

At-Large Workspace: Second Security, Stability, and Resiliency (SSR2) Review Team Draft Report

Public Comment Close	Statement Name	Status	Assignee (s)	Call for Comments Open	Call for Comments Close	Vote Open	Vote Close	Date of Submission	Staff Contact and Email	Statement Number
20 March 2020	Second Security, Stability, and Resiliency (SSR2) Review Team Draft Report	ADOPTED 13Y, 0N, 0A	Jonathan Zuck Alan Greenberg	26 February 2020	19 March 2020	20 March 2020	24 March 2020	20 March 2020	Jennifer Bryce jennifer.bryce@ican.n.org	AL-ALAC-ST-0320-02-01-EN

Hide the information below, please click [here](#) >>

Brief Overview

Purpose: This Public Comment proceeding is on behalf of the second Security, Stability, and Resiliency (SSR2) Review Team. The Security, Stability, and Resiliency Review is mandated by ICANN's Bylaws ([Article 4, Section 4.6\(c\)](#)) to review "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."

Current Status: The SSR2 Review Team seeks to solicit input on its [draft report](#).

Next Steps: The SSR2 Review Team will carefully consider comments received and amend the report as it deems appropriate and in the public interest before submitting its final report to the Board. The final report will be published for Public Comment in advance of the Board's consideration.

Section I: Description and Explanation

This Public Comment proceeding is on behalf of the second Security, Stability, and Resiliency (SSR2) Review Team who seeks to solicit input on its [draft report](#). The report contains findings and recommendations in four key areas:

- Implementation and impact of recommendations from the [first SSR review](#).
- Key stability issues within ICANN.
- Security, stability, and resilience of the Domain Name System (DNS).
- Future challenges.

Section II: Background

The Security, Stability, and Resiliency Review is mandated by ICANN's Bylaws ([Article 4, Section 4.6\(c\)](#)) to review "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."

Per the [Bylaws](#), the issues that the review team for the SSR Review ("SSR Review Team") may assess are the following:

(A) security, operational stability and resiliency matters, both physical and network, relating to the coordination of the Internet's system of unique identifiers;

(B) conformance with appropriate security contingency planning framework for the Internet's system of unique identifiers; and

(C) 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.

Section III: Relevant Resources

- Second Security, Stability, and Resiliency (SSR2) Review Team [Draft Report](#)

Section IV: Additional Information

- SSR2 Review Team wiki space: <https://community.icann.org/x/AE6AAw>
- Security, Stability, and Resiliency Review page on [icann.org](#): <https://www.icann.org/resources/reviews/specific-reviews/ssr>
- Final Report of the first Security, Stability, and Resiliency of the DNS Review Team (SSR1): <https://www.icann.org/en/system/files/files/final-report-20jun12-en.pdf>
- SSR1 Review implementation wiki page: <https://community.icann.org/x/tYdCAw>

Section V: Reports

The final version to be submitted, if the draft is ratified, will be placed here by upon completion of the vote.



AL-ALAC-ST-032...0-02-01-EN.pdf

FINAL DRAFT VERSION TO BE VOTED UPON BY THE ALAC

The final draft version to be voted upon by the ALAC will be placed here before the vote is to begin.



AL-ALAC-ST-032...0-02-00-EN.pdf

DRAFT SUBMITTED FOR DISCUSSION

The first draft submitted will be placed here before the call for comments begins. The Draft should be preceded by the name of the person submitting the draft and the date/time. If, during the discussion, the draft is revised, the older version(S) should be left in place and the new version along with a header line identifying the drafter and date/time should be placed above the older version(s), separated by a Horizontal Rule (available + Insert More Content control).

Draft submitted by Alan Greenberg and Jonathan Zuck, 25 February 2020, 16:20 UTC

Minor correction (confirming reference to CCT Review) and correcting a typo, 26 February 2020.

New text added in response to comments, shown in BLUE, added by Alan Greenberg, 19 March 2020, 20:48 UTC.

The ALAC appreciates the opportunity to comment on the Second Security, Stability, and Resiliency (SSR2) Review Team Draft Report.

Ensuring the security, stability and resiliency of the DNS is arguably ICANN's single most important role.

SSR1 issued 28 recommendations. The ICANN Org reports indicated the Board judged all to be relevant and implementable and that all were fully implemented. The SSR2 analysis was that of the 28 recommendations, 2 were not implemented at all, 26 were partially implemented and none fully implemented. Of these 27 of the 28 were found to still be relevant. That is an astounding analysis 8 years after the acceptance of the SSR1 recommendations.

The ALAC has a particular interest in the recommendations related to domain name abuse, and notes that several of the recommendations overlap with and complement those issued by the RDS-WHOIS2-RT and the CCT RT.

The ALAC also notes that in the opinion of the SSR2 RT, many of the recommendations are deemed to be of high priority. Given the current interest in ICANN of prioritizing activities with the implicit effect of not addressing those lower on the list, this could lead to not addressing issues critical to the SSR of the DNS. DNS Security, stability and resiliency is not something that we can afford to ignore. The lead item in ICANN's Strategic Plan is **"Strengthen the security of the Domain Name System and the DNS Root Server System."** This must be taken into account when allocating resources and we trust that this will be taken into account when the Board works with the RT Implementation Shepherds on deciding how to prioritize the recommendation implementation.

The ALAC has a particular focus on and interest in DNS Abuse. To address this may require contractual changes to facilitate Contractual Compliance action. Such changes require either negotiations with the contracted parties or a PDP. A PDP will take considerable time and the ALAC does not advocate such a path, but rather it is time for ICANN Org and specifically Contractual Compliance to meet with those contracted parties who have shown an interest in DNS Abuse mitigation, and come to an agreement on needed contractual changes, factoring in not only penalties but any incentives that can be reasonably provided to encourage compliance.

Given the potential for rejection or deferral of the large number of high priority items, the ALAC encourages the review team to strengthen the justification on the high priority items.

Summary:

We are living in a world where many parties seem to have an interest in destabilizing critical infrastructure and the Internet in particular. The fact that our systems have been sufficiently robust in the past is not an indication that this is sustainable moving forward. ICANN needs to take seriously the need to professionally and rigorously ensure the SSR of its DNS operations. In particular, known vulnerabilities need to be corrected with the utmost haste.