**DRAFT**

# Terms of Reference for the Second Review of the Security, Stability & Resiliency of the DNS (SSR2)

# 

**Background on SSR Reviews**

The origins of the Stability and Security Review (SSR) is found in [ICANN's Bylaws](https://www.icann.org/resources/pages/governance/bylaws-en), which provide accountability and transparency mechanisms through the empowered community. The reviews that were formally known as "AoC Reviews" are now referred to as "Specific Reviews" under these Bylaws.

Under the Bylaws, the Board is responsible for causing a periodic review of ICANN's execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect or are affected by the Internet's system of unique identifiers that ICANN coordinates (SSR Review). In [Resolution 2017.02.03.11](https://www.icann.org/resources/board-material/resolutions-2017-02-03-en#1.g) the Board convened the SSR2 Review Team and requested that this team develop and deliver to the Board their approved Terms of Reference and Work Plan, to ensure that the team's scope and timeline is consistent with the requirements of the ICANN Bylaws.

### ICANN Mission and Bylaws’ Requirements of the SSR2 Review

ICANN’s mission relative to the unique identifiers is the first article of its Bylaws:

*“Section 1.1. MISSION*

*(a) The mission of the Internet Corporation for Assigned Names and Numbers ("ICANN") is to ensure the stable and secure operation of the Internet's unique identifier systems as described in this Section 1.1(a) (the "Mission"). Specifically, ICANN:*

*(i) Coordinates the allocation and assignment of names in the root zone of the Domain Name System ("DNS") and coordinates the development and implementation of policies concerning the registration of second-level domain names in generic top-level domains ("gTLDs"). In this role, ICANN's scope is to coordinate the development and implementation of policies:*

*For which uniform or coordinated resolution is reasonably necessary to facilitate the openness, interoperability, resilience, security and/or stability of the DNS including, with respect to gTLD registrars and registries, policies in the areas described in Annex G-1 and Annex G-2; and*

*That are developed through a bottom-up consensus-based multistakeholder process and designed to ensure the stable and secure operation of the Internet's unique names systems.*

*The issues, policies, procedures, and principles addressed in Annex G-1 and Annex G-2 with respect to gTLD registrars and registries shall be deemed to be within ICANN's Mission.*

*(ii) Facilitates the coordination of the operation and evolution of the DNS root name server system.*

*(iii) Coordinates the allocation and assignment at the top-most level of Internet Protocol numbers and Autonomous System numbers. In service of its Mission, ICANN (A) provides registration services and open access for global number registries as requested by the Internet Engineering Task Force ("IETF") and the Regional Internet Registries ("RIRs") and (B) facilitates the development of global number registry policies by the affected community and other related tasks as agreed with the RIRs.*

*(iv) Collaborates with other bodies as appropriate to provide registries needed for the functioning of the Internet as specified by Internet protocol standards development organizations. In service of its Mission, ICANN's scope is to provide registration services and open access for registries in the public domain requested by Internet protocol development organizations.*

*(b) ICANN shall not act outside its Mission.*

*(c) ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide, outside the express scope of Section 1.1(a). For the avoidance of doubt, ICANN does not hold any governmentally authorized regulatory authority.”*

Under the [Bylaws](https://www.icann.org/resources/pages/governance/bylaws-en), Section 4.6(c), “(i) The Board shall cause a periodic review of ICANN’s execution of its commitment to enhance the operational stability, reliability, resiliency, security, and global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet’s system of unique identifiers that ICANN coordinates (“SSR Review”).

“(ii) The issues that the review team for the SSR Review (“SSR Review Team”) may assess are the following:

1. security, operational stability and resiliency matters, both physical and network, relating to the coordination of the Internet’s system of unique identifiers;
2. conformance with appropriate security contingency planning framework for the Internet’s system of unique identifiers;
3. maintaining clear and globally interoperable security processes for those portions of the Internet’s system of unique identifiers that ICANN coordinates.

“(iii) The SSR Review Team shall also assess the extent to which ICANN has successfully implemented its security efforts, the effectiveness of the security efforts to deal with actual and potential challenges and threats to the security and stability of the DNS, and the extent to which the security efforts are sufficiently robust to meet future challenges and threats to the security, stability and resiliency of the DNS, consistent with ICANN’s Mission.

“(iv) The SSR Review Team shall also assess the extent to which prior SSR Review recommendations have been implemented and the extent to which implementation of such recommendations has resulted in the intended effect.

“(v) The SSR Review shall be conducted no less frequently than every five years, measured from the date the previous SSR Review Team was convened” (see [Bylaws](https://www.icann.org/resources/pages/governance/bylaws-en), Section 4.6(c)).

**Operation of the Review Team**

* **Decision Making**

*Section 4.6. of ICANN’s Bylaws states: SPECIFIC REVIEWS (iii) – “Review team decision-making practices shall be specified in the Operating Standards, with the expectation that review teams shall try to operate on a consensus basis. In the event a consensus cannot be found among the members of a review team, a majority vote of the members may be taken.”*

In accordance with this article of the Bylaws the SSR2 Review Team (SSR2-RT) has agreed, by consensus, that all its decisions will be made on a consensus basis. To the extent that the SSR2- RT is unable to achieve consensus with respect to any recommendations, its reports and recommendations will reflect the variety and nature of the SSR2- RT views. Consensus will be based on the Operating Standards (when available). (See GNSO types of consensus as noted in Section 3.6 of the GNSO Guidelines for examples.)

As such, all decisions of the SSR2-RT should either be made at meetings, either face-to- face or via teleconference (teleconference or Adobe). On an exceptional basis where time is of the essence, the Co-Chairs may request input on a specific topic via email to the SSR2-RT email list, using commonly accepted practices (detailed explanation of the issue, required input, time to provide input, establishing a minimum number of responses, publication of results). Should a decision be made using email it will be re-confirmed at the following meeting of the SSR2-RT.

* **Leadership**

At its meeting on March 22 2017 the SSR2-RT selected by consensus Denise Michel, Emily Taylor and Eric Osterweil as Co-Chairs.

Responsibilities of the Co-Chairs include:

* + Remain neutral when serving as Co-Chair
  + Identify when speaking as an advocate
  + Maintain standards and focus on the aims of the Review Team as established in its Terms of Reference
  + Drive toward delivery of key milestones according to the Work Plan
  + Ensure effective communication between members and with broader community, board and staff
  + Set the agenda and run the meetings
  + Ensure that all meeting attendees get accurate, timely and clear information
  + Determine and identify the level of consensus within the team
  + Provide clarity on team decisions
  + Ensure decisions are acted upon
  + Build and develop teamwork
  + Facilitate RT reporting to the community to maintain accountability and transparency
* **Electronic Tools** 
  + The SSR2-RT will have a private email list (ssr2-review@icann.org) for review team members and support staff to use. All emails exchanged on this list will be [publicly archived](https://community.icann.org/display/SSR/Email+Archives). Email communication between the review team members regarding SSR2 work should be exchanged on this list.
  + There will be an [SSR2-RT wiki pag](https://community.icann.org/display/SSR/SSR2+Review)e where all relevant information about the review team and its work will be archived.
* **Outreach**

The SSR2-RT believes outreach to the ICANN community and beyond will be a key component of its approach given the global reach of the DNS.

As such the SSR2-RT will work with all communities to ensure they can interact directly with the RT or that the RT can attend key community events to present the work of the RT and hear input from those communities (subject to SSR2 budget requirements).

Here is an initial list of communities that the SSR2-RT may consult with:

ICANN Groups

-          Security Stability Advisory Committee (SSAC)

-          Governmental Advisory Committee (GAC)

-          GAC’s Public Safety Working Group (PSWG)

-          Root Server System Advisory Committee (RSSAC)

-          At-Large Advisory Committee (ALAC)

-          GNSO constituencies (see list on website)

-          Country Code Names Supporting Organization (ccNSO)

-          Address Supporting Organization (ASO)

-          Board

-          Board Technical Experts Group (TEG)

SSR1 Review Team

IETF

IAB

W3C

Regional Internet Registries (RIRs)

-          African Network Information Center (AFRINIC)

-          Asia-Pacific Network Information Centre (APNIC)

-          American Registry for Internet Numbers (ARIN)

-          Latin American and Caribbean Network Information Centre (LACNIC)

-          Réseaux IP Européens Network Coordination Centre (RIPE NCC)

Regional country code top-level domain organizations

-          African TLD Organization (AFTLD)

-          Council of European National TLD Registries (CENTR)

-          Asia Pacific TLD Organization (APTLD)

-          Latin American and Caribean TLD Organization (LACTLD)

Anti-Phishing Working Group (APWG)

Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG)

* **Meetings of the SSR2-RT**
  + Adobe Connect or telephone teleconferences
    - It is expected that the SSR2-RT will meet on a weekly schedule of rotating calls. The calls are between three times of day, roughly 8 hours apart to avoid imposing a participation burden to review team members from any one geographic region.
  + Face-to-face meetings

The current proposed schedule of face-to-face meetings is:

* + - ICANN58 – Copenhagen
    - ICANN DNS Symposium
    - ICANN59 – Johannesburg
    - ICANN60 Abu Dhabi
    - ICANN61 - TBD
    - ICANN62 – TBD
    - The SSR2-RT will review this schedule at the ICANN60 meeting.

All face-to-face meetings will allow for remote participation via Adobe Connect or a teleconference bridge.

* + Rules for meetings
    - Co-Chairs will publish a meeting agenda at least 24 hours in advance of each meeting. If an agenda has not been published by the Co-Chairs on the SSR2-RT email list at least 24 hours prior to a meeting, review team members should consider the meeting cancelled.
    - SSR2-RT weekly meetings are currently scheduled for a duration of 60 minutes.
    - It is expected that review team members who miss meetings will listen to the recordings of any meetings missed prior to attending the next meeting.
    - Holding part of a meeting Off the Record.
      * All SSR2-RT meetings will be recorded.
      * Any SSR2-RT member can request that the discussions be taken “off the record” at any point. If such a request is accepted by the Co-Chair leading the meeting, the meeting will go “off the record” while the SSR2-RT decides if the request should be approved.
      * When a meeting is taken “off the record,” the record shall reflect this decision as well as the underlying considerations that motivated such action. The Co-Chairs should ensure that the meeting becomes “on the record” again as soon as the topic requiring “off the record” is completed. Observers should be advised that the meeting has become “on the record” again.
      * If the SSR2-RT approves the request the meeting will remain “off the record” until the discussion of the issue approved to be “off the record” is completed.
      * If the SSR2-RT rejects the request the meeting will resume being “on the record”
      * RT members wishing to hold “off the record” discussions with the RT are encouraged to discuss this with a Co-Chair prior to the meeting. Should the Co-Chairs approve the request prior to the meeting this will allow for adequate preparations to be made ahead of time to facilitate going “off the record” during the meeting.
    - Decisions and action items from a meeting shall be published to the SSR2-RT wiki page and email distribution list within 24 hours of the meeting.
  + Transparency
    - All meetings of the RT will be announced on the SSR2 Wiki page at least 24 hours in advance of the meeting.
    - All meetings, including face-to-face meetings, of the RT will be recorded and made publicly available on the SSR2 Wiki page at <https://community.icann.org/pages/viewpage.action?pageId=64070219>
    - All meetings of the SSR2 will be open to observers via Adobe Connect or a teleconference bridge.
      * For Electronic meetings such as an Adobe Connect room meeting, a separate Adobe Connect room will be made available to observers which will carry the same feed as the RT Adobe Connect room but will not allow observers to interact with the RT.
      * Face-to-face meetings of the RT at an ICANN meeting will provide a separate Adobe Connect room for observers where a live feed to the RT meeting will be transmitted.
      * Face-to-face meetings of the RT not at an ICANN meeting will be broadcast in an Observer Adobe Connect room.
    - All Decisions and Actions items generated from an RT meeting will be published on the SSR2 Wiki.
    - To facilitate transparency and openness regarding ICANN's deliberations and operations, the review teams, or a subset thereof, shall have access to ICANN internal information and documents pursuant to the Confidential Disclosure Framework set forth in the Operating Standards (when available) (the "Confidential Disclosure Framework") and completion of ICANN’s Non-Disclosure Agreement (NDA).
    - The SSR2 [Fact Sheet](https://community.icann.org/display/SSR/Fact+Sheet) captures attendance of review team members, costs associated with professional services and travel to attend face-to-face meetings, and review milestones.  The SSR2 Fact Sheet is updated and posted quarterly.
* **Sub-teams of the SSR2-RT**
  + The SSR2-RT can create as many sub-teams as it deems necessary to complete its tasks through its standard decision process.
  + Sub-teams will be composed of SSR2-RT members and will have a clear scope, timeline, deliverables and leadership.
  + Sub-teams will operate per SSR2-RT rules and all sub-team requests will require SSR2-RT approval.
  + Sub-teams can arrange face-to-face meetings in conjunction with SSR2-RT face-to-face meetings.
  + All documents, reports and recommendations prepared by a sub-team will require SSR2-RT approval before being considered a product of the SSR2-RT.
  + The SSR2-RT may terminate any sub-group at any time.

**SSR2-RT Support**

* **Independent Experts**

*Section 4.6. SPECIFIC REVIEWS* (iv) - *“Review teams may also solicit and select independent experts to render advice as requested by the review team. ICANN shall pay the reasonable fees and expenses of such experts for each review contemplated by this Section 4.6 to the extent such fees and costs are consistent with the budget assigned for such review. Guidelines on how review teams are to work with and consider independent expert advice are specified in the Operating Standards.”*

The SSR2-RT currently has not identified any requirements for independent experts. Should the need arise the decision to request independent expert(s) will formally be approved by the SSR2-RT after considering input from ICANN Organization on budget implications and contracting requirements. If approved the Co-Chairs will communicate the request to ICANN so it can be processed per ICANN’s standard operating procedures.

* **Travel Support**

Members of the RT who request funding from ICANN to attend face-to-face meetings will receive it according ICANN’s standard travel policies and subject to the RT budget. Travel funding for RT members attending a face-to-face meeting being held in conjunction with and ICANN meeting will be for the duration of the ICANN meeting. RT members requiring funding for any face-to-face meeting should communicate this request to SSR2 support staff at least three months in advance of the meeting.

**Definitions**

An assessment of this type requires a common understanding of the key terms associated with the review:

* + Security - The capacity to protect and prevent misuse of Internet unique identifiers;
  + Stability – The capacity to ensure that the Identifier System operates as expected and that users of unique identifiers have confidence that the system operates as expected;
  + Resiliency – The capacity of the Identifier System to effectively withstand, tolerate and survive malicious attacks and other disruptive events without disruption or cessation of service.
  + Unique Identifiers - ICANN’s technical mission includes helping to coordinate, at the overall level, the allocation of the Internet’s system of unique identifiers: specifically, top-level domain names, blocks of Internet Protocol (IP) addresses and autonomous system (AS) numbers allocated to the Regional Internet Registries, and protocol parameters as directed by the IETF
  + physical security (TBD)
  + network security (TBD)
  + interoperable security processes (TBD)
  + global interoperability of the systems and processes, both internal and external, that directly affect and/or are affected by the Internet's system of unique identifiers that ICANN coordinates (TBD)
  + appropriate security contingency planning framework for the Internet's system of unique identifiers (TBD)
  + Others?

**Focus of the SSR2 – Scope of Work -**

(This is for the RT to draft and confirm. To assist in this we are providing the information that was captured on the 15 March brainstorming session)

From the requirement in the Bylaws:

*“(iii): The SSR Review Team shall also assess the extent to which ICANN has successfully implemented its security efforts, the effectiveness of the security efforts to deal with actual and potential challenges and threats to the security and stability of the DNS, and the extent to which the security efforts are sufficiently robust to meet future challenges and threats to the security, stability and resiliency of the DNS, consistent with ICANN’s Mission.”*

* What are ICANN’s security efforts and procedures? How does ICANN measure their effectiveness (what are the benchmarks/good practices/KPIs)?
* How effective is ICANN risk management?
* DNS abuse: Study the DNS abuse lifecycle and evaluate DNS abuse threat mitigation measures
* What are the changes to SSR with the IANA transition?
* What are actual/potential future challenges and threats?
* Explore forecasting research on Internet capacity and performance

*“(iv): The SSR Review Team shall also assess the extent to which prior SSR Review recommendations have been implemented and the extent to which implementation of such recommendations has resulted in the intended effect.”*

* Review of SSR1 recommendations:
  + Have they been implemented?
  + Impacts/results of implementation?
  + Which are still critical, post-transition?

*(ii)(A): May assess the “security, operational stability and resiliency matters, both physical and network, relating to the coordination of the Internet’s system of unique identifiers”*

* Define/clarify key terms:
  + Security; stability; resiliency; unique identifiers; physical security; network security; interoperable security processes
* Overview of procedures:
  + Unique identifiers
  + Interoperable security processes
  + Disaster and operational recovery
  + Risk management

*(ii)(B): May assess “conformance with appropriate security contingency planning framework for the Internet’s system of unique identifiers”*

* What is the appropriate security planning framework?
* What is the impact of moving the IANA services to PTI?
* What contingency planning has taken place as a result of CWG/CCWG?
* What measures are taken to ensure relevance and applicability of the contingency plan?

*(ii)(C): May assess “maintaining clear and globally interoperable security processes for those portions of the Internet’s system of unique identifiers that ICANN coordinates”.*

* How does ICANN compliance impact SSR?
* gTLD, ccTLD abuse
* How effective is ICANN’s coordination with IETF, others?

**Timeline**

* August-September 2017: Assemble findings and potential recommendations
* November 2017: Socialize draft recommendations with community
* January 2018: Publish draft report for public comment
* March-April 2018: Review input received and incorporate as appropriate
* June 2018: Send final report to ICANN Board
* June 2018: Socialize final recommendations with community