Summary of Public Comments on the Security, Stability & Resiliency of the DNS (SSR) Review Team's Set of Issues

This document provides an overview of the public comments[1] received in response to a set of issues, circulated by the Security, Stability & Resiliency of the DNS Review Team (SSR-RT), which features eleven questions. The comments are grouped per question addressed and comments not referring to any individual question are summarized under "General Comments". The summary does in no way substitute for the original contributions, which should be consulted for complete information. The number of comments submitted on this paper tallies up to six. The comments are hyperlinked below for easy access and available at: http://icann.org/en/public-comment/public-comment-201104-en.htm#ssr-rt-issues

Contributions provided by:

At-Large Advisory Committee	ALAC	International Trademark Association	INTA
Business Constituency	BC	Ramses Martinez	RM
International Chamber of Commerce	ICC	Registries Stakeholder Group	RySG

RECOMMENDATION/CONCLUSION	SUMMARY OF COMMENTS
General Comments	**ALAC.** ALAC commends the work undertaken by the SSR-RT and extends its thanks to the Team. **BC.** BC thanks the Review Team, supports ICANN's effort to improve SSR and believes that attention should be focused on three areas of concern: 1. Adequacy of measures to prevent DNS abuse; 2. Lack of collaboration with enterprise community; 3. Oversight and resources to ensure compliance. ICANN participation in coordinated, industry efforts to combat malicious DNS activity is essential. Fraudulent WHOIS, manipulation of DNS records, and failure to enforce obligations of contracted parties continue to provide fertile ground for abuses that erode trust in e-commerce. BC has 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. The current SSR proposal shows good intentions but provides few assurances of effectiveness. The introduction of new gTLDs makes it critical to develop a robust SSR plan that will protect e-commerce and promote security.

[1] The public comment period ran from 21 February 2011 to 6 April 2011.

	The SSR Review is an opportunity to describe shortfalls in current plans and compliance, and to recommend improvements to implement before doubling or tripling the number of TLDs in use. **ICC.** The SSR-RT will play an important role in reviewing ICANN's Plan for Enhancing Internet Security, Stability and Resiliency, and its preparedness to deal with actual and potential challenges and threats. The RT should review the areas within the scope of ICANN's limited technical mission; recommend whether the rules/criteria need to be modified; identify any specific gaps and overlaps with existing organizations; and recommend how they can be addressed. As the Internet evolves, it is critical that secure, stable and consistent functioning and operation of the DNS remain a top priority. **INTA.** INTA agrees with the list of issues and urges the SSR-RT to consider the rights of consumers as well as trademark and brand owners in order to reduce fraud and maintain the viability of the Internet as a business tool. The AoC requires that ICANN decisions are made in the public interest and promote consumer trust in the DNS. The SSR-RT should keep in mind that SSR aspects are not only technical concerns, but also business concerns that affect the confidence of brand owners and consumers using the Internet. The issues should be considered from the perspective of their effect on the users who rely on the Internet to conduct business. User perspectives and suggestions for improvement should be sought through public comment.
Question/Request for Input 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.	**ALAC.** "Stability, Security, and Resilience" is lacking definition; both as a policy construct and as a phenomenon sufficiently understood to support measurement. **BC.** The lack of understanding and agreement of ICANN's SSR role is a persistent problem in policy-making discussions. The HSTLD-AG is an example of a working group that had difficulties with these issues and, as a result, arrived at a less-than-satisfactory outcome. The BC strongly supports a rigorous analysis of this topic. **ICC.** Refer to 2. **INTA.** There is a need to study and improve SSR of the DNS system, to protect Internet users and the rights of consumers and trademark owners. DNS hijacking/spoofing can lead to large-scale consumer confusion and harm to business owners' reputation. The SSR-RT should consider the rights of consumers and business owners as well as: 1. mechanisms to prevent DNS spoofing in order to combat fraud and stem trademark counterfeiting; 2. the role and responsibility of ICANN in responding to legitimate requests for information concerning DNS attacks, from trademark owners, investigators, or prosecutors investigating trademark violations. ICANN should retain information on DNS attacks for at least 6 months and enable legitimate inquiries for ICANN to investigate the cause and effects of such attacks. **RySG.** The documents listed at https://community.icann.org/pages/viewpage.action?pageId=6488074

	contain important material. The SSR Review Team should provide a summary and analysis of existing materials that the community can read and react to.
<u>Question/Request for Input 2.</u> 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.	**ALAC.** The current limitations in scope are adequate. It should be noted that the WHOIS issue is not a SSR aspect of the DNS. While approving ICANN's decision to focus on global deployment of DNSSEC, ALAC points out that it will only become effective and useful once adopted and implemented by major TLDs, as well as by registrars and registrants. An awareness campaign is needed to convince the actors to support DNSSEC. **BC.** DNS abuse is pervasive, costly to mitigate, and becoming increasingly complex. Cybercriminals target BC members because they are seeking “high value” targets (financial resources). The current SSR Plan fails to provide steps that will allow ICANN to address DNS abuse. The introduction of new gTLDs may expand the opportunities for online fraud: these security concerns should be more carefully considered in any SSR plan. 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 SSR Plan understates the implications of the introduction of new gTLD while overstating the scope and efficacy of ICANN’s mitigation efforts. The SSR plan should include a focus on mitigating the DNS abuse threats against the e-commerce community, on reversing the compliance environment that fosters abuse, and on clarifying that there will be meaningful assistance to targeted enterprise users. **ICC.** ICC supports ICANN’s coordinating role in “Preserving and enhancing the operational stability, reliability, security, and global interoperability of the Internet” as outlined in the ICANN By-Laws. **INTA.** The scope of inquiry for the SSR-RT should include limitations on ICANN’s *abilities* (as opposed to *responsibilities*) in ensuring SSR of the DNS. An unstable, insecure and/or inelastic DNS would endanger and/or impede all Internet users and could have catastrophic results. If potential threats are identified, action should be taken. The relevant inquiry should not be whether taking such action is within the scope of ICANN’s *responsibilities*, but rather, whether such action is *permitted* by the bylaws and related documents. **RySG.** ICANN activities must flow from and be measured against its mission statement and set of values . The mission is specific and limited, but lack of common understanding is a significant problem and the SSR team would do well to define the terms. Distinctions are necessary between: 1. the global Internet's systems of unique identifiers; 2. the DNS root server system; 3. the DNS levels below the root; 4. DNS technical protocols; 5. software implementations of DNS protocols; 6. uses of domain names and numbers; 7. the Internet. ICANN cannot go beyond its technical coordination role nor be a substitute for the roles of law enforcement and governments. ICANN has no mandate to examine or regulate content or speech, nor can

	ICANN regulate social or technical use of the DNS and the Internet unless they threaten the DNS stability and security. ICANN should always be "respecting the creativity, innovation, and flow of information made possible by the Internet by limiting ICANN's activities to those matters within ICANN's mission requiring or significantly benefiting from global coordination." The GNSO's Registration Abuse Policy Working Group (RAPWG) has analyzed the limits of ICANN policy-making on security and stability - especially the difference between domain registration and domain use.
Question/Request for Input 3. Recent opinion on the DNS CERT proposal and on the need to coordinate/support detection and management of attacks/incidents to DNS	**ALAC.** DNS CERT is outside ICANN's mandate. The community would be better served by an independent organization running the CERT. **BC.** The DNS-CERT proposal was perceived as a top-down rather than bottom-up proposal and did not garner broad support in the community. This initiative should be reviewed and lessons-learned should be drawn from that. DNS-CERT suffered from lack of clear agreement on ICANN's scope and definition. Until that is worked out, ICANN needs to engage with the security community on any initiative, ranging from quick responses to threats to policy discussions. Agreeing on the nature of this engagement should be a priority. **ICC.** ICANN should engage in further consultation with operators of the DNS, businesses and all community members to develop such initiatives. Certain types of malicious attacks may fall outside of ICANN's mission: ICANN's role should be consistent with its charter and limited to its technical coordination, non-operational role. The DNS-CERT proposal implies issues concerning data sharing and liability that must be addressed to encourage operators to participate. A number of organizations address these concerns and focus on specific aspects of DNS security. ICANN should consult and facilitate coordination across these organizations to avoid duplication of efforts and resulting diminished value. A gap analysis identifying the threats is a necessary first step in developing SSR and DNS-CERT initiatives that will enhance SSR. **RySG.** The mission of establishing a DNS-CERT was outside of ICANN's technical coordination role. The need for and the potential responsibilities of a DNS-CERT remain unclear. Refer to: http://forum.icann.org/lists/dns-cert-proposal/msg00014.html
Question/Request for Input 4. Experiences, difficulties, unexpected advantages, and lessons learned in the implementation of DNSSEC.	**ALAC.** Recent events (e.g. software bug in .fr) may, according to some, show that the infrastructure is not ready for ubiquitous DNSSEC deployment. Relaxing pressure for DNSSEC deployment and proceeding carefully would allow all operators in the DNS chain to gain experience and mitigate risks. This includes the new gTLD program, where registries are mandated to deploy DNSSEC. Others contend that cost and complexity may decrease overtime and support mandatory DNSSEC deployment for new gTLDs. Long term benefits of DNSSEC are likely to prevail and ALAC cautiously warrants full DNSSEC deployment for new gTLDs, provided smaller applicants get a suitable time for adaptation. **BC.** A coordinated effort including the BC members is needed to effectively implement SSR policy. While not

	endorsing ICANN to manage a DNS CERT program, BC advocates creation of an industry managed compliance and security coordination system to ensure enforcement of SSR policy in the DNS. The successful DNSSEC implementation provides a model for security improvements that can be achieved by industry collaboration. **ICC.** DNS security will benefit from top-down deployment of DNSSEC. DNSSEC's data origin authentication and data integrity features can thwart cache-poisoning attacks. The DNS community is exploring other options, but no other solution has been fully developed, nor provides the same protection against this vulnerability. DNSSEC requires more maintenance functions and processing resources, and introduces more complexity. If not appropriately managed, this overhead can have negative impacts on security and stability. **RM.** Verisign encountered issues around the harmonization of current standards and policies from the physical security side to suit the needs of the key management infrastructure for DNSSEC. These issues were the result of the specs for the system being incorrectly attributed the same level of security as those for the previously managed PKI environment. When authentication and integrity functions are added to an information system it becomes more brittle. As a result, operational and change management procedures associated with those systems must be adapted and become more mechanical. As DNSSEC makes the system more brittle, it requires more care, as opposed to the previously prevalent 'fire and forget' model. **RySG.** DNSSEC implementation is complicated, and operational problems are still being discovered by gTLDs and ccTLDs. Registrant knowledge of DNSSEC remains low, and very few registrars offer user-friendly signing functionality to registrants. The marketplace should work to fill registrant needs.
<u>Question/Request for Input 5.</u> Sources of risk analysis for the DNS, as well as contingency planning, business continuity planning (BCP) and related work for the DNS.	**BC.** The security community has invested significant time to make recommendations on security improvements. The BC recommends that the law enforcement and technical security community and other security experts be recruited to ICANN working groups on DNS risk analysis. ICANN should follow the recommendations from such working groups on threat risk analysis and design improvements. **ICC.** Threats include the DNS vulnerability published by Kaminsky and others in 2008. Computer servers are particularly vulnerable to "cache-poisoning" that redirects unsuspecting Internet users to malicious sites or hijacks their email. DNSSEC mitigates this risk by adding data integrity capabilities to the system. **RM.** Risk analysis in the information security field should be conducted as a function of the business with specific consideration given to the position in the marketplace of the entity in question. Mature frameworks for these areas exist and should be used (COSO, NIST, ISO 27002) rather than developing purpose-made risk analysis standards for the DNS infrastructure space.
Question/Request for Input 6. Original solutions proposed to increase the Stability, Security, and Resilience of the DNS at the protocol level,	**ALAC.** While the current DNS works relatively well from a technical point of view, ICANN should also

including the design of the Root Server system.	encourage and possibly fund research to address challenges and needs of future naming systems. **ICC.** The current model seems to work well and has added observable resilience and scale to the system. **RM.** Operational or security issues are not the result of poor protocols or in the architecture flaws but rather poor implementation of existing standards, such as ITL, COSO, NIST or ISO, which enable operation at peak efficiency and often result in reduced cost of operation. Regarding the root server system, the current configuration enables the most reliability, security and resiliency for the global users of the Internet. **RySG.** The DNS protocols are the responsibility of the IETF. The design of the root server system is in some ways separate from the protocols.
<u>Question/Request for Input 7.</u> Processes used by DNS users and operators to guarantee that the Risk Analysis related to the DNS is comprehensive and updated.	**BC.** ICANN should continue to include the BC, law enforcement members and the technical community in consultations aimed at developing solutions to improve compliance enforcement. ICANN needs to enforce contractual obligations in a timely manner. BC commends the hiring of additional compliance staff and urges that this staff be empowered with support and authority for enforcement. The current narrow approach to compliance enforcement is unnecessary, harms business and cripples security. ICANN should define high security zone standards for domains requiring additional security. Large domain operators should have an appropriately weighted voice for advancing security matters, including input to the RAA. Registrant data must be accurate, maintained securely, and available upon appropriate request to mitigate abuse. Mechanisms for input to compliance staff on registrar/reseller problems and compliance violations should be improved. **RM.** Education is needed on how to conduct risk analysis using current frameworks and tools. Risk analysis would capture risk in discrete and aggregate form and allow for managing risk in a viable manner. Risk analysis models should recognize DNS as a critical asset that enables nearly all Internet-facing and internal transactions in today's IP networking environments. The application of well-practiced systematic approaches to risk analysis fully enumerates the role of the DNS in enabling user-desired or machine-initiated transactions and appropriately considers systemic elements of the DNS. **INTA.** The SSR-RT should solicit suggestions on practices and protocols for maintaining security and minimizing risks. Suggestions should be analyzed to help the SSR-RT formulate an action plan.
<u>Question/Request for Input 8.</u> Analysis of the relationships of ICANN with "contracted parties" (registries and registrars) as well as others (ccTLDs not bound contractually to ICANN, Root Server Operatorrs, etc.)	**ALAC.** Among the non-contracted parties, domain name resellers and WHOIS proxy/privacy providers are unaccountable to ICANN, and have been involved in many issues. One suggestion would be to have a clear accreditation mechanism for these and 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 as a way to formalize responsibilities for DNS stability.

	ICC. The relationship between ICANN and its contracted parties is an important component of ensuring SSR. The premises are that ICANN contracts with relevant parties form the basis of „self governance‟ and that all stakeholders must work together in a consensus-based, bottom-up policy process. ICANN should increase its efforts to meet its contractual enforcement and compliance responsibilities. **INTA.** Public comment should be invited on potential changes to ICANN's contracts to better protect DNS SSR. ICANN has different responsibilities with ccTLDs and Root Server Operators, but a system for sharing information regarding attacks, and the safety of the DNS as a whole, could be feasible and helpful. **RySG.** The SSR RT can reference the existing contracts and the scope of GNSO policy-making is well-defined.
Question/Request for Input 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.	**ALAC.** There is a need to reinforce the link with the IETF community, including clear agendas and timelines for features and changes in the DNS protocols, based on operators' and users' experience. **BC.** ICANN has not sufficiently included key stakeholders in its SSR initiatives. The SSR Plan indicates that ICANN will focus primarily on the contracted parties in such initiatives. ICANN must further engage users and enterprises in collaborative efforts. The sense of urgency to move forward with new gTLD expansion has hampered ICANN's ability and/or desire to understand stakeholder concerns. 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 and there has been too little collaboration with enterprises to design mitigation programs, which should assist enterprises exposed to abuse. **ICC.** ICC supports the private sector-led, multi-stakeholder, bottom-up policy development model that has made ICANN successful in ensuring SSR. ICC is aware of pressures by governments and IGOs to play a larger role in the design, implementation, and evolution of the DNS. ICC supports an advisory role in these areas for governments within current ICANN structures, and believes that any alternative arrangement would stifle innovation, and result in overly prescriptive and constrained working models. **INTA.** The proposal for a CERT for the DNS should be further analyzed. The main inquiry should be how to maximize these efforts and further inquiry is needed regarding the benefits of a central CERT to track efforts around the world to detect and manage attacks. Non-ICANN entities should be invited to assist and possibly implement and operate a coordinated methodology for combating cyber attacks and related incidents. **RySG.** ICANN's structure (http://www.icann.org/en/structure/) accommodates participation by a relevant set of stakeholders. ICANN has undertaken reviews of its Supporting Organizations and Advisory Committees.

Question/Request for Input 10. Solutions/Proposals on Root Server Governance, including transparency, accountability, security/performance measurements, policies, accessibility and the opportunity to have more RS operators	**BC.** Insufficient effort has been devoted to addressing concerns with enforcing contractual compliance. Vacant security and compliance positions in ICANN have only recently been filled and ICANN's restrained enforcement policy raises concerns about the effectiveness of any security plan. The oversight needed for a strong security program does not exist and without such, even the best SSR plan will fail. ICANN needs to acknowledge the role that its policies play in the process and to be accountable. ICANN often relies on the enterprise community to solve issues caused by compliance enforcement gaps. ICANN should establish a rigorous compliance mandate for all contracted parties and enforce accountability. The SSR Plan should clearly reflect this public trust responsibility. The failure to enforce contractual obligations casts doubts on ICANN's ability to effectively enforce new contracts. It is troubling if words like "collaborate", "enable," and "facilitate" in the SSR Plan imply an intention to distance ICANN from its obligations. Much effort has been put into recommendations to address security and stability issues with new gTLDs. The introduction of new gTLDs with increased number of contracts magnify existing concerns about contractual compliance. **ICC.** Ensuring adequate accountability and transparency in Root Server Governance is important. Mechanisms to enhance such accountability and transparency should be identified, but a gap analysis must first highlight what issues exist and might be better served by evolving the current Root Server Governance models. **INTA.** All Internet users are best served by transparent and accountable Root Server operators and operations. We question the need for additional RS operators. Additional RS operators may have the unintended consequence of complicating the existing system leading to less transparency and accountability. **RySG.** More root server operators lead to greater possibility for errors and omissions, which would make the root less reliable and consistent. Additional root operators could therefore create additional risk. Adding more *instances* of root servers adds to the technical stability and resiliency of the root.
Question/Request for Input 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	**BC.** ICANN should more actively engage with law enforcement, the technical security community, and BC members to identify DNS risk vectors and the appropriate metrics for measuring the threat landscape. **ICC.** ICC notes the work of the SSAC and the Root Scaling Report. These should be considered as part of the compendium of information on large-scale risks to the DNS. **INTA.** Internet's operation depends primarily on a secure DNS and the industry should look into adopting additional security measures relating to DNS and DNSSEC. One concern with DNSSEC is that it may increase exposure of DNS servers to denial of service (DOS) and distributed denial of service (DDOS) attacks. These increased risks should be weighed against the gains to be made by the DNSSEC. Additionally, where possible, these additional risks should be eliminated or mitigated.