EN

AL/ALAC/ST/0412/2
ORIGINAL: English
DATE: 15 Apr 2012
STATUS: Final

AT-LARGE ADVISORY COMMITTEE

ALAC Statement on the
Security, Stability & Resiliency of the DNS Review Team (SSR RT) - Draft Report

Introduction

By the Staff of ICANN

Julie Hammer, At-Large Advisory Committee (ALAC) SSAC Liaison, originally composed this Statement, with assistance by Salanieta T. Tamanikaiwaimaro, ALAC Member from the Asian, Australasian and Pacific Islands Regional At-Large Organization (APRALO).

On 3 April 2012, a draft of the Statement was posted on the *At-Large Security, Stability & Resiliency of the DNS Review Team (SSR RT) - Draft Report Workspace*. On that same day, Olivier Crépin-Leblond, Chair of the ALAC, requested At-Large Staff to send a three-day call for comments on the draft Statement to all At-Large members via the ALAC-Announce Mailing List.

On 9 April 2012, the Chair of the ALAC requested that Staff open a five-day ALAC ratification vote on the Statement.

On 15 April 2012, At-Large Staff confirmed that the online vote resulted in the ALAC endorsing the Statement with 12 votes in favor, 0 votes against, and 0 abstentions. You may review the result independently under: https://www.bigpulse.com/pollresults?code=2938UjMLPSvMQ3f9FmZ54q8z.

[End of Introduction]

The original version of this document is the English text available at http://www.atlarge.icann.org/correspondence. Where a difference of interpretation exists or is perceived to exist between a non-English edition of this document and the original text, the original shall prevail.

ALAC Statement on the Security, Stability & Resiliency of the DNS Review Team (SSR RT) - Draft Report

The ALAC acknowledges the comprehensive work done by the Stability, Security and Resiliency of the DNS Review Team (SSR-RT) in analyzing the extent to which ICANN is fulfilling its commitment to enhance operational stability, reliability, resiliency, security and global interoperability of the Domain Name System ("DNS"). The ALAC compliments the Review Team on the preparation of this Public Discussion Draft Report and welcomes the opportunity to comment on it and its recommendations.

The ALAC supports all 28 recommendations in the Draft Report and in particular makes the following observations:

- Recommendations 1-8, 9, 13, 14, 16-22 and 24 are all sensible and worthwhile 'housekeeping' initiatives which, when implemented, will demonstrate that ICANN pursues a 'best practice approach'.

- Recommendations 10-12 and 22 will directly contribute to improved metrics for promoting consumer confidence and trust, while Recommendations 17-21 will also contribute in a more subjective indirect way. These recommendations will prove beneficial to the future Review Team which is to be set up in accordance with Para 9.3 of the Affirmation of Commitments to examine the extent to which the introduction or expansion of gTLDs has promoted competition, consumer trust and consumer choice.

- Recommendations 9, 13, 15, 23 and 25-28 are likely to be informed and assisted by the analysis and outcomes of the Joint DNS Security and Stability Analysis Working Group (DSSA-WG).

- The relationship between Recommendations 7, 8, and 16-21, which discuss the evolution of and improvement of processes surrounding the SSR Framework, and Recommendations 25-27, which relate to the role and activities of the Board DNS Risk Management Framework Working Group, is not clear. The ALAC queries whether the outcomes of work undertaken by the latter (the Board Working Group) are intended to guide the evolution of the SSR Framework in the future. In any case, the ALAC agrees that ICANN needs to expedite the creation and publication of a formal and comprehensive DNS risk management framework and would be keen to input to that process.

Noting the scope of the SSR-RT task and taking into account that the Draft Report is necessarily based on a desktop review, the ALAC is cognizant that it is not a formal security audit at the technical operations level. However, the ALAC recommends that ICANN give consideration to undergoing a formal security audit through assessing the risks from a critical information infrastructure protection standpoint.