

DNS Security and Stability Analysis Working Group

Mr. Olivier Crepin-leBlond, chair of ALAC
Mr. Byron Holland, chair of the ccNSO
Mr. Jonathan Robinson, chair of the GNSO
Mr. John Curran, chair of the NRO

Cc:

Mr. Patrik Fältström, chair of SSAC
Mr. Mason Cole, co-chair GNSO
Mr. Wolf-Ulrich Knoben, co-chair GNSO

9 November 2013

Topic: Recommendation to accept Final Report and closure of the working group

Dear Chairs,

We are pleased to provide you with the attached Final Report and the work products contained in it.

The DSSA recommends the acceptance of the Final Report. It further recommends that the Final Report be disseminated to the membership of each of the participating Supporting Organizations and Advisory Committee's for their consideration. The DSSA believes that there is substantial value in the Report as it outlines a shared mechanism to rapidly collect and consolidate risk-assessment scenarios across a broad and diverse group of interested stakeholders.

It has been a long journey since Nairobi 2010, time consuming and, sometimes, arduous. We wish to thank all members of the working group, outside experts and staff for their participation, advice, encouragement and patience shown.

Submitted on behalf of the DSSA

Olivier Crepin-leBlond (ALAC)

Jim Galvin (SSAC)

Mark Kusters (NRO)

Mike O'Connor (GNSO)

Joerg Schweiger (ccNSO)

Co-chairs

Background

According to its charter the joint DNS Security and Stability Analysis working group was established by the participating Supporting Organisations and Advisory Committees ALAC, ccNSO, GNSO and NRO to better understand the security and stability of the global domain name system (DNS).

The objective of the DSSA-WG is to draw upon the collective expertise of the participating SOs and ACs, solicit expert input and advice and report to the respective participating SOs and ACs on:

- A. The actual level, frequency and severity of threats to the DNS;
- B. The current efforts and activities to mitigate these threats to the DNS; and
- C. The gaps (if any) in the current security response to DNS issues.

It was further agreed that the DSSA-WG should limit its activities to considering issues at the root and top level domains within the framework of ICANN's coordinating role in managing Internet naming and numbering resources as stated in its Mission in its Bylaws.

After consultation with chartering organizations, the DSSA broke its work into two phases. The first phase, which was concluded in October 2012, included the following:

- Clarifying definitional issues of the DNS system to be reviewed, and the organizational and functional scope of the effort
- Selection and tailoring of a risk-assessment methodology to structure the activities.
- Developed and tested mechanisms to rapidly collect and consolidate risk-assessment scenarios across a broad and diverse group of interested participants.
- Use an "alpha-test" of those systems to develop the high-level risk-scenarios, which will serve as the starting point for the activities in Phase 2.

In the second phase the WG planned to:

- Conduct a proof of concept analysis based on the Phase 1 methodology to refine and streamline the methodology, focusing on one broad risk-scenario topic
- Roll the methodology out to progressively broader groups of participants to introduce the methodology to the community
- Improve the process and tools on the way to completing the assessment.

Overview of major events

At the time the DSSA published its draft Report Phase 1 (August 2012), the DSSA noted and informed the participating SO's and AC's that in order to reflect the changed environment and working method, the charter of the DSSA would need to be updated to reflect these changes.

In October 2011 the ICANN Board of Directors established the Board DNS Risk Management Framework Working Group (DNS RMF WG), with the objective to oversee the development of a risk management framework and system for the DNS as it pertains to ICANN's role as defined in the ICANN Bylaws.

After the ICANN Board of Directors adopted the charter of its DNS RMF WG (March 2012), the DSSA noted potential overlap between its work and that conducted under auspices of the aforementioned DNS RMF WG. To mitigate the risk of potential divergence in approach and methods between the two groups, the DSSA WG deferred further activities in August 2012, awaiting the outcome of the study commissioned by the DNS RMF WG . This decision was made in accordance with the DSSA charter, which states that the DSSA should coordinate with other initiatives with respect to the DSSA-WG objectives, and do whatever it deems relevant and necessary to achieve its objectives.

The DSSA notes that as a result of the pause of 1 year, the interest and participation rate in the activities of the WG decreased substantially.

Options

Under these circumstances, the WG has identified two options as to how to proceed:

- The ALAC, ccNSO, GNSO and NRO consider the Final Report Phase 1 as the Final Report as envisioned in the charter of the DSSA WG, section 2.4. This will result in closure of the WG.
- The ALAC, ccNSO, GNSO and NRO all decide that DSSA WG should continue its work. In that case, the DSSA believes that the current charter needs to be updated, as it does not reflect either (a) the current environment, nor (b) the working method and scope of activities of the DSSA as agreed with the SO's and AC's.

Recommendation and Rationale

The DSSA recommends the acceptance of the Final Report. It further recommends that the Final Report be disseminated to the membership of each of the participating SO's

and AC's for their consideration. The DSSA believes that there is substantial value in the Phase 1 Report as it outlines a shared mechanism to rapidly collect and consolidate risk-assessment scenarios across a broad and diverse group of interested stakeholders.

Considerations regarding the second option. The DSSA believes that the Phase 2 effort, if considered, should be undertaken by a new set of volunteers with additional expertise. Volunteers will need to be aware that Phase 2 will take a considerable effort to conclude (both in intensity and duration of the work). The DSSA notes that maintaining the continuity of the work with this team will be very difficult as most of the few remaining Phase 1 volunteers lack the specific knowledge needed, and the majority of original volunteers have moved on to other activities.

It is anticipated that the DNS Risk Management Framework developed under auspices of the DNS RMF WG will be transitioned to ICANN staff for implementation and the Board Risk Committee will handle ongoing oversight of the DNS Risk Management Framework. Based on an analysis of the DNS RMF WG report the DSSA foresees a high risk that if the DSSA were to continue, two diverging initiatives and methodologies will be developed under the ICANN umbrella. The primary reason for this conclusion is our belief that the report indicates the use of a proprietary methodology, while the DSSA work has from its onset been based on an "open source" method.

In order to decrease the risk of divergence, members of the DSSA working on Phase 2, would not only need to be focused on the activities of the DSSA itself, but they also would need to closely monitor and coordinate with the parallel activities under auspices of ICANN. Given our experience to date, this will further increase the risk of "burn-out" of volunteers.

Finally, once again we wish to thank all who helped with this effort, volunteers and staff alike.