PATRICK JONES: Can everyone hear me okay? This is Patrick Jones, Senior Director of Security, from the ICANN security team. As you know I've provided a briefing to the Review Team in Beijing on where we were in the progress of implementation. Since that time we are still advancing through the various recommendations.

I think at this stage it's still premature to say where we are on implementation and the lessons learned because we're still in the progress. The board adopted the final report of the SSR Review Team at the ICANN meeting in Toronto and we're now working through those recommendations that can be done by staff and identifying those recommendations where there will need to be staff and community or staff and advisory committee collaboration in order for those to be properly implemented.

I will also add that we did publish for community review a status report of the 28 recommendations as part of the FY 14 security stability and resiliency framework. That was published on March 6 before the Beijing meeting. It is now in the reply phase of comments. It's my intention that the spreadsheet of responses to the ATRT-2 would also be made available for public consumption. So that would be an addendum or an additional document that would show the community where we are in implementation in our progress.

BRIAN CUTE: Okay. We're just trying to follow on the screen. We're having some technical difficulties. When you talk about implementation efforts could you refer to the recommendation number as well just so we can follow along on the screen? We've got one through four in front of us and can scroll down to read the rest.

PATRICK JONES: Sure. One of the advantages that we had is while the SSR Review Team was doing its work we were following along in parallel and in some cases we're taking steps of doing advance work on implementation, so a good example is recommendation 1, publishing a single clear consistent statement of the SSR Role and Remit. In May of last year we published a draft statement while the Review Team was doing its work to again to socialize the ideas with the community. We ran a longer than normal public comment process on that document. In fact, it ran through September of 2012, and then we synthesized the comment and made that available at the ICANN – in advance of the ICANN meeting in Toronto in October of 2012. A revised version of that work that took into account the public comment was incorporated into the FY 14 document that was published in March. So that's an example of how we've done some implementation along the way. Another example is with recommendation 15 of providing some...

BRIAN CUTE: That's 14 you said, with a five?

PATRICK JONES: Yes, recommendation 15. One, five. That's to facilitate responsible disclosure of security threats and mitigation techniques. So in March of this year we published a set of guidelines for the community, particularly for security researchers and others, a way to report things to the ICANN security team so that they can be dealt with in an appropriate manner. That also grew out of collaborative discussions with SSAC and I think largely that the publication of that process has been well received.

BRIAN CUTE: Let me ask you a question, Patrick. I'm reading the recommendation that ICANN should act as a facilitator in a responsible disclosure and dissemination of DNS security threats and mitigation techniques. Did that recommendation or the implementation of it shed any new light on ICANN's role in this ecosystem?

I have an understanding that from an operator's standpoint or operators DNS infrastructure that ICANN does have a role to play, facilitator as defined here. ICANN also operates a root and has relationships contractually with the operators of infrastructure. Did it provide any light or clarification either for yourself or an understanding with the infrastructure operators in that respect?

PATRICK JONES: Look, I think the work of the review team was helpful in crystalizing the thought process for the security team over the last 18 months of when and how to reach out to different operators. Over the course of the work of the Review Team there were also some real-world examples that helped show when we needed to be a responsible party in the process.

A good example I believe was a year ago in the threats from Anonymous on potentially attacking the root operations resulted in collaboration with the parties in the ecosystem, and that was a good example of how different parties were able to talk to each other and that we could play a facilitating role not a governing role, or even largely a coordinating role. It was just a way to bring different groups together.

BRIAN CUTE: Thank you. I think another area that's not clear for a lot of people in the community, the broader global community, the Internet community is necessarily the scope of what ICANN is responsible for when it comes to security. In the implementation of any of these recommendations, do you think that effort helped to clarify ICANN's role in the ecosystem, if you will, and if so which ones would you point to? Or if any of them made things worse in your estimation, which ones would you point to?

PATRICK JONES: Well at this point I don't know if I can point to anything that the recommendations have made worse because largely what the Review Team has done is given a set of practical, usable recommendations that could be implemented. I think what we've seen from the early work that was done around recommendation 1, but also the work on

recommendation 4 of documenting the security relationships with the community.

All along this process we have tried to come up with some clear definitions of what we think security, stability and resiliency means for ICANN and a very clear explanation of what ICANN's (limited) technical mission is, and these guidelines or recommendations have been reasonable enough that we have been able to work with them.

And I think from the public comments we've received to date and also the public comments on the earlier draft statement of ICANN's role when we met, the community reaction has been largely positive and I think if you take a look where we've progressed from the draft statement to the current documents that's out for public comment the input that has come in has been that we can see that the security team has made changes to the statement that reflect the public comments and now we're at a point where we're really trying to reach out beyond the usual groups that are aware……

BRIAN CUTE: Are you there? Patrick?

STEVE CROCKER: I assume this is the case, but I am just double-checking. We are anticipating a spreadsheet similar to WHOIS and ATRT for the SSR?

BRIAN CUTE: Yes. That's coming. Thank you very much.

STEVE CROCKER: And that will be today or…?

UNIDENTIFIED FEMALE: Well, we'll confirm (inaudible) in the next two days.

STEVE CROCKER: Oh, I see. Okay. Thanks.

BRIAN CUTE: For those of you online, Patrick has fallen off and we are waiting for him to get up.

PATRICK JONES: Hello!

BRIAN CUTE: There you are.

PATRICK JONES: Hey. I'll blame it on (inaudible).

BRIAN CUTE: Okay. Fine by us. Please carry on.

PATRICK JONES: Okay. So I was answering your question about where we think the recommendations have been helpful in having us implement our role and remit, in clarifying our role and remit? Is that correct? And I was rolling with a really good comment, so I am not sure where you lost me in that process, but maybe I should stop and see if there's other questions.

BRIAN CUTE: Well, yeah, and we can open up to other questions and the other thing we were thinking while you were offline too is if you wouldn't mind you

could walk us through the recommendations in order numerically. That's what we've been trying to do with the other presenters. You touched on number one already, but if – are there any questions for Patrick at this juncture. And I'm looking online as well. Not seeing any.

Yeah, Patrick why don't you pick it up at recommendation number 2 and then just walk us forward. Again, the effect of implementation on this recommendation – positive, neutral, negative. If it hasn't been implemented yet just a clear explanation as to what have been the challenges or obstacles to achieving that. Thanks

PATRICK JONES: Okay. Take it to recommendation 2. Doing our definition and implementation that it should be reviewed in order to maintain consensus and elicit feedback from the community. So I don't believe that this recommendation has been implemented yet, because one way to read this is that first we have to have a single clear consistent statement that is recognized by the community. So I think that work is reflected within the existing FY 14 framework, that we need to close that off and the public comment process that is associated with it first.

I will say that each year we have published a security, stability and resiliency framework, at least going back to 2009, so we have now done an annual process of publishing a document. In the FY 12 framework was published while the Review Team was beginning its work and one of their early comments to us was that it would be helpful for the security team and for ICANN to publish a status report showing what had been implemented along the way or how the previous years' activities had been completed.

And so in the FY 13 document we, published a status report from FY 12, showing the Review Team that we were taking in consideration their early thoughts before their work was done and they referenced that in their report as a positive step for us. In the FY 14 version I think we took it a bit farther and tried to provide more information in our status report and that will keep getting refined, especially as we adapt that to the at-task reporting that Fadi introduced at the Beijing meeting.

BRIAN CUTE: So, let me ask you, Patrick, looking at it kind of for the first time, if you boil this down it's saying ICANN – provide a statement, a definition of what your remit is and tell the community how you've implemented against that remit to maintain consensus and elicit feedback and do that on a regular basis. How do you measure consensus to make sure that the community is still with you on, yeah, this is an appropriate statement of your role and we agree with the way you are implementing under your remit?

PARTICK JONES: You know, that's a big question that you could ask of any of the policy processes that ICANN does. One way that we look at this is making sure that we take into account the comments that are received on the draft

statement and the statement that's in the existing framework, make sure that we are conducting a very thorough socialization of that statement with all the supporting organizations, advisory committees, reaching out broadly to stakeholder groups and making sure that they are largely pleased, or at least with the definition of consensus that we use in other policy processes, agree that that's the appropriate statement. And then we move into reviewing that on a regular basis.

BRIAN CUTE: Thank you. Any other questions for Patrick? Recommendation 2? Okay. Would you please proceed down to recommendation 3 please, Patrick.

PATRICK JONES: Sure. So this one, again, this is once we've done a consensus- based statement and we need to make sure that the definitions of security, stability, and resiliency and the other terms that are in the document – for example what the definition of ICANN's technical mission is and the role and remit are used across the organization. So I think this one, our approach will be first to make sure that there is several opportunities for all staff and also board to be aware of what the Role and Remit Statement is and how we've treated the recommendations. Providing a webinar, educational materials. Also making sure that in the communications and in the outreach materials that are used by ICANN department's presentations are consistent with the terminology that has gone through this public comment process – and that education effort is going to take some time.

BRIAN CUTE: Thank you. Questions? Looking around the room, online. No questions? Recommendation 4 please, Patrick.

PATRICK JONES: Sure. So this is one of defining the nature of the relationships that ICANN has in the community. One approach that we've already taken and you saw it in the FY 14 framework was a visualization of the functions of security at ICANN. So we had this image that showed the organizational risk management, the threat awareness component, the coordination component, and the (bot) leadership and technical engagement component.

Within those four components we are then going to identify the existing relationships. So some of these are apparent in (inaudible)of understanding in contracts and accountability frameworks and partnerships or contracts with registries and registrars. There are other relationships that are not so apparent. Some of them are either based out of trust-based lists that ICANN participates in. They're also from providing technical engagements at different events and requests for ICANN participation. So we're in the process of doing - the easy bit is that you can document the contracts and the MOUs and things, but then the next step is, from an internal staff perspective, making sure that it's clear where there are existing channels of communication and relationships with different entities in the community and making those apparent for the public, and for the community, too.

BRIAN CUTE: Thank you. And actually we are pulling that image up on the screen in the room so everyone can take a look at it and see if it generates any questions here, and just walk thought it and see from a consumer prospective how it works on our end. It's a pictoral diagram, Patrick?

PATRICK JONES: Yes, it's page 16 of the framework.

DENISE MICHEL: So what they're looking at Patrick – hi, this is Denise – is you know on your blog post you have the tracking for the Review Team recommendations. We're looking at that. Do you want to look at something else?

PATRICK JONES: You know, we don't have to have them divert away from this document right now. I will just point out that it is on page 16 of the current FY 14 SSR framework.

BRIAN CUTE: Yeah, why don't we go to the diagram just so we can see it? I think it will provide some context, too, that could be helpful for the discussion.

PATRICK JONES: It's the x-plane graphic that is within the document.

BRIAN CUTE: Right. Then we can come back to the tracking document efforts. I just think that for those of us who are not close to SSR issues in ICANN, it might be useful to see the picture and gain an understanding and we might be able to have a more fruitful discussion with you, too, as well. Just bear with us.

PATRICK JONES: And while you're pulling it up, so this document is, I will say in version one status, so as part of the public comment period its – we can certainly take input on the document, but even separate from that, if any of the Review Team members or others in the community have recommendations for how better to depict the relationships and the functions of security, we'd be welcome to hear those.

BRIAN CUTE: Do you anticipate that this diagram by x-plane, once it's gone through its process, be on the front page of the website like the other diagrams, kind of front and center for the community to see or do you intend a different use for it for positioning?

PATRICK JONES: No. I think it could be. One of the nice things to see is how some of the different stakeholder groups and constituencies have asked for material like this. So at the Beijing meeting, the business constituency included this graphic in page three or four of their newsletter that they handed out to participants at the ICANN meeting. So this is the type of thing that could go in collateral that people hand out or in presentations that others in the community could use. I know our global stakeholder engagement team asks for material like this all of the time, and so having something that people are able to draw from and even break it down into its component parts. So for example you'd be giving a talk and want to focus in on the threat awareness piece or focus in on the

technical engagement piece. We're able to do that and provide more detail.

BRIAN CUTE: Thank you. We've got it up on the screen now. If you could just, at a high level there's clearly four distinct parts to this and I can see the organizational risk management at the top and then threat awareness, coordination and technical engagement across the bottom. If you can just kind of conceptually walk us through those pieces and again focus in on SSR and ICANN and where it fits and what its role is.

PATRICK JONES: Sure. So the top part outlines the more traditional function of security in any organization and so that we've defined as the organizational risk management piece, and that is everything from the network security, internal physical security, the traveler security, security at ICANN meetings, our work with finance and legal and making sure that as new services are introduced that there's appropriate auditing and risk management done. This would be typical for any organization. It's not unique to ICANN.

When we move into the bottom areas, our functions of security that are more outward facing. So the thread awareness component is ICANN may receive information in a variety of ways and it shows the flow of communication to the community and out to the global layer of the community. The coordination piece focuses on ICANN's coordination of the root zone operations, the IANA functions, L-root and then also courting the parties in policy development as they work with SOs and ACs.

And the last quadrant is on the technical engagement piece, and that is explaining the function of the security team providing a service for the community, their requested trainings through the regional TLD organizations or in partnership with others like the Network Startup Resource Center or ISOC. We do quite a bit of training, and we've done this over ten years and it's one of the things that I think the community sees as a positive from the security team.

BRIAN CUTE: I'm just asking an overarching question here not necessarily tied to this recommendation, but just in terms of accountability and transparency, in these different roles – threat awareness, coordination, technical engagement – in what way to you feel accountable to the community or communities you work with? What are the mechanisms or interactions that hold you accountable in your role?

PATRICK JONES: So from a threat awareness standpoint, in some cases we've provided after action reports either on an after action report of exercises that we've done. The publication of that document is something that the community could see and ask questions. Another example is the publication of the reports from the annual security, stability and resiliency symposiums that have been done so that if the community

has questions about the functioning of the symposia or another event, that the materials are published and we can take feedback on them.

The other way is – this is somewhat of a new thing, for individual functions that ICANN have a high-level explanation of what they are. And in some cases the security team might be ahead of other parts of the organization in being clear, or at least as clear as they can be, of the different functions that it plays. And so maybe this is a leadership thing that other departments can see or other departments of the organization can use.

BRIAN CUTE: Thank you very much. Any questions on the diagram? Okay. Why don't we jump back to the recommendations? Thank you Patrick. That was helpful. Are we on Recommendation 4 or 5?

PATRICK JONES: We're on five now.

BRIAN CUTE: We're on five. Yes, if you would. Thanks.

PATRICK JONES: So I think four and five are closely tied together and this is one that until we get the definition of SSR, of the role and remit and off the documentation (inaudible) relationships, we're not in a position to show how this has improved things yet.

BRIAN CUTE: Fair enough. Thank you. Notes, questions? Nope? Let's move on to 6.

PATRICK JONES: Okay. So Recommendation 6. I think this is one that will require collaboration with the advisory committees that are referenced in the recommendation. So this is publishing a document that outlines the roles and responsibilities for SSAC and RSAC.

SSAC largely has this in their operating procedures, and after the Toronto meeting I presented our proposed implementation plan at the November workshop for SSAC in Los Angeles and they were largely in agreement that the language that describes the role and responsibilities of SSAC in the operational procedures met this.

There's a step that I think that needs to happen of carving that out and taking it back to them and making sure that it has their approval. For RSAC the ICANN board implemented by-law changes impacting RSAC at the Beijing meeting. Now we're at the place where once those bylaw changes are implemented we can go back to them and see if they are in agreement with the text on roles and responsibilities.

BRIAN CUTE: Thank you. Questions? Seeing none. Can we move on to 7?

PATRICK JONES: So this is one that over the last few years with the existing SSR frameworks. We've had a set of objectives and initiatives published. Now with the addition of the new management delivery process that Fadi and the executive team are implementing and also the development of a new strategic plan, this is one that will come in

parallel with that work. The other thing that we need to do is make sure that it is done with the cost-benefit and risk analysis and that is something that groups such as the ccNSO has been very keen to make sure that we do.

BRIAN CUTE: Do you see this implementation being kind of overtaken by the new strategic priorities being set by the CEO? Are they going to be reshaped, if you will?

PATRICK JONES: What helps is security is part of the core mission of the organization, so unless there is a plan to change the mission and the core values for ICANN security will be there. I think this work will need to wait until there is an updated strategic plan, and also is part of the publication of the next budget and operating plan.

BRIAN CUTE: Thanks. One of the things we've asked other staffers to provide – and the same would be asked, Patrick – if a recommendation has not been fully implemented for whatever reason, whether it was poorly designed by the review team or there are resource constraints or whatever it was, that to the extent you can, provide us with clear statements of the reasons why.

If one of these is that the new CEO has a strategic priority that is being launched, and ergo this implementation will be in a hold status for a while, that is useful to us. One of the things we want to do is to learn from the experience of implementation and also provide useful and well-designed recommendations going forward. So if you can provide specifics on that after the fact, that's very welcomed.

I'd like to ask you a question on recommendation 8. What do you mean by the phrase DNS availability? Just so I'm clear. The goal of maintaining and driving DNS availability. Is that from an operational prospective? Is that the resources that are used to provide DNS operationally? What's the exact meaning of that phrase?

PATRICK JONES: So that is a good question. It's one that we've tried to provide a specific answer to what is meant by availability as part of the – we did put it in the FY 14 framework as part of the definition of unique ICANN identifier health and this is one that came out of the work of the Kyoto SSR symposium. I think that was from 2010. I know those more technical in the room who worked on this might also be of assistance, but this is one that we wanted to point to the technical uses of the term availability and the use of availability in the previous strategic plan was a new term from the year before. So we want to make sure that its being used in the most accurate way reflected to ICANN's work.

BRIAN CUTE: So how do you view the meaning of the term?

PATRICK JONES: Why don't I provide that in a full response that is technically accurate in material to the review team?

BRIAN CUTE: Sure. Fair enough. Steve?

STEVE CROCKER: Hi. Steve Crocker here. Hi, Patrick. One of the things – kind of continuing along the same lines of availability, the natural thing for most of us to think about is the uptime of the DNS servers, and in the past whenever we've tried to follow this line of questioning and what is ICANN's role in this respect, the conversation usually goes very quickly to "we can't keep the L-root servers running." Well that's very nice and I know that ICANN does a stellar job of doing that, but that's a long way from the whole of the domain name system. It's a long way from the whole of the root for that matter, and the root is an infinitesimally small part of the whole domain name system.

So it makes me a little uncomfortable when we make a claim like that and we don't have the authority or the responsibility or the mechanisms to apply that in the largest sense that people might actually expect us to or think that we have something to do with. So I'd like to keep our words aligned with what our real capabilities are.

BRIAN CUTE: Go ahead, Patrick.

PATRICK JONES: One thing to keep in mind is that when the review team was doing its work, this is the language that was in the strategic plan at that time. If the next version of the strategic plan or our future uses are going to change on where we're more specific on what we mean about DNS availability, then I think our implementation of the recommendation will take that into account.

BRIAN CUTE: Thanks very much. Any other questions? Move on to recommendation 9, please.

PATRICK JONES: So this is one where implementation will require collaboration with our IT Department in addition to making sure that there's agreement and approval of our other departments that are impacted by IT. So I think that there's existing work within the IANA team for a SysTrust audit and the requirements that the IANA functions must be met under the agreement with NTIA. So this recommendation is in process and we are assessing the options based on recognized international standards.

BRIAN CUTE: Yes, David.

DAVID CONRAD: Patrick, the recommendation I guess says ICANN should access the certification standards. So far, as I understand it, the certifications have been applied to certain portions within ICANN – for example IANA or IT or whatever. Is there a roadmap to get ICANN as the corporate entity certification or is it going to remain focused on specific components of ICANN.

PATRICK JONES: So at this stage I think it's too early to tell. I think that will depend on the function. So an example may be that there may be certification that

is required in order to operate RPKI or to have ICANN operate as a certificate authority. So that is work that I think will have to depend by the departments that are impacted, but one of the things that the Review Team did not want to do while they were developing this recommendation is specify the approach. This gave ICANN the flexibility to see where the certification was most needed.

BRIAN CUTE: Do you have a sense of when the roadmap would be published? Roughly?

PATRICK JONES: No, at this stage. Not yet.

BRIAN CUTE: Okay. Thank you. Any other questions? Okay, Recommendation 10, please.

PATRICK JONES: So in our review of this recommendation, I think it is tied closely to the implementation of the WHOIS Review Team work and the work that is already well-documented for compliance as part of the implementation of that review.

BRIAN CUTE: So implementation of this is tied to implementation of other recommendations under the WHOIS Review Team from a timing perspective?

PATRICK JONES: This recommendation is – I think this highlights one of the challenges we have with all of these recommendations is that in some cases they are rather broadly worded. In reading the words, it's that we should continue our efforts to step up contract compliance enforcement and provide adequate resources for these functions.

The compliance team has grown over the last two years and has done quite a bit of work in documenting and establishing their processes. So that is one of the things that we will be able to point to in showing how compliance has changed over time and has stepped up their work. I think also the work that the compliance team is doing to meet the obligations in the WHOIS Review Team will be useful in completing this recommendation.

BRIAN CUTE: You're right. The way it reads, it's very generic. And I'm looking at recommendation 11 which says ICANN should finalize and implement measures of success for new gTLDs and IDN fast track that expressly relate to its SSR-related program objectives. You don't have that SSR-related program objectives qualify in recommendation 10 so looking at it, it looks very broad. It's the subject of a recommendation from another review team. How did you receive this recommendation? How did you understand it when you received it? Does the report behind these recommendations provide you any clarify about exactly what the SSR piece of this recommendation is?

DENISE MICHEL: Hey this is Denise. Hey, Patrick. I just wanted to add some additional background here since I was also involved in with the team and in the development of these recommendations. During the course of the SSR review, and think Patrick can expand on this, and during the course of the SSR review, the team also looked at and they wanted to make sure that they reinforced the connection between some of the compliance activities in ICANN and the WHOIS issues in security, stability and resiliency.

But they also recognized that for, especially the WHOIS component, was the purview of the WHOIS Review Team. They still wanted to call it out to acknowledge the importance of the SSR connection to that and so you have a sort of a broad recommendation and then behind that is the understanding that ICANN has a series of implementation activities that flow from the commitments ICANN has made and the CEO has made and also flow from that WHOIS Review Team. And then similarly with 11 they recognize the in-depth metrics activities that are going to flow from the Consumer Choice Competition and Consumer Trust, which is a final review that will be coming shortly. So that's a reference to that, and again an acknowledgment that SSR is a component there. And Patrick, I don't know if you have more to add there.

PATRICK JONES: No, I do not.

BRIAN CUTE Thanks, Denise. Fiona Alexander.

FIONA ALEXANDER: So I think just as a practical matter for recommendation 10, the presentation we heard yesterday from Maguy and Margie that was sort of fulfilled with that actually. It would make sense to me, but I just want to make sure that is what you are saying.

BRIAN CUTE: Just so you have a prospective of this Review Team and improving on the structure recommendations, the focus of recommendations, I clearly understand the desire to have an express tie-in to SSR on compliance. I don't quibble with that at all. I also think of it not just from how to construct recommendations well and in an focused way, but from an organizational sense, if you've got a recommendation the WHOIS Review Team report and then a similar one in this one, in my own organization I could see that leading to a potential circumstance of someone saying, "I've got that ball, no, you've got that ball."

And just when you get down to execution against this – something for review teams to be aware of when they are writing recommendation is what I am getting at that if there is execution against a recommendation that it is clear who owns it. And there could be benefits in other parts of the organization, but we wouldn't want to make the mistake of confusing internally who has got the responsibility of executing.

DENISE MICHEL: Yeah, and Patrick can speak more to this, but we have a pretty cross-functional cooperative team approach at the staff level and I don't

believe staff has any concerns about our ability to coordinate on the programs and execute on this. And Patrick will be giving you more information as he goes forward on these.

BRIAN CUTE: Great. Thank you. Patrick, do you want to pick that up?

PATRICK JONES: Yeah. So I think that we're now down to recommendations 12 and 13.

BRIAN CUTE: I see 11. Could you pick it up there?

PATRICK JONES: I thought Denise covered 11.

BRIAN CUTE: Oh, that's dependent on the Consumer Choice and Trust….

DENISE MICHEL: Yes, and there's an IDN fast track component, too, that we'll pull out and we'll be providing more information on the activities that are occurring that will relate to the fast track that tie in here and what the deliverables are.

BRIAN CUTE: Thank you. 12, please, Patrick.

PATRICK JONES: So 12, in our implementation approach, we've linked 12 and 13 closely together because one is identifying best practices that can go into contracts, agreements, MIUs and other mechanisms. And the other is encouraging the supporting organizations, and as the registries noted this should also include stakeholders to encourage them to develop and publish their best practices for their members.

So an example in 13 is that the ccNSO has a tech working group and that working group is looking at developing a – right now they are not using the term "best practices" but they're using guidelines for ccTLDs to follow. It would basically include best practices but it is something that would be coming from the ccNSO. So they're already taking a leap on developing something to meet this. What we need to do now is to go back to the SOs and stakeholder groups and explain what these two recommendations are and get some – involve them in the approach to implementation. And that's a step that we'll be doing between now and Durban.

BRIAN CUTE: Thanks. So it that a series of presentations and meetings? I'm thinking about how do you implement this and then report back to your boss and the Review Team that we've done a good job here. The recommendations that you encourage all supporting organizations – that's not the clearest word. How do you do that, Patrick?

PATRICK JONES: I think we would start with either offering a webinar or some kind of presentation on the stakeholder group or their supporting organization's regular call. I'm not sure that's the best use of the GNSO's time as a whole, so this is probably one that I would break down into going to the IPC and going to the business constituency, and to the registries and the registrars, and presenting what the recommendation

is and working with them on what would be a set of best practices that they might want to publish for their members.

BRIAN CUTE: David?

DAVID CONRAD: So 12 actually talks about contract, agreements MIUs and other mechanisms. Has there been any efforts in that area actually to enter into contracts that are identifying best practices and supporting them through contracts and MIUs and stuff?

PATRICK JONES: I think that this is where probably what we should do is highlight in the current Registrar Accreditation Agreement that's out for public comment as well as the recently-posted new gTLD registry agreement, that there are a set of SSR-related components in both of those new agreements and that the staff did work with, or the security agreement did participate with the new gTLD team and other staff that reviewed those documents while the negotiations with the respective parties were happening. We could point to the areas in those agreements where we think that those show up.

BRIAN CUTE: Thanks. Yeah, actually if you could provide that, just as part of this further input that would be useful. Thank you. Any other questions on 12 or 13? Okay. Let's keep moving.

UNIDENTIFIED FEMALE: Patrick, you have a hard stop at what time?

PATRICK JONES: Well, I could probably go for another 15 minutes, but it's on Eastern Time here. I should probably not go much past the next 15 minutes.

UNIDENTIFIED FEMALE: We've got – I think there's a total of 28? Is that 28 recommendations?

PATRICK JONES: Yeah. We're about halfway. I could do a few more.

UNIDENTIFIED FEMALE: Do you want to go in sequential order? And I guess it's a question for you and the team. Would you want Patrick to highlight a couple that he thinks are particularly important, and perhaps worth discussing?

BRIAN CUTE: We can do that just as long as we keep track of what he doesn't address today and we can schedule a follow-up.

UNIDENTIFIED FEMALE: Sure. We can definitely do that.

PATRICK JONES: Well, one thing I would mention is that we're going to get into a set of recommendations that are tied closely together, so we might be able to move through a few of them a bit more quickly.

BRIAN CUTE: Okay. Which ones are those?

PATRICK JONES: So near the end, the risk management recommendations – those are recommendations 25, 26, 27. That's all work that is tied to the DNS risk management framework working group effort.

BRIAN CUTE: Please.

PATRICK: Sure. So at the Beijing meeting, there was a presentation from Westlake Governance, which is the consultants that are assisting with that work, so recommendation 25 is that we should put in place mechanisms to identify both near and longer-term risks as part of risk management framework, and that recommendation 26 is that we should prioritize timely completion of a risk management framework.

So this is one that – there's a board-level working group. I don't know if there's other board members in the room on the call who would be able to talk to this effort. Bill Graham is the chair of that working group, and it does include a cross-section of some non-board members as well,([Patrick Polstrom) and (Roloff Meyer) are on the working group in addition to ICANN board members, and this is one that – we've retained Westlake they presented a draft framework in Beijing. Between Beijing and Durban they will be finalizing a framework that can go to the working group and then also go out to the community for comment. So we are putting emphasis on a timely completing of that, and then the next step is to do a cycle of (inaudible) assessment.

BRIAN CUTE: Thanks, Patrick. When you're undertaking these types of activities, risk management processes, procedures, mechanisms, obviously in assessing risk and mitigating risk, part of security is identifying the risk and coming up with tools to mitigate against risks, but at the same time, not – you're saying in recommendation 26, "ICANN should prioritize the time of completion of this framework and the work should follow high standards of participation and transparency," and when it comes to security, sometimes being transparent about the tools and actions you're taking to mitigate risk is not the smartest thing to do in terms of exposing to bad actors what you're doing to protect yourself.

So how do you – how are you going to walk that line in being transparent about this while being smart from a security perspective? What approaches will you take where you can't be as transparent as the recommendation might ask? How do you address that?

PATRICK JONES: Well, so this is one where there's a difference from being transparent about the process and about the framework itself from sensitive information that might arise in doing the work of the risk management. I think we've also seen examples from the community-driven effort, the DNS security instability – now working group – came up with some approaches for handling sensitive information in the context of a DNS risk review, so there are examples that we can follow.

BRIAN CUTE: And you'll document those, and to the extent that you can identify them as part of your procedures, that'll be – that part will be transparent to the community?

PATRICK JONES: Yeah. And this specific recommendation is on the development of the framework. The board-level working group has had public sessions at the ICANN meetings in – I guess going back to Costa Rica to Prague, Toronto and in Beijing, so their work at those meetings has been open for anyone to attend. And in fact, in Beijing, it was a pretty full room. There was a lot of discussion, and so that work has definitely been participatory for those who have taken advantage of it.

BRIAN CUTE: Thank you. Questions? Okay. Seeing no questions – yeah, Fiona?

PATRICK JONES: So if I could, do you have a minute?

BRIAN CUTE: Go ahead, Patrick.

PATRICK JONES: No, Fiona.

BRIAN CUTE: Fiona Alexander.

FIONA ALEXANDER: Sure. Just recognizing Patrick's limited time. So recommendation 28 and recommendation 15 seem very similar when I read them, but I was curious what Patrick's perspective was on those two recommendations and how they were different, if I was reading it differently, and also what the plan was for the two those. Both of those remind me of the proposal several years ago for a DNS cert that received a wide variety of these amongst the ICANN community, so I'm just curious as to how that is playing out as he reads these and if he's reading them in the same way I do refer them.

PATRICK: Right. No, so I do read them differently, and earlier in the call, I talked about our handling of recommendation 15 as the publication of a responsible disclosure process so that if researchers or others in the community see the issues with either ICANN networks or systems or processes, that there's a way to report those and appropriately disclose them to ICANN.

So I see that as – this was one – recommendation 15 is either as a facilitator or where parties can responsibly disclose them so that we can route them to the right place and report them appropriately after the fact. That's not the same as functioning as a DNS cert.

Recommendation 28 – this is more in line of some of the other recommendations that talk about engagement. This is more, I think, I see as a supportive recommendation, and so for this one, I think we would need to document the different ways that we are engaging in this activity and showing in the types of efforts that are done to do the things that are covered in this recommendation.

I don't think that this is one that – it's not an easy one to show how you're implementing, other than describing the different flora that we're participating in to do this activity.

FIONA ALEXANDER: But it's clearly not a cert issue, and in fact, the FSR review team did a lot of very in-depth research and discussion about that whole phase of considering when a cert was considered, and made very strong distinctions about what they felt was appropriate and what they were asking ICANN to do in that previous activity.

BRIAN CUTE: Okay. I'm going to suggest that we break here to respect your time, Patrick. We'll schedule a follow-up with you for recommendations 14 through 24 – presentation on that – and we're going to about the business of hopefully developing some follow-on questions, too, that may come at you in the interim. So, Denise I'm sure will work with you to schedule a follow-on to finish up the presentation. Thank you very much for your time with us today.