EN

AL/ALAC/ST/0411/4
ORIGINAL: English
DATE: 11 April 2011
STATUS: FINALRev1

AT-LARGE ADVISORY COMMITTEE

Statement of the ALAC on the Public Call by the Stability, Security, and Resilience of the DNS Review Team (SSR-RT)

Introduction

By the Staff of ICANN

Patrick Vande Walle, At-Large community liaison to the SSAC, originally composed this statement.

A wiki workspace on the ALAC Statement on the Public Call by the Stability, Security, and Resilience of the DNS Review Team (SSR-RT) was posted on 29 March 2011. On 4 April 2011, a call for comments was sent to the ALAC-Announce, Technical Issues Working Group and regional At-Large mailing lists.

After a lively discussion on the lists, Patrick Vande Walle, with assistance by Lutz Donnerhacke, prepared a second version on 6 April 2011 which incorporated comments received.

On 31 March 2011, Olivier Crépin-Leblond, Chairman of the ALAC, requested the At-Large Staff to begin a five day ALAC vote on this statement starting 6 April 2011.

On 6 April 2011, the enclosed statement was submitted to the public comment for this issue, the relevant staff person, and the Board Secretary, with a note saying that the document was currently undergoing ALAC ratification.

On 8 April 2011, several comments were posted on the At-Large mailing lists following the filing of the second version of this ALAC Statement. Based on input from these comments, the ALAC Executive Committee added an Addendum which modified the consensus response to Question 4 to more broadly represent the diversity of the At-Large community.

On 11 April 2011, the ALAC began a five day vote on the third version (the present document), consisting of the ALAC Statement with the Addendum. This statement was sent to the staff person responsible for this issue and the Board Secretary, with a note saying that this document was currently undergoing the ALAC ratification process.

[End of Introduction]

The original version of this document is the English text available at 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.

Statement of the ALAC on the
Public Call by the Stability, Security, and Resilience of the DNS Review Team (SSR-RT)

The ALAC would like to commend the work undertaken by the Stability, Security and Resilience of the DNS Review Team and extends its thanks to the Team for its questions.

Some questions in the present document are listed but remain unanswered. They are kept for the purpose of completeness, and no answer is supplied in this document because the diverse At-Large input did not reach consensus.

Questions and request for input from the community based on the SSR-RT

1. Existing analysis of the impact of ICANN's responsibilities, as stated in the bylaws and related documents, on the Stability, Security, and Resilience of the DNS.

The fairly frequent recourse to "Stability, Security, and Resilience" is currently lacking definition, as a policy construct, and as a phenomenon sufficiently understood to support measurement.

2. Opinions on the limitations of the scope of ICANN's responsibilities, as stated in the bylaws and related documents, on the Stability, Security, and Resilience of the DNS.

We believe that the current limitations in scope are adequate. However, in order to prevent confusion, it should be stated that the WHOIS issue is not a stability, security and resilience aspect of the DNS. Both issues are technically independent and unrelated.

While we certainly approve ICANN's decision to focus on the deployment of DNSSEC on a global scale, we point out that it will only become effective and useful for Internet users once this will be adopted and implemented by major TLDs, as well as registrars and registrants. Having signed the root does not mean the work is done. A huge awareness campaign is still needed to convince registrars, registrants, ISPs, CPE manufacturers and others to actually offer support for DNSSEC.

3. Recent opinion on the DNS CERT proposal and on the need to coordinate/support detection and management of attacks/incidents to DNS.

While the DNS CERT proposal is an interesting one that should be further examined, we believe it is outside ICANN's mandate. Further, this could position ICANN as a judge and party on some issues. The community would be better served by an independent organization running the CERT.

4. Experiences, difficulties, unexpected advantages, and lessons learned in the implementation of DNSSEC.

Recent events, like the one that happened to .fr a few weeks ago, due to a software bug, seem to demonstrate the infrastructure may not be ready yet for the full, ubiquitous deployment of DNSSEC. Relaxing the pressure for the deployment of DNSSEC and proceeding carefully would allow all operators in the DNS chain to gain additional experience and mitigate the risks. This includes the new gTLD program, where registries and their backend providers are mandated to deploy DNSSEC from day one. Rather, DNSSEC signing should be advised only when the utility of zone signing and key management justifies the cost, as with all other engineering choices.

5. Sources of risk analysis for the DNS, as well as contingency planning, business continuity planning (BCP) and related work for the DNS.

6. Original solutions proposed to increase the Stability, Security, and Resilience of the DNS at the protocol level, including the design of the Root Server system.

While we believe the current system of hierarchical DNS works relatively well from a technical point of view, we think that one of the roles of ICANN would be to encourage, help and possibly fund research that would address the challenges and needs of on future naming systems[1].

7. Processes used by DNS users and operators to guarantee that the Risk Analysis related to the DNS is comprehensive and updated.

8. Analysis of the relationships of ICANN with “contracted parties” (registries and registrars) as well as others (ccTLDs not bound contractually to ICANN, Root Server Operators, etc.).

Among the non-contracted parties, one should mention domain name resellers and WHOIS proxy/privacy providers. Those are unaccountable to ICANN, and have been involved in many issues in the past. One suggestion from the At-Large would be to have a clear accreditation mechanism for these and, of course, to include provisions in the RAA to prevent registrars from working with unaccredited resellers or proxy providers.

ICANN should continue its current successful approach to obtain formal MoUs with ccTLDs. These exchanges of letters are a way to formalize each party's responsibilities in the stability of the DNS.

9. Involvement, present or possible, of non-ICANN entities in the design, implementation, operation, and evolution of the DNS, in its potential impact on the Stability, Security, and Resilience of the DNS.

There is a need to reinforce the link with the IETF community, including having clear agendas and timelines for features and changes in the DNS protocols, based on the operators and users experience.

[1] For example, having multiple registries managing domains under the same TLD. Such proposals have been floating around for a long time. See, for example, the original proposal for the SRS protocol at ftp://ftp.cuhk.edu.hk/pub/doc/ripe/ietf/98dec/drp-minutes-98dec.txt, or academic research on alternative name resolution systems like CoDoNS at http://www.cs.cornell.edu/people/egs/beehive/codons.php.

10. Solutions/Proposals on Root Server Governance, including transparency, accountability, security/performance measurements, policies, accessibility and the opportunity to have more RS operators

11. Studies or informed opinion related to large-scale risks that can alter the environment of the DNS, and indicators, metrics or harbingers of such risks, including models/frameworks to measure Security, Stability and Resilience of the DNS as a system.

Addendum:

Several late comments have come to light since the filing of the first version of this ALAC Statement. Based on input from these comments we have modified our consensus response to Question 4 to more broadly represent the diversity of our community:

Recent events, like the one that happened to .fr a few weeks ago, due to a software bug, seem to demonstrate the infrastructure may not be ready yet for the full, ubiquitous deployment of DNSSEC.

Some of our members believe that relaxing the pressure for the deployment of DNSSEC and proceeding carefully would allow all operators in the DNS chain to gain additional experience and mitigate the risks.

This would include the new gTLD program, where registries and their backend providers are mandated to deploy DNSSEC from day one.

Others believe that the cost and complexity of deploying DNSSEC is likely to decrease with time and therefore look forward to making DNSSEC mandatory for all new gTLDs. As a result, small new registries from developing countries are not likely to be affected as much by higher costs as initially thought.

The long-term benefits of DNSSEC implementation are likely to outweigh its short term trade-offs and the ALAC would therefore cautiously warrant the full deployment of DNSSEC for all new gTLDs, provided smaller sized applicants are allowed a period of adaptation for them to be able to sign their zone.