Draft - DNS Risk Management Framework WG Charter

A. Purpose

The ICANN Board has asked (2011.03.18.07) the Board Governance Committee to recommend to the Board a working group 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.

The purpose of the **DNS Risk Management Framework WG** (DNRMF WG) is to develop goals and milestones towards the implementation of a DNS security risk management framework for Internet naming and address allocation services, accompanied by defined timelines and budgetary implications. Further, the DNRMF WG will oversee the creation of an initial assessment which will serve as a baseline for the task.

To develop a security risk management framework for Internet naming and, as relevant, address allocation services that defines the key focus areas, and identifies where the responsibilities for each area lie. The committee will focus on the operational considerations of critical naming infrastructure.

B. Scope

The scope of the DNRMF WG is limited to providing oversight towards the definition of goals, milestones and reports for a newly created DNS security framework. In addition, the DNRMF WG will oversee the creation of a baseline assessment and the integration of this function into regular ICANN staff activity.

In considering its task, the DNRMF WG should take into account and be guided by:

- The overarching requirement to preserve the security and stability of the DNS;
- ICANN's limited role with regard to security and stability;
- Input and advice from the technical community in respect to the implementation of the framework;
- the relevant documents that have been produced by the SSAC.

If issues become apparent to the DNRMF WG that are outside of its scope, the DNRMF WG Chair should inform the Board of the issue so that it can be taken into account.

Upon completion of the work of the DNRMF WG, the ongoing oversight of the DNS security framework will be integrated into the scope of the Board Risk Committee.

C. Membership of the DNS Security Framework Working Group

The DNS Security Framework Working Group will have the following members:

Bill Graham*;
Ray Plzak;
Ram Mohan;
Suzanne Woolf;
Patrik Fältström [SSAC Chair];
Bill Woodcock [CEO, Packet Clearing House];
Roelof Meijer [CEO, SIDN]

* Bill Graham is the Chair of the DNRMF WG.

The following factors were considered while recommending WG members:
Risk management experience; Security & Stability knowledge/experience; gTLD and ccTLD registry operations experience; DNS operational experience; IP addressing experience; and government & public policy experience.

ICANN will provide adequate staff support to the DNRMF WG, including liaisons from the ICANN Security, IANA and root server operations teams.

D. DNS Security Framework WG Tasks

1. Goals, Milestones and Resource Impact

The DNRMF WG shall publish for Board review an initial set of goals and milestones for the development of the DNS Security Framework, including indications about financial and resource impacts.

2. Initial Assessment Report

At the end of the review period (in #1 above), the DNRMF WG shall task staff to prepare an initial assessment of the DNS Security risk management framework. This should take into consideration prior work on DNS security for Internet naming and address allocation services, including, but not limited to

- ICANN's annual Security, Stability and Resiliency Framework and Plans,
- Recommendations from the Affirmation Review Team on Security, Stability and Resiliency (if available), and
- Recommendations from the DNS Security and Stability Analysis Working Group

A public workshop to share information and seek inputs to the Initial Assessment Report will be held at the ICANN meeting in March 2012, and a public comments on the DNRMF WG final draft report will be held at the June meeting.

3. Integration into Staff Function

The DNRMF WG shall work with staff to ensure that the DNS Security Framework function is integrated into the normal operations of ICANN. This shall include consideration of the financial and resource impact of the addition of this function.

4. Board Consideration

The DNRMF WG shall present to the Board a proposal to execute the DNS Security Framework function in a reliable manner, including consideration of resources required to fulfill this function. Such a proposal is expected to be developed by staff, in consultation with the ICANN community for consideration by the DNRMF WG.

5. Oversight by Board Risk Committee

At the completion of its term, oversight of the DNS Security Framework function shall be transitioned from the DNRMF WG to the Board Risk Committee.

E. DNRMF WG Time Line*

Activity	Date	Closure
Publish Goals, Milestones	29 February 2012	23 March 2012
Scoping & Prelim. Resource Impact	10 March 2012	
Conduct Initial Assessment Workshop (Costa Rica)	12 March 2012 (TBC)	
Publish Initial Assessment Report	2 April	
Public Comment on Initial Assessment Report	2 April (begin)	18 May 2012
Plan for integration into ICANN staff activity	18 May 2012	1 June 2012
DNRMF WG Completes Work	15 June 2012	
DNRMF Outputs Workshop (Prague)	25 June 2012 (TBC)	
Board approval; Transition to Board Risk Committee	22 June 2012	29 June 2012

F. Background and References

In its final report published 29 January 2010 <http://www.icann.org/en/reviews/ssac/ssac-review-wg-final-report-29jan10-en.pdf> [PDF, 282 KB], the Security and Stability Advisory Committee (SSAC) recommended that task area one of the SSAC Charter (Section 2(2)(a)(1)

<http://www.icann.org/en/general/bylaws.htm#XI>) should be removed because it is out of scope of the activities of the SSAC.

On 12 March 2010, the Board received the SSAC final report and directed the Structural Improvements Committee (SIC) to identify actions necessary to address the recommendations within the report, at <http://www.icann.org/en/minutes/resolutions-12mar10-en.htm#1.6>.

The SIC, at its 14 October 2010 meeting, recommended that the Bylaws should be amended to achieve the recommendation of the Working Group on improvements to the SSAC by removing task area one and renumbering the other task areas.

On 18 March 2011, the Board approved the amendment to the Bylaws reflecting the removal of task area one from the SSAC Charter, which read "To develop a security framework for Internet naming and address allocation services that defines the key focus areas, and identifies where the responsibilities for each area lie. The committee shall focus on the operational considerations of critical naming infrastructure."

The ICANN Board desires that the work foreseen within task area should be performed by ICANN.

At the San Francisco Board Meeting, the Board resolved (2011.03.18.07):

The Board directs the Board Governance Committee to recommend to the Board a working group 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. The Board recommends that the BGC consider in its recommendation the inclusion of a member of the working group to come from the SSAC. The Board requests that the BGC submit its recommendation consideration at the Board meeting in Singapore in June 2011.

PRELIMINARY LIST OF RISKS (v. 28-02-12)

1. Develop a definition of "the DNS" and map the entities that are part of the environment for the purposes of this Working Group.

2. Looking broadly at DNS security and stability issues (within and beyond ICANN), what are the greatest risks in the current environment?
    a. which of those are within ICANN's span of control?
    b. for those outside ICANN's span of control, are there entities that should be alerted to those risks?

3. Business impact analysis (what are the services most essential to ICANN's business with regard to the security and stability of the DNS)

4. Risks analysis (what are the risks that threaten those services)

5. What measures need to be in place to control the (largest) risks on critical services.

6. Is the DNS software environment sufficiently robust to adequately deal with risks to the DNS?
    a. are there systemic risks to the DNS due to having a single predominant DNS software implementation?
    b. does the resource intensive nature of developing DNS software result in vulnerabilities? Are there other mechanisms that might address those challenges?
    c. are adequate procedures (e.g. documentation, security testing, change & release management, (external) code review) incorporated in the development of DNS software?

7. Systemic risks associated with the diversity and possible fragility of entities in the DNS, including non-ICANN accredited entities.
    a. registration vulnerability
    b. name service robustness
    c. compromise of personnel
    d. incompatibility of policies
    e. knowledge levels
    f. anti-abuse procedures (or lack thereof)
    g. international variation

8. DNSSEC Deployment
    a. risks from key management errors
    b. knowledge levels (at registries, registrars, and levels below)

9. IPv6 readiness (and IPv4 transition)

10. New gTLD operational capability
    a. is the current system of name servers able to handle anticipated growth of the Internet's naming system?