ICANN Specific Reviews - Second Security, Stability and Resiliency of the DNS Review (SSR2) Recommendation 10.1 - Implementation Documentation

Published on 9 June 2023

SSR2 Final Report
https://www.icann.org/en/system/files/files/ssr2-review-team-final-report-25jan21-en.pdf

Board resolution on SSR2 Final Report
https://www.icann.org/resources/board-material/resolutions-2021-07-22-en#2.a

- Recommendation submitted: January 2021
- Recommendation approved: July 2021
- Implementation completed: May 2023

See https://community.icann.org/display/SSR/Implementation for more information on SSR2 implementation.

SSR2 Recommendation 10.1

ICANN org should post a web page that includes their working definition of DNS abuse, i.e., what it uses for projects, documents, and contracts. The definition should explicitly note what types of security threats ICANN org currently considers within its remit to address through contractual and compliance mechanisms, as well as those ICANN org understands to be outside its remit. If ICANN org uses other similar terminology -- e.g., security threat, malicious conduct -- ICANN org should include both its working definition of those terms and precisely how ICANN org is distinguishing those terms from DNS abuse. This page should include links to excerpts of all current abuse-related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse. ICANN org should update this page annually, date the latest version, and link to older versions with associated dates of publication.

Board Action on SSR2 Recommendation 4.1

To the extent that this recommendation is intended to enhance transparency, accountability, and clarity of ICANN org's work on Domain Name System (DNS) security threat mitigation through its existing contractual and compliance mechanisms, and thereby facilitate ongoing community discussions around definitions of DNS security threats, the Board approves this recommendation subject to prioritization, risk assessment and mitigation, costing and other implementation considerations. The Board notes that these considerations may be particularly important as definitions, procedures and protocols may evolve over time. In this regard, the Board understands that it may be appropriate for ICANN org to consider certain aspects of implementation as part of the work of ICANN org's Information Transparency Initiative (ITI).

Final Implementation Report

ICANN org has enhanced its focal webpage for DNS abuse which can be found at icann.org/dnsabuse. The webpage content will undergo annual review with ongoing maintenance and updates as required.

ICANN org has clearly denoted on this webpage the five broad categories of harmful activity that are consistent with ICANN's remit as defined by the ICANN Bylaws, which together comprise the current working definition for DNS abuse that ICANN utilizes in its contracts, projects and documents.

To address the request to define terminologies used, ICANN org has included hyperlinks of key terms to the ICANN acronyms page, icann.org/en/icann-acronyms-and-terms, and will regularly review and expand upon these as required.

ICANN org has also enhanced the webpage by adding a section on 'Enforcing Contractual Obligations with Registries and Registrars' in order to address the recommendation to provide "links to excerpts of all current abuse-related obligations in contracts with contracted parties, including any procedures and protocols for responding to abuse".

Lastly, ICANN Org has provided a notation corresponding to the date in which the page was most recently updated, and included an archive of older versions of the page, which will be updated on an annual basis.

Rationale

This recommendation is complete at the time of evaluation and implementation, and ICANN org will continue to update this webpage, as and when necessary, given the evolutionary nature of DNS abuse.

The topic of DNS abuse has been and continues to be widely discussed and debated within the ICANN community. The topic has the attention of nearly all of the SO/ACs within the gTLD space. The community's approach and response to DNS security threats is evolving in light of the threat landscape, and ICANN org will continue to monitor and evolve this webpage as required.

Timeline

Expected implementation date: June 2023
Final implementation date: May 2023

Milestones

8 May 2023 - The requested content updates were incorporated into the icann.org/dnsabuse webpage. Content reviews and corresponding website updates will be conducted, at the minimum, on an annual basis.