TLD-OPS Standing Committee Charter
Version 2,
Adoption by the ccNSO Council: 21 September 2017

1.   Statement of Purpose: Description and Objective

The TLD-OPS Standing Committee is the oversight body of the TLD-OPS group activities as documented in the scope section below.

The primary purpose of the Standing Committee is to govern the daily operation of the TLD-OPS email list; and, when deemed necessary, to develop and implement progress plans for future improvements and developments of TLD-OPS group activities to enhance security and stability of ccTLDs through cooperation and coordination between members [1].

The TLD-OPS Standing Committee will also expand and contract the scope of activities following discussions with members.

More information on the list is available on the TLD-OPS homepage [2].

2.   Scope

The scope of activities of the TLD-OPS Standing Committee is to do what it deems relevant and necessary to facilitate and improve a smooth running of the TLD-OPS mailing list and on-going development of the TLD-OPS community.

In achieving its objective, the Standing Committee will undertake, but is not limited to, the following activities:

- Mailing list operation: A basic incident response facility that serves as a Contact Repository for ccTLDs. The TLD-OPS list enables ccTLD operators to easily and quickly look up each other's contact information, thus allowing them to better handle incidents that require a coordinated response of ccTLDs at the global level. Examples of these incidents may include targeted attacks on or malfunctions of registration systems, the DNS, or the Internet at large. More information on the list is available on the TLD-OPS homepage [2].

- Decide on which ccTLDs to subscribe to or unsubscribe from the TLD-OPS list in cases where the TLD-OPS validator believes this requires a decision from the standing Committee.

- Advise the TLD-OPS Validator on what action to take on unforeseen issues that arise around the operation of the TLD-OPS email list.

- To co-ordinate, organise and run, Security related workshops, both within ICANN meetings but also by request at other Internet events/organisations. These workshops will be used to develop and disseminate information and experiences of members of TLD-OPS to ensure that attendees benefit from the experiences of others.

- Help to develop a maturity model so that ccTLDs may self assess themselves to gain confidence they may be at an acceptable level of security operations.

- Help to develop high level security frameworks, such that less experienced TLD-OPS members may benefit from the experience of others ensuring that the ccTLD space becomes more secure overall.

- Develop and implement new TLD-OPS policies and technical features in collaboration with the ccTLD community and other stakeholders such as IANA, SSAC, and ICANN's Security Stability Resiliency (SSR) team.

- Work with the TLD-OPS Validator, IANA, SSAC, and SSR to "detect" ccTLDs that have gone through a redelegation and invoke the corresponding procedures.

- Regularly review TLD-OPS processes, system performance, and agreements with contracted service providers, such as the TLD-OPS Hosting Provider. The latter includes the renegotiating of these contracts and if necessary contracting other parties.

- Report to the ccNSO Council, TLD-OPS list members (Security and Stability Contacts of ccTLDs) as well as to the ccTLD community at large on the status and expected development of the TLD-OPS ecosystem.

- Request and manage a budget for the TLD-OPS list should this be required to manage and innovate TLD-OPS.

- Identity work items to further develop the TLD-OPS ecosystem, policies, and technical systems and initiate working groups in collaboration with the ccNSO Council to carry out the work.

3. Chair, Members and Support

The TLD-OPS Standing Committee should represent the global ccTLD incident response community. The Committee should be as small as feasible, however membership should at least meet following requirements:

- At least 3 members should be subscribed as Security and Stability Contacts on the TLD-OPS list.

- At least one member from each of the ICANN regions (AF, AP, EUR, NA, LAC).

- The ccTLD manager Committee members represent, may be members of the ccNSO, but are not required to be so.

After a community-wide call for volunteers, the members will be appointed by the ccNSO Council.

The members of the Committee will nominate a chair, who will then be appointed by the ccNSO Council. If considered appropriate by the Committee, they may also nominate a vice-chair and a secretary, who will then also be appointed by the ccNSO Council.

Once the Committee is established, the chair will invite both SSAC and ICANN's IANA and/or SSR department to each appoint a liaison to the Committee.

In consultation with the members of the Committee, the chair of the Committee may invite observers from other relevant stakeholders, such as DNS operators and ISPs. It is however expected that this will be a more long-term evolution of the Committee.

The members, liaisons, observers of the Committee will be listed on the TLD-OPS homepage [2].

Support is provided by ICANN's ccNSO Support Staff, who will also act as the TLD-OPS Validator, unless the TLD-OPS Standing Committee decides on another arrangement.

4.   Omission/Review of Charter and Activities of the Standing Committee

If this Statement of Purpose does not provide guidance and/or the impact of the Statement of Purpose is unreasonable in conducting the business of the TLD-OPS Standing Committee, the Chair of the Committee will decide on the most appropriate remedy, including suggesting a change of the Purpose Statement. A changed Purpose Statement will only be effective after, it has been adopted by the ccNSO Council and published on the webpage of the Committee.

The TLD-OPS Standing Committee will review the charter whenever necessary and on a regular basis (at least every 2 years).

5.   Reporting

The Chair of the Standing Committee will report regularly through email to the ccNSO Council and will also provide updates to the Community.

References

[1] Final Report of the ccNSO working group "Secure Email Communication for ccTLD Incident Response", August 2015, https://ccnso.icann.org/workinggroups/secir-final-30jun15-en.pdf

[2] TLD-OPS Homepage, http://ccnso.icann.org/resources/tld-ops-secure-communication.htm