CONSULTATION PAPER

ICANN – DNS RISK ASSESSMENT

Purpose

The purpose of this document is to:

- Brief the ICANN Community on the approach used in an initial assessment of DNS risks; and
- Through a process of consultation at ICANN 50, receive feedback to help further refine the approach prior to subsequent rounds of engagement with the wider Community in a more broad-based assessment of DNS risks.

Background

In November 2013 at ICANN 48 in Buenos Aires, the ICANN Board adopted the ICANN DNS Risk Management Framework ("Framework") and in February 2014 a group of selected ICANN staff undertook an initial (limited scope) DNS risk assessment using the Framework.

The initial DNS risk assessment was intended to serve as a pilot, with a focus on features that would help ensure it remains durable (practical, dynamic and adaptable) and 'fit-for-purpose' given the evolutionary nature of the Internet and ICANN's multi-stakeholder model.

The results were presented to the ICANN Board Risk Committee at ICANN 49 in Singapore and comprised of:

- A DNS Risk Assessment report, similar in form and content to this consultation paper;
- An accompanying risk register articulating the risks initially identified; and
- An illustrated overview of the approach used in the form of a 'resilience model', expanded upon below.

Subsequent to ICANN 49, the risks were evaluated through an online survey involving the group of ICANN staff who undertook the initial risk identification. Feedback received was used to make further refinements to the approach.

DNS Risks - Scope

DNS Risks depend upon the perspective of the stakeholder. This assessment does not attempt any explicit definition of scope, but relies instead on stakeholders to form their own views suited to their individual circumstance and interest. The DNS risk universe (all possible permutations of DNS risks) is accordingly framed in broad terms through a combination 'asset' classes and 'Responsible Party(s)', illustratively described in in Figures 1 and 2 below.

Figure 1 illustrates the progression in thinking to define the scope of this DNS risk assessment from an initial stylised overview of the Internet, to ICANN's and the ICANN Community's areas of interest and finally the scope of the DNS Risk Assessment:

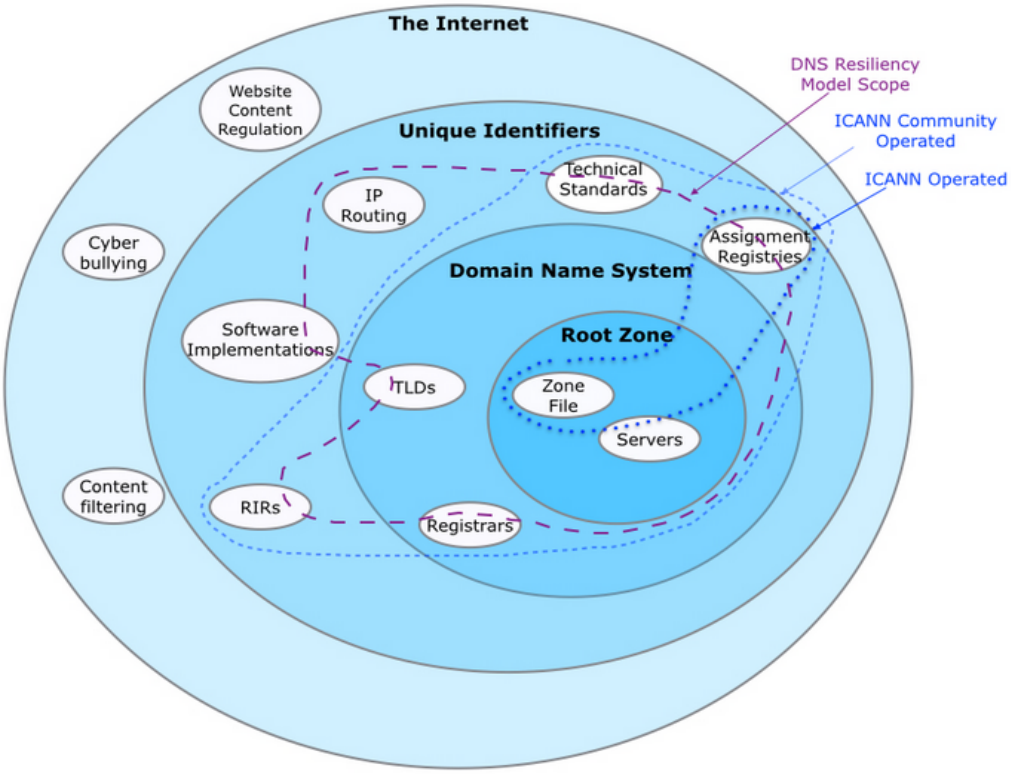

Figure 1: DNS Risks Scope – Asset View

(Provided for illustrative purposes. Not intended to provide an exhaustive scope of the risks.)

		RESPONSIBLE PARTIES (Illustrative only. Not exhaustive)				
ASSETS (Illustrative only. Not exhaustive)		**ICANN**	**TLD Managers**	**Governments**	**Companies**	**Etc.**
Root Servers	L - Root	X				
	A - Root			X		
	↓					
TLDs	.Typically large TLD		X			
(Size)	.Typically smaller TLDs		X			
	.gov		X	X		
	.ccTLD A		X			
	.ccTLD B		X			
	.Brand TLDs		X			
	.IDN TLDs		X	X		
	↓					

EACH INTERSECTION RATED ON SEVERITY

Figure 2: DNS Risks Scope – Asset / Responsible Parties Matrix

(Provided for illustrative purposes. Not intended to provide an exhaustive scope of the risks.)

The DNS Risk Assessment

The approach to the DNS risk assessment recognises that:

- The Internet and its (core) systems of unique identifiers constitute, in substance, an ecosystem, a system that adapts organically through time as a direct result of the interaction of many active participants benefiting from the mutual exchange of information;
- The success of the Domain Name System (and the Internet itself) is in large part due to the trust its users have placed in its:
    - *Availability* – meaning that a properly configured resolver that is connected to the Internet can resolve a name within a reasonable response time.
    - *Consistency* – a request to resolve a name on the Internet should return the same result wherever it is asked and whenever it is asked (subject to the DNS records not being changed in the meantime).
    - *Integrity* – DNS lookups will be an accurate reflection of the records in the zone files.

The core foundations of this trust are similarly reflected in user expectations regarding the *operational stability, reliability, security, and global interoperability of the Internet,* that lie at the heart of ICANN's mandate.

In this context the objective of risk assessments can be viewed as protecting DNS related assets and in turn stakeholder trust.

The approach adopted accordingly favours transparency with the ICANN community in developing and using a common approach, so as to encourage collective stakeholder interest in identifying and dealing with potential threats to the ecosystem and to stakeholder trust. In contrast, the alternative of *prescriptive* approaches appears increasingly less compelling in complex, evolutionary systems as, for example, the global financial crisis demonstrated.

A DNS Resilience Model

The *DNS Resilience Model* brings the above components together in a visual relational context as the schematic in Attachment 1. The Model provides examples of risks categorised into two groups: *systematic*, being those inherent in the aggregate internet domain and that cannot per se be avoided. These risks are in turn impacted by systemic amplifiers and attenuators[1]. I*diosyncratic* risks are those unique to a particular asset or Responsible Party. The ultimate objective and outcomes for undertaking risk management is shown at left.

The interrelationships between the components and the cause-and-effect chains between identified risks (as well as connections to any risk treatments and counter measures) are potentially complex but necessary to explore as the risk assessment process matures in future.

[1] Refer International Risk Governance Council (IRGC). http://www.irgc.org/

Consultation questions

Considering the *DNS Risk Assessment and DNS Resilience Model* above:

1. On the DNS Risk Assessment
   - Does the approach as described appear robust?
   - Is anything substantive missing? Is there additional substance that should be added?
   - In what ways could successive risk assessments be improved?
   - Do you foresee any unintended consequences of continuing to use this approach in future?
   - Any other comments?

2. On the Asset / Responsible Party(s) matrix
   - Does the conceptualisation of Asset classes make sense?
   - Does the conceptualisation of Responsible Party(s) categories make sense?
   - Is the allocation of Responsible Party(s) to asset classes (or vice-versa) appropriate and reasonable?
   - Is the matrix practically useful, assuming completed by Responsible Party(s) in relation to their specific context and purpose?

3. On the DNS Resilience Model
   - Is the role of the Model in supporting a risk assessment clear?
   - Where could improvements be made?
   - Are there, in your view, omissions or inconsistencies?
   - Any other comments?

4. General
   - Do you have any further comments or feedback?
   - What else, in your view, could or should be added to the risk assessment approach and / or Resilience Model to improve it and its usefulness to you and your organization?

Responses to consultation questions

We welcome your feedback, which can be provided by e-mail to Jack Khawaja at: jack.khawaja@icann.org

++++++++++++