ANNEX 2

Date: **25 January 2018**

Subject **Invitation for comments on Proposed Interim Models for Compliance with ICANN Agreements and Policies in Relation to European Union's General Data Protection Regulation (published 12 January 2018):**

Informal comments by the Secretariat of the Secretariat of the Cybercrime Convention Committee

Against the background expressed in the letter, the Secretariat of the Cybercrime Convention Committee[1] is offering the following comments on the proposed interim models:

General comments

- An ICANN WHOIS policy should state clearly that WHOIS serves "important reasons of public interest". These include, inter alia, public safety and the investigation of crime. This public interest in open access to WHOIS data may override data protection rights of individuals. The Hamilton Memorandum – Part 3 (see section 2.8) provides examples of other public databases and references to case law in this respect. However, any solution needs to be carefully calibrated to ensure that only data necessary to meet the public interest is made public.

- It should be kept in mind that public safety is not a matter of discretion for criminal justice authorities. States have an obligation to protect individuals and their rights including through criminal law provisions allowing for effective investigations and prosecutions (see European Court of Human Rights in K.U. v. Finland). This implies that rules that do not permit to meet public safety needs effectively may raise other legal and policy problems.

- The publication of WHOIS data should thus be designed to be necessary and proportionate to serve specific purposes. Each field should be assessed as to whether it contains personal data and whether public access to such personal data is necessary and proportionate.

- WHOIS data is subscriber information and does not represent traffic data. This distinction is essential. Subscriber information does not "allow very precise conclusions to be drawn concerning the private lives of the persons" as may be the case for traffic data (as argued by the European Court of Justice in relation to data retention rules).

- For non-public WHOIS data, the models propose different layered access solutions. The legal, technical and practical issues related to these solutions would need to be evaluated. For example, access to public WHOIS data by public safety authorities can be considered to be covered by Article 32a Budapest Convention on Cybercrime and

[1] The Cybercrime Convention Committee represents the currently 56 Parties to the Budapest Convention on Cybercrime. Given limited time available it has not been possible to arrive at a formal opinion of this Committee. The present comments have been prepared by the Secretariat following informal consultations with the Parties

this provision is increasingly considered international customary law. It is unclear whether additional domestic or international legal bases are required for access by public safety authorities to non-public databases in other jurisdictions. It remains to be seen whether such issues can be resolved in the short-term.

- From a public safety perspective it is, therefore preferred that, to the extent possible, WHOIS data remain publicly accessible.

Comments on models proposed

- From a public safety perspective, Model 1 is preferred in terms of the fields to be displayed and the two-year retention period. The distinction between natural and legal persons is warranted from data protection and public safety perspectives.

- Some of the fields of Model 1 would need to be discussed in greater detail from both public safety and data protection perspectives (e.g. what is the justification for not displaying the email address of the registrant but the physical address?). And some of the fields currently indicated as "do not display" could be indicated as "display unless field includes personal data" (as in model 3).

- A major shortcoming of Model 1 is that it leaves it to the discretion of the registry or registrar to decide whether or not to respond to a request for non-public data. This model is likely to raise the same type of problems that criminal justice authorities are facing with regard to voluntary cooperation models with other types of service providers (see this report of the T-CY Cloud Evidence Group). Thus the "enforcement solution" proposed in Model 2 where "registries and registrars must [emphasis added] provide 'certified' requestors access to non-public Whois data based on pre-defined criteria and limitations", is more likely to meet public safety needs.

- For the accreditation of legitimate requestors a centralized model with accreditation by ICANN is preferred.

- However, this enforcement solution of Model 2 may raise legal and policy problems as a registrar or registry providing such access directly to "foreign" requestors may violate domestic laws, and such access may be perceived as an infringement of sovereignty by the State hosting the registry or registrar[2].

- The feasibility of a centralized model in which ICANN (rather than individual registries or registrars WHOIS) provides the point of access to non-public WHOIS data could be assessed in future reflections.

- Model 3 is not feasible and would not permit to meet public safety and other important public interests.

[2] This type of issues has been discussed by the Cybercrime Convention Committee through its work on access to cloud evidence for several years. The Committee is currently negotiating a Protocol to the Budapest Convention which is to address, inter alia, the question of direct cooperation with providers in other jurisdictions as well as the question of transborder access to data.