Registries Stakeholder Group Statements Regarding the "Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR)" and "Global DNS-CERT Business Case"

14 April 2010

The comments below are submitted on behalf of the gTLD Registries Stakeholder Group (RySG). The comments that follow represent a consensus position of the RySG as further detailed at the end of the document.

The Registries Stakeholder Group (RySG) submits these comments in response to ICANN's "Proposed Initiatives for Improved DNS Security, Stability and Resiliency" ("SSR") and ICANN's "Global DNS-CERT Business Case." We offer comment on the foundations of those documents, and offer recommendations for further work.

TLD Registry Operators play a critical role in the secure and stable operation of the DNS and we welcome the opportunity to discuss initiatives to improve DNS security, stability, and resiliency. Registries' infrastructures, personnel, expertise, technology, investments, and operational practices have underpinned the secure and stable functioning of the Internet as it has scaled globally over the past two decades. Indeed, registries are on the "front lines" of defense against a variety of security threats that occur on a daily basis. As such, registries have developed expertise in addressing a broad range of threats. Registries have successfully coordinated with other actors in the DNS and Internet services spaces to address threats ranging from simple operator errors to those caused by sophisticated bad actors. Registries look forward to consulting with ICANN on these important issues and to engaging with other actors to further develop these initiatives.

ICANN's SSR and DNS-CERT documents are based on two primary assumptions: 1) operators that provide DNS services often react to emerging threats in a largely uncoordinated and under-resourced fashion; and 2) the need to develop a "system-wide" approach to DNS security, stability, and resiliency. With regard to the first assumption, the RySG points to the broad and coordinated responses to the Kaminsky bug and the Conficker worm. Both of these recent collaborations demonstrated a very effective level of coordination, information sharing, and action. Indeed many of the entities in question have been collaborating regularly for many years to address security threats. This engagement and network of relationships already provide a foundation on which to build institutionalized coordination structures should they be deemed necessary. With regard to the second assumption, ICANN has called attention to addressing problems with the DNS and/or the Internet as a whole. However, the scope of the proposed initiatives goes

far beyond ICANN's mission—proposing to address a variety of issues that do not threaten the DNS system itself.

ICANN points to its Bylaws and the Affirmation of Commitments (AoC) to define its responsibility to ensure the stable and secure operation of the Internet's unique identifier systems. In general terms, ICANN plays a coordinating, non-operational role in managing Internet naming and numbering resources. However, in the SSR and DNS-CERT documents, ICANN's proposed role seems both unclear and over-broad. The RySG shares the concern already voiced by some in the community that ICANN's role in these potential initiatives and undertakings not cross over into an operational capacity. ICANN should undertake activities that are consistent with its limited technical coordination role. There should be a systematic examination of that role in relation to the SSR and DNS-CERT, using existing community processes. ICANN must be able to explain its remit and work within it, rather than expanding its mission to meet unrealistic or uninformed expectations, or into areas best filled by other entities.

The SSR proposes a number of initiatives and undertakings. Many of these proposed initiatives are substantive and robust:

- creation of an accepted DNS risk framework and refining approaches to measuring risk.
- a DNS root server system information-sharing mechanism – with ICANN having the responsibility to orchestrate a biannual system-wide DNS exercise focused on response to key contingencies.
- a system-wide DNS exercise program to ensure response capabilities is evaluated and deficits identified.
- Continued support of root server operators' contingency planning and exercises.
- ICANN staff and other members of the DNS community participation in the multilateral Cyber Storm III exercise and perhaps other international exercises.
- ICANN and TLD registry operators to conduct data escrow testing throughout 2010 and into 2011 based on the development of the data escrow specification for the new generic top-level domain (gTLD) process.

Some of the proposed initiatives have already been undertaken in other fora (e.g. Cyber Storm exercises in the U.S. President's NSTAC), and others are new initiatives that would require broad and careful participation and coordination among all key actors. We have concerns about others. For example, please see our notes below regarding the DNS Risk Assessment and Contingency Planning expert advisory group, and the scope issues associated with DNS-wide exercise and evaluation programs.

It is very possible that additional capabilities or resources will be useful to the DNS community for responding to future large-scale security incidents, and we support community exploration. What kinds of incidents might qualify is poorly defined at present. Whether such a capability should be called a "CERT", exactly what capabilities are needed, where they should be located, and how they should be funded are not addressed adequately and need further work.

RySG Recommendations

The RySG feels that ICANN must engage in further, deeper consultation with the key operators and community members to do the following:

1. Develop a clear articulation of the threats facing the DNS that require system-wide, concerted, and structured action. This has not yet been done, and such fact-finding is necessary before defining or funding any programs. The DNS-CERT concept is predicated on "a wide-scale coordinated attack against the DNS." What needs to be established is what attacks could threaten the DNS itself.
2. Identify what elements of the DNS threat review are properly within ICANN's technical coordination mission.
3. Perform a gap analysis to see if there are needs that are not already addressed by industry and governments. This analysis should include examination of what parties are already engaged with what threats, what needs those parties do and do not already satisfy, and how existing entities might be engaged to fill any gaps.
4. Better identify stakeholders relevant to the mission and scope. The DNS-CERT proposal identifies a tremendously wide range of stakeholders, including potentially almost every company and user on the Internet. Focus on the DNS system itself is needed to narrow down to a more relevant group of stakeholders.
5. After the above are done, it would be appropriate to decide what role ICANN should have, including whether any functions should be located with ICANN, whether any functions should be located in existing or new entities outside ICANN, and how ICANN resources or funds should be used.

The RySG believes that core DNS issues are within the scope of ICANN's security and stability mission. ICANN should be concerned with threats to the DNS itself—those that could seriously impact the functioning of the DNS or Internet, i.e. the system overall. These include:

- Significant technical risks to core protocols or functions: such as the Kaminsky bug, and load issues associated with DNSSEC or expansions of the root.
- We agree that "reliable, resilient operations of the root server system and the top-level domains must be a first-tier ICANN priority. " For example, the ability of the root servers to withstand DDoS attacks, and the reliability and consistency of root server response across the globe. The proposed root system information-sharing mechanism, and business continuity planning for root server and gTLD operators, is appropriate.

The RySG believes that the following are outside of ICANN's mission, and should be dropped from the SSR and the "Global DNS-CERT Business Case." We are concerned that those two documents go from a focus on threats to *the* DNS to getting ICANN involved in the many things that happen *on* or *via* the DNS. In general, ICANN and the DNS-CERT should not be operationally focused, and many issues are best addressed by industry and governments. As per ICANN's core values, ICANN should be "[t]o the extent feasible and appropriate, delegating coordination functions to or recognizing the policy role of other responsible entities that reflect the interests of affected parties." Out-of-scope activities include:

- Monitoring of or response to ordinary problems, such as:
    - Monitoring and/or mitigating attacks on private infrastructure not related to root operations, including most DDoS attacks. Impactful attacks against the root servers are of great concern, but ICANN cannot and should not be concerned with attacks against Web sites, Internet services across the Internet, or contracted parties. These do not "destabilize the Internet's infrastructure" as the "Proposed Initiatives" claims, and are an unfortunate but unavoidable risk associated with providing Internet services.
    - Registry and registrar operations not related to their core functions. For example, the "Proposed Initiatives" discuss how miscreants attack registrar's Web sites, and hijack domains via social engineering. ICANN is not in a position to monitor or mitigate such issues, or to provide resources for another entity to do so. ICANN has delegated responsibility to gTLD registry operators, who are responsible for delivering on the service level agreements in their contracts for DNS provision and registry availability. The gTLD registry operators have an excellent record of living up to those agreements.
    - E-crime. Operations to address criminal uses of domain names are not reasonably and appropriately related to ICANN's technical coordination function, and ICANN cannot be a substitute for or compensate for the roles of law enforcement, governments, and industry. The "Proposed Initiatives" identifies malicious activities such as "fraud, extortion, and other illicit online activity." The DNS-CERT proposal speaks about monitoring and mitigating botnets, phishing, and malware, and how they "illustrate the need for a standing DNS security response capability" involving stakeholders across the Internet. However, such problems have not threatened the basic security or stability of the DNS itself.
- Running Internet-wide exercises and evaluation programs. ICANN participation in such can be useful. However, the "Proposed Initiatives" and "DNS-CERT Business Case" propose that ICANN and the DNS-CERT run exercises involving a tremendously wide range of stakeholders, which may need to be narrowed.
- The proposals contain initiatives to make up for the "less capable and less well funded DNS operators and other stakeholders who are not aware of threats and risks and who lack capabilities to adequately respond when such threats to security, stability and resiliency are realized." The DNS-CERT proposal says it

will provide both proactive and "reactive incident services that aid constituents with significant resource constraints, such as registrars in lesser-developed regions of the globe." It is unclear what this entails exactly. It might be useful to develop better resources for communication and referrals, for example. However, ICANN must be careful to manage expectations, and ICANN cannot make up for shortcomings at all the entities that contribute to DNS security, which includes: registry operators world-wide, software and operating system vendors, ISPs, registrars, etc. The decentralized nature of the Internet is one of its core strengths, and is a designed-in feature. Malefactors may take advantage of the fact that responsibilities and resources are delegated to entities of varying capabilities, and in various national jurisdictions, but delegation is one of ICANN's core values, and a technical reality fundamental to the Internet. ICANN cannot always compensate for the drawbacks of that reality.

- National security, cyber-war, etc. The "Proposed Initiatives" paper says: "As ICANN plans to address its role in managing the risks to the security, stability and resiliency of the DNS, it does not address issues related to national security competition between states in the realm of cyber war or espionage or address control of content hosted on the Internet…." However, the DNS-CERT Business Case's "Situational Analysis" mentions these issues, including "politically-motivated attempts to influence or disrupt DNS operations" and "demonstration[s] of technical superiority." Issues such as the DDoS attacks against Georgian infrastructure during the 2008 South Ossetia War are beyond ICANN's mission to monitor or mitigate.

The "Proposed Initiatives" calls for the establishment of a "DNS Risk Assessment and Contingency Planning expert advisory group," to be "composed of experts from the DNS operations and cyber security communities," and could create action plans that would "constitute input to ICANN's annual cycle for its security, stability and resiliency and operational planning budgeting." There should be significant community discussion about this idea. We are concerned that this new group would duplicate or usurp the role of ICANN's Security and Stability Advisory Committee (SSAC), and could provide budget advice outside of existing channels. As per the ICANN Bylaws, it is the SSAC's role to advise the ICANN community and the ICANN Board on matters relating to the security and integrity of those systems, to develop a security framework for Internet naming and address allocation services that defines the key focus areas, and to perform ongoing threat assessment and risk analysis to assess where the principal threats to stability and security lie.

Finally, ICANN has proposed significant human resources and budgetary resources for the proposed initiatives, including more than US$4 million for the DNS-CERT. The RySG believes that given the clear need for additional consultation and clarification of the underlying threats and their respective relevance to the DNS, ICANN's appropriate role, a gap analysis and a reformulation of the proposed initiatives thereafter, it is premature for ICANN to be establishing budgetary estimates for these programs.

GNSO gTLD Registries Stakeholder Statement of Support

Issues: **"Proposed Strategic Initiatives for Improved DNS Security, Stability and Resiliency (SSR)" and "Global DNS-CERT Business Case"**

A supermajority of 10 RySG members supported this statement.

General RySG Information

- Total # of eligible RySG Members[1]: 14
- Total # of RySG Members: 13
- Total # of Active RySG Members[2]: 13
- Minimum requirement for supermajority of Active Members: 9
- Minimum requirement for majority of Active Members: 7
- # of Members that participated in this process: 13
- Names of Members that participated in this process:

1. Afilias (.info and .mobi)
2. DotAsia Organisation (.asia)
3. DotCooperation (.coop)
4. Employ Media (.jobs)
5. Fundació puntCAT (.cat)
6. Museum Domain Management Association – MuseDoma (.museum)
7. NeuStar (.biz)
8. Public Interest Registry (.org)
9. RegistryPro (.pro)
10. Societe Internationale de Telecommunication Aeronautiques – SITA (.aero)
11. Telnic (.tel)
12. The Travel Partnership Corporation – TTPC (.travel)
13. VeriSign (.com, .name & .net)

[1] All top-level domain sponsors or registry operators that have agreements with ICANN to provide Registry Services in support of one or more gTLDs are eligible for membership upon the "effective date" set forth in the operator's or sponsor's agreement (RySG Articles of Operation, Article III, Membership, ¶ 1). The RySG Articles of Operation can be found at <http://gnso.icann.org/files/gnso/en/improvements/registries-sg-proposed-charter-30jul09-en.pdf>. The Universal Postal Union recently concluded the .POST agreement with ICANN, but as of this writing the UPU has not applied for RySG membership.

[2] Per the RySG Articles of Operation, Article III, Membership, ¶ 6: Members shall be classified as "Active" or "Inactive". A member shall be classified as "Active" unless it is classified as "Inactive" pursuant to the provisions of this paragraph. Members become Inactive by failing to participate in a RySG meeting or voting process for a total of three consecutive meetings or voting processes or both. An Inactive member shall have all rights and duties of membership other than being counted as present or absent in the determination of a quorum. An Inactive member may resume Active status at any time by participating in a RySG meeting or by voting.

- Names & email addresses for points of contact:
  - Chair: David Maher, dmaher@pir.org
  - Alternate Chair: Jeff Neuman, Jeff.Neuman@Neustar.us
  - Secretariat: Cherie Stubbs, Cherstubbs@aol.com

Regarding the issue noted above, the level of support in the RySG is summarized below.

1. **Level of Support of Active Members**: Supermajority
   1.1. # of Members in Favor: 10
   1.2. # of Members Opposed: 0
   1.3. # of Members that Abstained: 0
   1.4. # of Members that did not vote: 3
2. **Minority Position**(s): N/A