative level, much less at the technical level. So I think there's a lot of work yet to be done in that and SSAC is probably going to pursue it. But read the first paper because that's actually going to be the principle on which we'll pursue all the rest.

Patrick Jones: So I think we're now at the end of our allotted hour and there's another group coming in after us, so at this point, Jeff, do you have some parting remarks?

Jeff Moss: Yes, I want to thank everyone for coming in and meeting us. I think we're almost all here through Friday or Saturday and if you have any questions we'll be in the back of the room right after this session and then we're… Just feel free to approach any of us if you have something of a more confidential nature; then don't talk to us in front of everybody, wait until we're close to the sun. Well, thank you very much for taking your time. We're officially closed.

[End if Transcript]