ICANN

Los Angeles Headquarters

12025 Waterfront Drive, Suite 300
Los Angeles, CA 90094-2536
USA

+1 310 301 5800

+1 310 823 8649

20 October 2017

For the attention of
Vice Minister for Policy Coordination (International Affairs)
Ministry of Internal Affairs and Communications
Japan

RE: Postponement of upcoming changes to root zone DNS Security Extensions

Dear Mr. Tominaga Masahiko,

I want to refer to my previous letter to you dated 6 June 2017 related to upcoming changes to root zone DNS Security Extensions (DNSSEC). I am writing to you today to share our recent decision to postpone the cryptographic key change that helps protect the Domain Name System (DNS) which was planned to occur on 11 Oct 2017 (as expressed in my last letter in June).

In my initial correspondence, I explained the importance of the planned change to this crucial security configuration parameter related to the root zone.

The DNS root zone is digitally signed using a security protocol called DNSSEC, which adds a layer of trust on top of the DNS by providing a way to authenticate DNS data. DNSSEC enables network operators to protect their users from a form of malicious attack known as "cache poisoning," that could redirect their users' traffic to an incorrect website to, for example, steal passwords or financial information. DNSSEC deployment is optional and not all network operators have enabled it, but operators who have deployed it could be affected by the upcoming change.

The DNS is organized in a hierarchy and ICANN manages changes to the top-most level of the DNS, known as the root. ICANN also manages the top-most cryptographic key in the DNSSEC protocol, known as the root zone key signing key, or KSK. ICANN will change this key in a process called a key rollover. This is the first time the key will be changed since DNSSEC was enabled in 2010. This change must be widely and carefully coordinated with network operators that have enabled DNSSEC to ensure that the rollover does not interfere with normal operations.

Some recently obtained data shows that a significant number of resolvers used by Internet Service Providers (ISPs) and Network Operators are not yet ready for the Key Rollover.

Because the security, stability and resiliency of the domain name system is ICANN's foremost responsibility towards the global Internet community, the organization decided to delay the rollover. We announced the delay on 27 September (https://www.icann.org/news/announcement-2017-09-27-en).

A new date for the Key Roll has not yet been determined but we are considering rescheduling it during the first quarter of 2018.

ICANN is informing you about the delay so you can encourage Internet operators and user communities in your country to use this additional time to be certain that their systems are ready for the Key Roll. If an operator fails to update systems with the new KSK, end users in your country could encounter errors when using the domain name system.

We encourage you to share the information related to the postponement of the KSK rollover and ICANN's testing platform as an easy way for your operators to confirm their infrastructure is ready to handle the rollover. The testing platform can be found at https://go.icann.org/KSKtest.

Approximately 750 million people are on DNSSEC deployed networks and we want to make sure as few as possible are affected by the KSK rollover worldwide. It is critical that we coordinate our efforts to keep the Internet users in your country from experiencing difficulties with domain name lookups.

If you or your operators have any questions, you can contact my team by emailing globalsupport@icann.org with the subject line "KSK Rollover."

Thank you in advance for your support,

Göran Marby
President & CEO, ICANN
cc: ICANN Governmental Advisory Committee (GAC) Representatives