The ICANN GNSO "Business Constituency"

# Review Team on the Security, Stability and Resiliency of the DNS

## *Set of Issues*

Status: FINAL
Version: 3.0
6 APR 2011

**Commercial & Business Users Constituency Submission**

**GNSO//CSG//BC**

# Submission:

The Security, Stability and Resiliency of the DNS Review Team (SSR RT) commenced its activities in October 2010 and held its first face-to-face meeting with the community in Cartagena last December. In Colombia, the SSR RT drafted and issued Terms of Reference, which will guide this Affirmation of Commitments (AoC) team throughout its exercise.

The Commercial Users & Business Constituency (BC) thanks the Board for initiating this Affirmation review of security, stability and resiliency. Moreover, we thank the Review Team members for volunteering several months of time and effort to conduct this review and prepare their reports and recommendations.

Business users rely on a stable and secure Internet and e-commerce experience, one that serves their users and customers on a global basis. Although ICANN is an independent non-profit corporation, its decisions directly impact a larger eco system that is extensively designed and financed by BC members, including communication service providers, ISPs, cable providers; application and content service providers, as well as domain portfolio managers, and the online commerce community.

The BC supports ICANN's continuing effort to improve SSR and believes that attention of this review should be focused on three areas of current concern:

1. Adequacy of measures to prevent DNS Abuse
2. Lack of Collaboration with Enterprise Community
3. Oversight and resources to ensure compliance obligations are enforced

ICANN's Bylaws require it "to ensure the stable and secure operation" of the DNS. Therefore, ICANN must view participation in coordinated, industry efforts to combat malicious DNS activity as absolutely essential to that mission.

Fraudulent WHOIS, manipulation of DNS records, and ICANN's failure to adequately enforce obligations of contracted parties continues to provide fertile ground for abuses that erode trust in e-commerce.

The BC is not advocating "mission creep" by ICANN. But we are encouraging ICANN to recognize that its mission requires timely enforcement of contracted party compliance obligations and collaborative support for enterprise efforts to combat persistent attacks that abuse DNS technologies.

The BC has strong concerns that ICANN's current SSR plans fail to adequately emphasize cooperation with the business community to protect e-commerce. The SSR plan also lacks a detailed description of how ICANN will focus on creating an effective compliance program.

Even if an adequate plan is introduced, the lack of an emphasis on improving compliance leaves doubt that any plan will be effective. ICANN continues to endorse a narrow view of its compliance obligations. This provides little assurance that ICANN will take the necessary action to enforce security standards. The current SSR proposal appears heavy with good intentions, but provides few substantive details or assurances of action that would persuade the BC that it would be effective.

The introduction of new gTLDs makes this a critically important moment for ICANN to develop a robust SSR plan that will protect e-commerce and promote security. This SSR Review is an excellent way to

describe shortfalls in current plans and compliance, and to recommend improvements that can be implemented before doubling or tripling the number of TLDs in use.

The SSR RT is soliciting input from the community on its suggested set of issues:

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.
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.
3. Recent opinion on the DNS CERT proposal and on the need to coordinate/support detection and management of attacks/incidents to DNS
4. Experiences, difficulties, unexpected advantages, and lessons learned in the implementation of DNSSEC.
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.
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.)
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.
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 resiliency of the DNS as a system.

Each of these issues is addressed below.

**1.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 lack of understanding and agreement of the scope and nature of ICANN's SSR role has been one of the most persistent problems in various recent policy-making discussions in this area. The HSTLD-AG is a good example of a working group that had a very difficult time with these issues and, as a result, arrived at a less-than-satisfactory outcome for almost all parties involved.

The BC strongly supports a rigorous analysis of this topic.

**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.**

DNS abuse is pervasive, costly to mitigate, and becoming increasingly complex. It is not "going away" and cannot be ignored.

Cybercriminals target BC members because they are seeking "high value" targets where there are significant users and financial resources. The BC members represent companies that are among the most popular by Internet users, the very public with whom ICANN has stated it shares a "mission of public trust". While BC members applaud the start of a dialogue on SSR, the scope of attacks against BC members creates urgency for specific and tangible assistance rather than the ambiguous "good intentions" found in the SSR plan. This is a security crisis for which ICANN can and should perform a significant role. The current SSR Plan fails to provide definitive and actionable steps that will allow ICANN to address the DNS abuse environment that allows for these cyber threats to become pervasive.

ICANN's ambiguous security plan is of even greater concern considering the critical period of expansion and change in the DNS. The introduction of new gTLDs may expand the environment and opportunities for online fraud beyond the current critical levels that have already been noted. While the BC supports a free market open to new gTLDs and does not advocate further unnecessary delay, it is critical that these security concerns be more carefully considered in any SSR plan. To fail to do so ignores a critical security threat that will likely exacerbate the existing harm to BC members. The SSR Plan states that ICANN "will continue to pursue implementation of measures to combat the potential for malicious conduct arising from the establishment of new gTLDs" yet the ICANN Board has stated that "the implementation work completed to date by the community and staff to address the mitigation of malicious conduct issue is sufficient to proceed to launch the first new gTLD application round." The proposed SSR Plan understates the implications of the introduction of new gTLD while simultaneously overstating the scope and anticipated efficacy of ICANN's efforts to mitigate these implications.

The SSR plan acknowledges "ICANN's role includes participating in activities with the broader Internet community to combat abuse of the unique identifier systems." The BC would like greater assurance from ICANN that the SSR plan will include a focus on mitigating the threats against the e-commerce community that are based on DNS abuse, reversing the compliance environment that fosters abuse, and clarifying that the scope of assistance will be adequate to include meaningful assistance to enterprise users being targeted by DNS based threats.

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

The DNS-CERT proposal was broadly perceived as top-down rather than bottom-up proposal that originated from within the ICANN staff. As such, it did not garner broad support in the community (both inside and outside of ICANN). The way this initiative was launched should be carefully reviewed and lessons-learned should be drawn from that analysis.

As with several other initiatives, DNS-CERT suffered from the lack of a clear, broadly agreed-upon, agreement as to what the appropriate scope and definition of ICANN's role when it comes to matters relating to SSR. Until that is worked out, any number of initiatives is likely to fail.

There is a broadly held view, which the BC supports, that ICANN needs to actively engage with the broader security community in several ways. This engagement ranges from very quick responses to emerging threats at the operational level to broad policy discussions that continue over a much longer period of time. Again, arriving at agreement on the nature and scope of this engagement should be a high priority.

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

A coordinated effort that includes the BC membership is necessary to effectively implement SSR policy. While the BC membership does not endorse the expansion of ICANN to manage a DNS CERT program, it does strongly advocate for the creation of an industry managed compliance and security coordination system that will ensure enforcement of SSR policy in the DNS. The largely successful implementation of DNSSEC provides a model for the security improvements that can be achieved by broad industry collaboration and effective implementation.

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

The security community has invested significant time to make recommendations on security improvements. During the last ICANN community meeting in San Francisco the law enforcement and technical security community gathered for a full day to discuss best practices and improvements for security in the DNS. The BC recommends that this group and other security experts be actively recruited to become part of ICANN working groups tasked with conducting DNS risk analyses. ICANN should incorporate the specific recommendations for threat risk analysis and design improvements that are recommended by such working groups.

**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.**

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

ICANN should continue to include the BC, law enforcement members, and the technical community in consultations aimed at developing pro-active and practical solutions to improving compliance enforcement. The BC strongly urges ICANN to firmly enforce contractual obligations in a timely manner. We commend the hiring of additional compliance staff but now also urge that this staff be empowered with the support and authority to enforce contractual obligations. The current narrow and restrictive approach to compliance enforcement is not only unnecessary but it harms the business community and cripples security efforts. The resources of ICANN staff must be applied to enforce contractual obligations and to aggressively oppose conduct that is noncompliant with contractual obligations.

ICANN should, at a minimum, continue to pursue efforts to define high security zone standards for domains requiring additional security. Large domain operators should also be provided an appropriately weighted voice for advancing security matters within ICANN. This should include input into open and fair negotiation of the registrar accreditation agreement. Registrant data must be mandated to be accurate, maintained securely, and available to mitigate abuse upon an appropriate request. ICANN should also clarify and strengthen existing mechanisms for input to compliance staff on rogue registrar/reseller problems and compliance violations that will be acted upon by staff.

**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.)**

**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.**

Given the BC's strong recommendation for industry collaboration on SSR development, it is concerning that ICANN has not sufficiently included key stakeholders such as enterprises and users in its security, stability, and resiliency initiatives. The SSR Plan further indicates that ICANN will continue to focus primarily on the contracted parties in such initiatives. Although the SSR Plan contains numerous references to 'core stakeholders," it is clear that ICANN considers gTLD registries and registrars, not users and enterprises, to be these core stakeholders. The key partners identified as the subjects of ICANN's global security outreach do not represent users and enterprises. ICANN must further engage users and enterprises in collaborative efforts to enhance security, stability and resiliency.

The sense of urgency to move forward with new gTLD expansion seems to have hampered ICANN's ability and/or desire to understand the stakeholder concerns around the security, stability, and resilience of the Internet. Commercial enterprises, government agencies, nonprofits, Internet startups, and consumers all depend upon the security of the Internet. ICANN has failed to provide specific examples of how security assistance will be implemented in its SSR proposal. This is especially concerning given that there has been so little collaboration with enterprises to design these mitigation programs. Any such programs, it is assumed, should be primarily designed to assist enterprises that are suffering the most targeted abuses, yet enterprises appear to be a secondary afterthought in the SSR proposal.

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

The BC membership is concerned that insufficient effort has been devoted to addressing concerns with enforcing contractual compliance, despite repeated concerns being raised during public comment. Vacant positions in critical ICANN security and compliance positions have only recently been filled and ICANN's endorsement of a tightly restrained enforcement policy continues to raise serious concerns about the effectiveness of any security plan. The effective oversight needed for a strong security program does not exist and without such, even the best SSR plan will fail.

To work effectively with stakeholders in addressing security and stability issues, ICANN needs to acknowledge the role that their policies play in the process, and they must be accountable for these policies. Too often, ICANN relies upon the enterprise community to solve issues that are caused by compliance enforcement gaps. This places the burden on the enterprise community to address security concerns caused by ICANN's oversight failures. ICANN needs to establish a more rigorous compliance mandate for all contracted parties (i.e. Registries, Registrars) and enforce accountability.

ICANN's mission of public trust is extraordinarily important. It is disappointing, however, that the SSR Plan does not more clearly reflect this public trust responsibility in the area of effective contractual compliance. The failure to effectively enforce contractual obligations among existing contracted parties calls into question ICANN's ability to effectively enforce new contracts. To the extent that the SSR Plan's use of words such as "collaborate", "enable," and "facilitate" suggest ICANN's intention to distance itself from its contractual compliance obligations, such an intention is also troubling.

A tremendous amount of effort has been devoted into recommendations to address security and stability issues related to the new gTLD proposal. The introduction of new gTLDs and -- more specifically, the predicted increase in contracts and contracted parties -- magnifies existing concerns about ICANN's ability to ensure contractual compliance. This does not bode well for assuring BC members of ICANN's ability to conduct compliance enforcement activities effectively.

**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 resiliency of the DNS as a system.**

As noted in previous sections in this paper, ICANN should more actively recruit and engage with law enforcement, the technical security community, and BC individual members to identify DNS risk vectors and the appropriate metrics for measuring the threat landscape.

# Constituency Support:

**Rapporteur for this Discussion Draft:** Adam Palmer

**Level of Support of BC Members:**

This document was posted to BC members for review and comment on 24-Mar-2011. Several BC members suggested edits that were accepted and circulated for further review. Pursuant to section 7.2 of the BC Charter, this document is deemed approved since no substantively opposing comments were received as of 6-Apr-2011.

Attesting BC Officer: Steve DelBianco, Vice Chair for policy coordination