March 18, 2013

Mr. Akram Atallah
Chief Operating Officer
Internet Corporation for Assigned Names and Numbers
12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

Dear Akram,

On behalf of the Registries Stakeholder Group (RySG), I respectfully submit this letter to you for your urgent review and action. This letter is submitted in response to your letter of February 21, which replied to the RySG's February 8 letter on unresolved new gTLD implementation issues.

The RySG is committed to the timely, secure and stable introduction of new gTLDs. We bring the following issues to your urgent attention to help ICANN and all applicants meet the stated deadlines.

As described in detail below, the RySG has identified several critical areas associated with Pre-Delegation Testing (PDT) that require urgent clarification and communication to new gTLD applicants and back-end registry service providers. While we have noted ICANN's March 13 update http://newgtlds.icann.org/en/applicants/pdt , upon careful review, we have determined that sufficient detail has not been provided in several key areas. By omitting or delaying communication of these important details, ICANN risks preventing registries and applicants from being able to conduct pre-delegation testing in a secure, predictable and timely manner.

The outstanding issues that require immediate attention, referenced to your February 13 letter, are as follows:

1. Test Plan Documentation: We have not yet received the PDT "Master Test Plan," nor have we received the "Level Test Plans" and "Level Test Cases" referenced in the "Applicant input specification for pre-delegation testing" Version 1.1. Additionally, no information has been provided on what "query-by-proxy" entails and we are already well inside of operational change control timelines. We are extremely concerned that ICANN has not taken into account the need for a registry to conduct security audits and internal testing prior to external engagement in order to ensure operational readiness and preserve the security and stability of existing services. Frankly, we are perplexed that this was not accounted for in ICANN's timeline. When will we receive this important information?

2. Load Capacity Testing: Section 8.1 -- Re: load capacity testing, without the intended "load" information it is difficult to understand what level of resources will be required for said testing. This information needs to be provided in advance such that engineering and operations teams can ensure the desired objectives can be met without impacting other

services that may be operating within a given environment. While we understand the desire to conduct network infrastructure stress tests, the methodology seems flawed and is not feasible. We would entertain a load capacity test that is more bottoms-up in nature, which demonstrates stability at increased volume levels, but not to the point of network degradation and/or packet loss. Furthermore, if test cases were to be deployed on operational infrastructure that accommodates other services, any attempts to induce “10% query loss against a randomly selected subset of servers within the applicant’s DNS infrastructure” could result in either link saturation or degradation of operational services. Lastly, we are not in a position to run tests of this nature on production infrastructure with live customers; and as noted in our correspondence last month, such tests could likely invoke Response Rate Limiting (RRL), which would skew the results. Absent the “Master Test Plan” and other information it is unclear of the intention here.

3. Reachability Documentation: Relative to Section 8.2 on Reachability Documentation, without a thorough understanding of the "safeguards" have been put in place with *all* parties that would have access to this information, and assurances that these safeguards are and will continue to be maintained until the information is securely purged and we have been notified, we remain highly concerned about releasing this information. As stated in our correspondence last month, this information is extremely sensitive. Many operators employ literally hundreds of controls to protect this and other such information, the compromise of which could have serious security and stability or broader implications. Once again, we recommend less stringent tests that demonstrate that registry service providers possess the technical competence required to run registries.

4. TCP and DNSSEC Capabilities: Relative to Section 8.3 on TCP and DNSSEC Capabilities, a "strict non-disclosure agreement with ICANN" does not give assurances that the information will be protected. What controls have been put in place by the pre-delegation testing provider to protect this information, and how are these controls assured, etc..? See S8.2 response above.

5. TCP and DNSSEC Capabilities: Section 8.3 (continued) – What precisely does "query-by-proxy" entail? Where the software originated, who performed security and services audits on it, and how it should be provisioned to access the "direct instances" are still unclear. In operational networks, it takes substantial time to update secure controls and operationalize new servers and systems. The lack of information about "query-by-proxy" here gives us considerable concern given the expected timing, as it may pose a risk to security and stability of registry operator networks and infrastructure. We believe that query-by-proxy could be easily gamed and that simply querying the Internet-facing name server addresses on the globally anycasted addresses would yield the most consumer-centric results.

6. TCP and DNSSEC Capabilities: Section 8.3 (continued) -- Regarding "additional security, queries to the proxy may be filtered and/or rate limited if required by the DNS service

provider", it is unclear what circumstances or concerns would introduce the need for such a capability for a purpose-built proxy that will not be employed for anything beyond protocol compliance and zone propagation delay testing. It is also unclear how many instances of a given anycasted service would need to be available through the proxy, the frequency of queries that would be used, or the period over which the proxy would be expected to be operational. The potential intermediary effect introduced by the proxy itself will also bias any tests performed. Again, we believe that simply querying the Internet-facing name server addresses on the globally anycasted addresses would yield results most representative of consumer-centric results.

7. Tests Against Existing Infrastructure: Relative to Section 8.5, Tests Against Existing Infrastructure, what testing procedures and methodology are being used? What rate and scale of testing are we talking about? From what systems (IP addresses) will testing be performed? Systems that registry operators use for things like volumetric attack detection and mitigation might result in artifacts in any measurements, and this could potentially trigger broader collateral damage, particularly in multi-tenant DNS systems. Also, it should be observed that taking the servers "out of the DNS anycast cloud" would itself bias the results, as they'd potentially be much less loaded than they are under normal operational conditions. It is unclear what testing procedures, methodology, timing, frequency, duration, scale, etc. will be employed. As stated above in the Load Capacity section, this causes us concern. We believe that simply querying the Internet-facing name server addresses on the globally anycasted addresses would yield the most representative consumer-centric results.

8. IDN Table Testing: Based on the March 13 update, "Applicant input specification for pre-delegation testing", version 1.1, ICANN is requesting that testers provide the appropriate IDN tables, and documenting the policies on how the tables will be processed, and how variant relationships between codepoints are managed. How does ICANN plan to test this component? Will ICANN be developing generic test cases specific to each language script or will the test cases be specific to the tables and policies that the applicant provides? Will EPP be used as the interface to carry out their test cases? If so, the appropriate EPP extensions will need to be provided to the PDT provider, but this information was not requested in the posted document.

9. Trademark Clearinghouse: Will registry interaction with the Trademark Clearinghouse be a component of the PDT?

The RySG is extremely concerned that these critical operational implementation details have yet to be finalized and/or communicated. We are available to engage with ICANN and its contractors, as appropriate, to further discuss and resolve these outstanding issues. The RySG is fully committed to the timely, secure and stable introduction of new gTLDs. Not addressing these concerns in a timely manner will undoubtedly have a negative impact on the projected timeline for introduction of new gTLDs.

Sincerely,

Keith Drazek
Chair,
Registries Stakeholder Group

Cc: Mr. Fadi Chehadé, President & CEO, ICANN
Mr. Cherine Chalaby, Chair, ICANN Board New gTLD Committee