Dear Patrik,

Thank you for SSAC's work providing advice and recommendations in your reports on Root Scaling concerns (SAC 046 dated 06 December 2010), and Internal Name Certificates issues (SAC 057 dated 15 March 2013). In addressing these two reports the ICANN Board has adopted resolutions to implement the SSAC's recommendations in SAC 046, and staff are working on implementing them. ICANN has also taken the SSAC's recommended actions to mitigate the risks identified in SAC 057, and continues to pursue additional actions to deal with derivative risks.

This email outlines the specific steps ICANN has taken to address the concerns raised by the SSAC in SAC 046 and SAC 057 and also provides an update on our ongoing actions to manage these concerns.

SAC 046: Root Scaling

In September 12, 2013, the ICANN Board passed resolutions to specifically implement the SSAC's recommendations on root scaling identified in SAC 046. Below is a status update on implementation of each SSAC recommendation in SAC 046.

SSAC Recommendation 1: Formalize and publicly document the interactions between ICANN and the root server operators with respect to root zone scaling. ICANN and the root server operators may choose to utilize RSSAC to facilitate this interaction.

- **Board Action:** The Board requested the CEO direct staff to work with the *root server operators via RSSAC* to complete the documentation of the interactions between ICANN and the root server operators with respect to root zone scaling.

- **Implementation Status:** ICANN as L-Root operator participates in regular discussions with other Root Server Operators regarding instrumentation of the Root Server system. With respect to measurements directly motivated by concerns over root zone scaling, these discussions have been ongoing since May 2011. While a record of discussions on the RSSAC list exists in the form of its archive, no specific documentation on the interactions between ICANN and other root server operators on this topic has been drafted. ***[This task is not complete]***

SSAC Recommendation 2: ICANN, National Telecommunications and Information Administration (NTIA), and VeriSign should publish statements, or a joint statement,

that they are materially prepared for the proposed changes.

- **Board Action:** The Board recommended the CEO to *direct staff to work with NTIA and Verisign* to explore publication of one or more statements regarding preparation for the proposed changes.

- **Implementation Status:** ICANN staff worked with NTIA and Verisign and the parties released a joint statement on 5 November 2012. A copy of the joint statement was sent to the SSAC (via Patrik Fältström) on 8 November 2012. ***[COMPLETED]***

SSAC Recommendation 3: ICANN should publish estimates of expected and maximum growth rates of TLDs, including IDNs and their variants, and solicit public feedback on these estimates, with the end goal of being as transparent as possible about the justification for these estimates.

- **Board Action:** The Board recommended the CEO to direct staff to publish current estimates of the expected growth rates of TLDs. The Board suggested the publication of the expected growth rates of TLDs be coordinated with the re-examination of the process for evaluating gTLD applications.

- **Implementation Status:** ICANN has been regularly publishing the expected and maximum growth rates of TLDs. For example, see page *2* of: http://newgtlds.icann.org/en/applicants/batching/drawing-prioritization-10oct12-en.pdf) as well as in other regular new gTLD updates. ***[COMPLETED]***

    1) **Batching / Metering:** After careful analysis of public comment and possible solutions for processing new gTLD applications, ICANN proposed a drawing for prioritizing applications through the steps leading to delegation. ICANN held a Prioritization Draw (Draw) on *17 December 2012* in Los Angeles to assign priority numbers to all new gTLD applications. Each application was assigned a randomly-drawn priority number. ***[COMPLETED]***

SSAC Recommendation 4: ICANN should update its "Plan for Enhancing Internet Security, Stability, and Resiliency," to include actual measurement, monitoring, and data sharing capability of root zone performance, in cooperation with RSSAC and other root zone management participants to define the specific measurements, monitoring,

and data sharing framework.

- **Board Action:** The Board formally asked RSSAC for its advice on this topic and an update on plans to satisfy this recommendation. The Board also asked the CEO whether there are other parties who should be consulted, and to ask such parties to participate.

- **Implementation Status:**

  1) In response to a letter to the SSAC from the ICANN Chairman dated 25 September 2012 (http://www.icann.org/en/news/correspondence/crocker-to-murai-larson-25sep12-en), on 18 October 2012, Matt Larson, SSAC Vice Chairman acknowledged the receipt of the Board request, and requested RSSAC form a work party to collect the existing measurements used by the root server operators and determine, along with ICANN staff, the appropriate parties to participate on the task. As a result, the RSSAC work party prepared a document entitled "Recommendation on Measurement of Root Server System" dated 16 April 2013. Currently, it is in last call for comments by the RSSAC. ***[ONGOING]***

  2) In addition to the RSSAC effort, on 7 December 2012 ICANN published Root Zone Scaling Measurements at L-root" that describes the planned measurements, and includes a timeline for implementation for L-root. Trending data is published for L-root at: http://dns.icann.org/services/root-zone-scaling-report-zone-contents/

  http://dns.icann.org/services/root-zone-scaling-root-zone-system/

  The announcements of the reports and the reports can be found:

  http://www.icann.org/en/news/announcements/announcement-3-07dec12-en.htm

  [ONGOING]

SSAC Recommendation 5: ICANN should commission and incent interdisciplinary studies of security and stability implications from expanding the root zone more than an order of magnitude, particularly for enterprises and other user communities who may implement strong assumptions about the number of TLDs or use local TLDs that may conflict with future allocations.

- **Board Action:** The Board formally requested SSAC for its advice on how interdisciplinary studies of security and stability implications from expanding the root zone more than an order of magnitude should be carried out and whom else should be consulted, and tasked staff with formulating and executing one or more studies, as needed.

- **Implementation:** After submission of a letter to the SSAC from the ICANN Chairman on 25 September 2012 (http://www.icann.org/en/news/correspondence/crocker-to-faltstrom-25sep12-en), the SSAC formed a work party to provide a response to the ICANN Board. On 16 April 2013, the SSAC submitted the requested clarifications to the ICANN Board. ***[ONGOING]***

SAC 057: Internal Name Certificates

On 31 January 2013, ICANN security team received SAC 057: SSAC Advisory on Internal Name Certificates. SAC 057 recommended that the ICANN Security Team immediately develop and execute a risk management plan to address the internal name certificates issue. To this end, ICANN has taken the following recommended steps:

1. ICANN worked with the Certificate Authority Browser Forum (CA/B Forum), which passed Ballot 96 at its annual meeting to address the concern. Ballot 96 calls for Certification Authorities (CAs) to stop issuing certificates that end in an applied-for-gTLD string within 30 days of ICANN signing the contract with the registry operator, and revoke any existing certificates within 120 days of ICANN signing the contract with the registry operator. ***[COMPLETED]***

2. ICANN developed and published a coordinated disclosure policy on 11 March 2013 based on industry best practices (http://www.icann.org/en/about/staff/security/vulnerability-disclosure-11mar13-en.pdf). ***[COMPLETED]***

3. On 15 March 2013, ICANN notified new gTLD applicants and browser vendors about the potential issues with internal name certificates, and further discussed the issue during public sessions at the ICANN Beijing meeting 7-11 April 2013. ***[COMPLETED]***

4. ICANN developed a notification service to CAs and browser vendors alerting them of the applied-for-gTLD strings as well as contracting milestone for each string. ***[COMPLETED]***

ICANN intends to take the following actions to address residual risks that may remain with the internal name certificates issue:

5. Work with browsers to reach out to CAs who are not on the CA / Browser forum but are in browser's CA certification program. To date, Mozilla has notified all of its CAs of the internal name certificate issue. ICANN is actively working with others. ***[ONGOING]***

6. Work with browser vendors to require CAs to comply with Ballot 96. To date, Mozilla has initiated a process to update its Certificate Policy to require conformance with Ballot 96. Once Mozilla adopts this policy, it applies to all CAs regardless whether they are on CA/Browser forum or not. ICANN is actively working with others. ***[ONGOING]***

7. Work with browser vendors to discuss revocation issues, including scalability to handle Ballot 96 revocations. ***[ONGOING]***

8. Commission a study, through a third party, on the number of invalid queries to the root zone and potential impacts to the applied-for new gTLD strings. In addition, the commissioned study would provide ICANN with recommendations on which strings represent high collision risks and steps ICANN should take moving forward to address these strings. The recommendations will be presented to the Board for acceptance, and once implemented, they will manage and mitigate the concerns expressed by the SSAC. ***[ONGOING]***

Overall, ICANN has taken the appropriate steps to address the SSAC's concerns and to implement the SSAC's recommendations in SAC 046 and SAC 057. While all work is not yet complete it remains a high priority within both the security team and the NewGTLD team to address the concerns the SSAC have raised.

Thank you for your support and advice on these matters, and please let us know if you have any additional advice.

Sincerely,

Jeff Moss
Chief Security Officer