**WTPF-IEG/3/7**

Dear Mr. Kantchev,

Thank you for the opportunity to comment on the “Fourth Draft of the Secretary-General’s Report for the Fifth World Telecommunication/Information and Communication Technologies Policy Forum 2013.”

In the attached Annex please find comments on the third draft of the Secretary General’s report to the WTPF’13. Thank you for your consideration of these comments.

Sincerely,

Hascall Sharp

Director, Technology Policy & Internet Governance

**WTPF-IEG/3/7**

**Annex 1**

**2.3.4.1. c)**

Proposal: Replace 2.3.4.1 c) with the following text

Reason: Provide more clarity and additional references to the RFCs.

c) As specified by IETF (RFC3761), ENUM defines a method for entering telephone numbers based on Recommendation E.164 into the Internet’s DNS[109]. Following the direction of the Internet Architecture Board (IAB) and IETF, IANA delegated a specific zone under the .arpa gTLD, namely "e164.arpa", for use by ENUM. Consistent with *recognizing (a)* of Resolution 133 (Guadalajara, 2010) the IAB, ITU-T and RIPE NCC established a procedure for review by ITU-T of delegations of E.164 Country Codes into e164.arpa[109a][109b].

[109] See <http://www.itu.int/en/ITU-T/inr/enum>.

[109a] See <http://www.ripe.net/data-tools/dns/enum>

[109b] Klensin, J., Ed., and IAB, "The History and Context of Telephone Number Mapping (ENUM) Operational Decisions: Informational Documents Contributed to ITU-T Study Group 2 (SG2)", RFC 3245, March 2002.

**2.3.4.3 b)**

Proposal: Remove this text or move to another section.

Reason: This text does not seem to be relevant to security of DNS. Therefore it should be removed from this section.

**2.3.4.3 c)**

Proposal: Modify c) as follows:

1. The IETF developed a set of Security Extensions to the DNS, known as DNSSEC[[1]](#footnote-1), to provide origin authentication and validation of integrity of DNS data to DNS clients – a mechanism that provides an added layer of assurance that a responding entity (name server) really is what it purports to be.

Reason: Change from passive to active voice, clarifying the source of DNSSEC (IETF). DNSSEC verifies the data and the source of the data, not the responding entity (name server).

**2.3.4.3 d)**

Proposal: Delete last sentence “If any part of the authentication chain breaks due to a response from an unrecognized entity, then the resolution of that address is not achieved.”

Reason: DNSSEC helps verify the origin of the data and its integrity, not the server that responds to the client.

1. DNSSEC Protocol RFC (IETF): RFC 4033, RFC 4034, and RFC 4035. [↑](#footnote-ref-1)