For Best Audio: Join via Telephone Using Dial-Out

Connecting via the audio bridge is always preferable to the AC audio connection.

Upon logging into Adobe Connect, a pop-up window will appear for the AC to call your phone. This preferred method will assure the best audio for the meeting.

Join Audio Conference

How would you like to join the meeting's audio conference?

- ● Dial-out [Receive a call from the meeting]

  +1 (USA) ▼   310-111-11111

- ○ Dial-in to the Audio Conference via Phone
- ○ Using Microphone (Computer/Device)

  [Join] [Listen Only]

After 2 background noise occurrences, staff will mute the offending line (either Telephone or Adobe Connect).

After two failed attempts to speak over the audio, participants will be invited to type their comments in the chat or take them to the mailing list.

PLEASE ALWAYS MUTE WHEN NOT SPEAKING!
*6 to mute and *6 to unmute

For any questions, dial out requests, apologies, please email: mssi-secretariat@icann.org

SSR2 Review Team Plenary Call #43

13 September 2018

Agenda

1. Welcome, roll call, SOI updates
   a) Staff to highlight rec. 16 in CCT report for team

2. Barcelona update from staff & confirm if any team members have not yet heard from constituency travel team

3. Finalize comms/outreach plan

4. KSK rollover - what does the team need to look in to?

5. Review of SSR1 recommendations
   a) Review table of outstanding questions
   b) Discuss SSR1 recommendations

6. AOB

7. Confirm action items / decisions reached

CCT Recommendation 16

See page 101 of the [Final Report](#)

Recommendation 16: Further study the relationship between specific registry operators, registrars, and DNS Security Abuse by commissioning ongoing data collection, including but not limited to, the ICANN Domain Abuse Activity Reporting (DAAR) initiative. For transparency purposes, this information should be regularly published, ideally quarterly and no less than annually, in order to enable identification of registries and registrars that require greater scrutiny, investigation, and potential enforcement action by the ICANN organization. Upon identifying abuse phenomena, ICANN should put in place an action plan to respond to such studies, remedy problems identified, and define future ongoing data collection.

To: The ICANN Board, the Registry Stakeholders Group, the Registrar Stakeholders Group, the Generic Names Supporting Organization, and the Subsequent Procedures PDP WG, **SSR2 Review Team.**

Update from Staff on Barcelona

Confirm if any team members have not yet heard from ICANN Constituency Travel team

Finalize Comms / Outreach Plan

KSK rollover - what does the team need to look in to?

Review of SSR1 Recommendations

a) Review table of outstanding questions

b) Discuss SSR1 recommendations

Proposed SSR1 Recommendations Table

RECOMMENDATION 1: ICANN should publish a single, clear and consistent statement of its SSR remit and limited technical mission. ICANN should elicit and gain public feedback in order to reach a consensus-based statement.
What was done to implement the recommendation? Was the recommendation fully implemented?
Did the implementation have the intended effect? How was the assessment conducted?
Is the recommendation still relevant today? If so, what further work needed? If not, why not?

SSR1 Recommendations

#	Detail	Grouping
1	ICANN should publish a single, clear and consistent statement of its SSR remit and limited technical mission.	OCTO
2	ICANN's definition and implementation of its SSR remit and limited technical mission should be reviewed in order to maintain consensus and elicit feedback from the Community.	Ops & Finance
3	Once ICANN issues a consensus-based statement of its SSR remit and limited technical mission, ICANN should utilize consistent terminology and descriptions of this statement in all materials.	
4	ICANN should document and clearly define the nature of the SSR relationships it has within the ICANN Community in order to provide a single focal point for understanding the interdependencies between organizations.	OCTO
5	ICANN should use the definition of its SSR relationships to maintain effective working arrangements and to demonstrate how these relationships are utilized to achieve each SSR goal.	OCTO
6	ICANN should publish a document clearly outlining the roles and responsibilities for both the SSAC and RSSAC in order to clearly delineate the activities of the two groups.	Policy
7	ICANN should build on its current SSR Framework by establishing a clear set of objectives and prioritizing its initiatives and activities in accordance with these objectives.	Ops & Finance
8	ICANN should continue to refine its Strategic Plan objectives, particularly the goal of maintaining and driving DNS availability. The Strategic Plan and SSR Framework should reflect consistent priorities and objectives to ensure clear alignment.	Ops & Finance
9	ICANN should assess certification options with commonly accepted international standards (e.g. ITIL, ISO and SAS-70) for its operational responsibilities. ICANN should publish a clear roadmap towards certification.	Ops & Finance

SSR1 Recommendations

#	Detail	Grouping
10	ICANN should continue its efforts to step up contract compliance enforcement and provide adequate resources for this function. ICANN also should develop and implement a more structured process for monitoring compliance issues and investigations.	Compliance
11	ICANN should finalize and implement measures of success for new gTLDs and IDN fast track that expressly relate to its SSR-related program objectives, including measurements for the effectiveness of mechanisms to mitigate domain name abuse.	GDD
12	ICANN should work with the Community to identify SSR-related best practices and support the implementation of such practices through contracts, agreements and MOUs and other mechanisms.	GDD
13	ICANN should encourage all Supporting Organizations to develop and publish SSR related best practices for their members.	Policy
14	ICANN should ensure that its SSR-related outreach activities continuously evolve to remain relevant, timely and appropriate. Feedback from the Community should provide a mechanism to review and increase this relevance.	OCTO
15	ICANN should act as facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques.	OCTO
16	ICANN should continue its outreach efforts to expand Community participation and input into the SSR Framework development process. ICANN also should establish a process for obtaining more systematic input from other ecosystem participants.	OCTO
17	ICANN should establish a more structured internal process for showing how activities and initiatives relate to specific strategic goals, objectives and priorities in the SSR Framework. It also should establish metrics and milestones for implementation.	Ops & Finance
18	ICANN should conduct an annual operational review of its progress in implementing the SSR Framework and include this assessment as a component of the following year's SSR Framework.	OCTO

SSR1 Recommendations

#	Detail	Grouping
19	ICANN should establish a process that allows the Community to track the implementation of the SSR Framework. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities, while not harming ICANN's ability to operate effectively. The dashboard process being used to track implementation of the ATRT recommendations serves as a good model.	OCTO
20	ICANN should increase the transparency of information about organization and budget related to implementing the SSR Framework and performing SSR-related functions. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities, while not impeding ICANN's ability to operate effectively.	Ops & Finance
21	ICANN should establish a more structured internal process for showing how organization and budget decisions relate to the SSR Framework, including the underlying cost-benefit analysis.	Ops & Finance
22	ICANN should publish, monitor and update documentation on the organization and budget resources needed to manage SSR issues in conjunction with introduction of new gTLDs.	Ops & Finance
23	ICANN must provide appropriate resources for SSR-related Working Groups and Advisory Committees, consistent with the demands placed upon them. ICANN also must ensure decisions reached by Working Groups and Advisory Committees are reached in an objective manner that is free from external or internal pressure.	Policy
24	ICANN must clearly define the charter, roles and responsibilities of the Chief Security Office Team	OCTO
25	ICANN should put in place mechanisms for identifying both near and longer-term risks and strategic factors in its Risk Management Framework. This process should be informed by insights from research, business partnerships, ICANN Supporting Organizations and other sources. ICANN should publish information about risks, recognizing the sensitive nature of some of these factors.	Risk Management
26	ICANN should prioritize the timely completion of a Risk-Management Framework. This work should follow high standards of participation and transparency.	Risk Management

SSR1 Recommendations

#	Detail	Grouping
27	ICANN should establish a process that allows the Community to track the implementation of the SSR Framework. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities, while not harming ICANN's ability to operate effectively. The dashboard process being used to track implementation of the ATRT recommendations serves as a good model.	Risk Management
28	ICANN should continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information.	OCTO

AOB
Confirm action items / decisions reached

ICANN