

# Comments on the Accountability and Transparency of ICANN

----by Internet Society of China

We appreciate ICANN's improvements on accountability and transparency with efforts and progresses such as encouraging wide participation from various Internet communities in the process of policy-making, seeking public comments on policy documents, posting the Board meeting transcripts online, etc. We consider that it is those measures and actions on accountability and transparency which makes ICANN as an organization recognized by global Internet community. However, as Internet plays an increasing important role in every aspects of the social life, to maintain a secured, stable and unified Internet is the basic need for global Internet community. It is noticed that ICANN had been conducting review process on accountability and transparency by means of case study, and inviting communities to provide comments. We propose that the following cases could be studied to enhance the

accountability and transparency and to promote the voluntary participation of Internet community in ICANN-related activities.

## I. Language Synchronization

### 1. Translation of Documents

ICANN claims itself as a multi-stakeholder body which is transparent and accountable to all the stakeholders. However, it is very disappointing that many important documents, such as DAG v4, latest annual report and ICANN bylaw, are merely in English version, while the Chinese versions are seldom produced. It has been always inconvenient for the Chinese-speaking Internet community to get involve in ICANN-related activities. Furthermore, this problem impedes contribution made by the Chinese-speaking Internet community for ICANN processes.

### 2. Simultaneous Interpretation for Meetings

Taking ICANN public meeting in Brussels for example, the simultaneous interpretation service was provided in French and Spanish, but not including Chinese. In most of AC/SO meetings, English is the only working language.

### 3. Website Multilingualization

ICANN is making efforts to provide multilingual content on its website. Nevertheless, the translated web pages account

for very small amount. And it is far from covering all the pages and contents on the website. At present, the Chinese Internet users already exceed 400 million. ICANN should maintain real-time contents and services in Chinese on its website for Chinese-speaking community to follow and join in ICANN processes.

## II. IANA Contract

As Internet is global applicable infrastructure, ICANN manages Internet resources including IP addresses, domain names, and protocols and parameters. ICANN should be accountable to and overseen by all countries and stakeholders around the globe.

But when it comes to the performing of IANA function, the practice that ICANN submits reports to one government authority tremendously undermines its accountability and transparency<sup>1</sup>. C 3.1 to C 3.3 in the IANA contract defines ICANN submits a set of reports concerning management of

---

<sup>1</sup> IANA Contract C.3.1 to C.3.2 :

C.3.1 Monthly Performance Progress Report -- The Contractor shall prepare and submit to the Contracting Officer and COTR a performance progress report every month (no later than 15 calendar days following the end of each month) that contains statistical and narrative information on the performance of the IANA functions (i.e., assignment of technical protocol parameters; administrative functions associated with root zone management; and allocation of internet numbering resources) during the previous 30-day period.

C.3.2 Audit Data -- The Contractor shall generate and retain security process audit record data for one year and provide an annual audit report to the Contracting Officer and the COTR. Specific audit record data will be provided to the Contracting Officer and COTR upon request. All root operations shall be included in the audit, and records on modifications to the root zone file shall be retained for a period of at least one year.

C.3.3 Final Report -- The Contractor shall prepare and submit a final report on the performance of the IANA functions that documents standard operating procedures, including a description of the techniques, methods, software, and tools employed in the performance of the IANA functions. This report shall be submitted to the Contracting Officer and the COTR no later than 30 days after expiration of the purchase order.

Internet resources to one country. The IANA contract also stipulates that it does not authorize modifications, additions, or deletions to the root zone file or associated information. On this matter, Amendment 11 of the Cooperative Agreement NCR-9218742 prevails<sup>2</sup>.

Under IANA contract, ICANN can not guarantee accountability to all countries and stakeholders. The existence of IANA contract eliminates the possibility that ICANN can be fully accountable and transparent. Accordingly, the IANA contract should be a case study in the review process.

### III. The Deployment of DNSSEC

The deployment of DNSSEC needs a large amount of investment to upgrade the DNS servers, while the well-known experts in the community indicate that the deployment of DNSSEC solves nothing more than a part of security issues<sup>3</sup>. Without fully soliciting the views of the industry and the stakeholders, ICANN made the decision to deploy DNSSEC and determined the timeline accordingly. Therefore, the deployment

---

<sup>2</sup> <http://www.icann.org/en/nsi/coopagmt-amend11-07oct98.htm>

<sup>3</sup> Steve Crocker, co-chair of ICANN's DNSSEC deployment initiative and chair of the Security and Stability Advisory Committee, said on the 38th ICANN meeting. "There are two very broad classes of threats. One is that the information is going to be modified or corrupted. And the other is that the systems are going to be made unavailable by denial of service attacks. So if you take those two pairs and, you know, all the combinations, DNSSEC closes big holes in one-quarter of that space, that is, it protects the information during the lookup side. It does not do anything to protect the information about being put in. If incorrect information is put into the system or is modified at registration, then you're in trouble. And in either case, if the registration side or the lookup side is attacked from a denial of service attack or taken down in some other way, DNSSEC doesn't help at all."

Dan Kaminsky, expert of the Internet Security, said in the 38th ICANN Meeting: "Microsoft's New Zealand operations get hijacked; Comcast, one of the large ISPs in the United States, whose domain name get hijacked. They all get hijacked from the registrar side"

of DNSSEC causes ICANN to lose credibility and face great challenges in accountability and transparency.

The trust mechanism of DNSSEC starts from Root Zone and achieves by the top-down signing authentication from father zone to son zone so as to form the Authentication Chain. Once the Root Name Server performs as the single and exclusive trust source, Root Name Server will become the Trust Anchor of all name servers. The Key Signing Key (KSK) and the Zone Signing Key (ZSK) of the Root Zone play crucial roles in the authentication of DNSSEC signing. Therefore, it is quite important to keep the procedure and process of issuing, managing, changing and distributing the KSK and ZSK of Root Zone accountable and transparent.

*DNSSEC Practice Statement for the Root Zone KSK operator*<sup>4</sup> and *DNSSEC Practice Statement for the Root Zone ZSK operator*<sup>5</sup> stipulate that ICANN and VeriSign are responsible for issuing, managing, changing and distributing of KSK and ZSK respectively. The two documents also state that ICANN and VeriSign on behalf of one government authority perform the said functions and execute its requests unconditionally. Currently, DNS system has become the Internet

---

<sup>4</sup> <http://www.root-dnssec.org/wp-content/uploads/2010/06/icann-dps-00.txt>

<sup>5</sup> <http://www.root-dnssec.org/wp-content/uploads/2010/06/vrsn-dps-00.txt>

infrastructure worldwide; this arrangement greatly damages the accountability and transparency of ICANN. Thus, it is necessary to add the deployment of DNSSEC as a case study in order to make up the deficiency of ICANN in accountability and transparency and make improvement.