**Briefing paper Incident Response Planning WG**

*Purpose and scope of Incident response planning WG*

The purpose of the incident response planning working group was to assist in implementing sustainable mechanisms for the engagement of and interaction with ccTLD registries during incidents that may impact the DNS. The activities of the WG were limited (scope) to define a repository of ccTLD contacts, use cases and channels of communication for incident response.

*Results/Outcome*

- Definition of incident for the purpose of incident response
- Description of use cases of contact repository i.e. for what purposes can repository be used:
    - Information exchange
    - Counter action
- Definition of contact repository data attributes
- General criteria for implementation and maintenance of repository:
    - Support the envisioned use cases
    - High availability (24/7)
    - Alternative communication channels (not using the internet)
    - Actively Maintain and keep data up-to-date

The WG did not consider implementation, operation and maintenance of the repository as part of its mandate, in particular in view of the organizational, costs and financing issues involved. In order to understand these issues and a model to maintain the repository the working group has been in touch with a potential external provider of the services needed. This provider, Trusted Introducer, supports the trust network for Computer Security Incident Response Teams (CSIRTs) or CERTs in Europe. Their model could be easily adapted to implement and maintain the incident repository as envisioned. However, the estimated costs for this service would be:

- (one time) set up fee of $ 1,300 per participant
- $ 1,400 $ per annum per participant.

The working group notes that several financing models can be envisioned (ranging from full coverage for costs by each participating ccTLD to full coverage by ICANN) and have not been discussed. The working group is of the view that any make or buy decision and service level of the contact repository implementation heavily depends on financing abilities and model.

In the view of the working group, and assuming the need for an incident response repository and its use cases remains to be broadly supported, the following decisions need to be made:

- Who and how will the implementation, operation and maintenance of the incident repository be funded?

- Make („browse“ or „query“ solution (resulting in different look & feel and maintenance models) or buy (select existing, external provider)

*Next steps*

Create a wg to implement incident repository with the purpose to:

1. Explore different funding models and establish preferred option, and report this to the community and council;
2. Explore in detail costs to implement, maintain and operate an incident repository specifically made or already provided (make or buy) and report on this to the ccTLD community and council
3. After conclusion of 1 and 2 and at the explicit request of the ccNSO council:
    - prepare and send out a request for proposal (RfP),
    - review the responses and
    - advise the ccTLD community and ccNSO council a solution

    to implement, maintain and operate incident response repository and propose a provider if