Draft Framework for the Registry Operator to Respond to Security Threats
NCSG comment

General observations

The Non-Commercial Stakeholders Group (NCSG) welcomes the opportunity to comment on Draft Framework for the Registry Operator to Respond to Security Threats. We support ICANN effort to address global security threat issue with outlining the response recommendation to threat notifications.

Issues to be addressed

1. Since the following examination of threat report is identified in the Framework, we strongly suggest including a recommendation on Responsible Threat Disclosure to be included in the document:

"Each RO should scrutinize, question or otherwise inquire about the legitimacy of the origin of a request, in accordance with their own internal policies and processes."

We have seen a broad variation in handling security threat reports, varying from constructive actions addressing the issues to punishment of the reporting party. Benefits of responsible threat submission are obvious.
In this context, it is important to underline benefits and importance of responsible threat disclosure. We request recommendation to extend goodwill and not cause harm to the reporting party whenever possible:

When applicable, RO should provide:

- an easy way to report security threats and violation
- encrypted ways of communication
- option of anonymous submission

<u>The following quote is provided for context In order to expand on points 5 and 6:</u>

> "With respect to the safeguards regarding security checks, the NGPC considered that the comments in opposition raise important questions about the costs and timing of implementing this measure, and the scope and framework of the security checks.
>
> The NGPC is mindful that there are various ways a registry operator could implement the required security checks, and has taken these concerns into consideration in its response to the GAC's advice. The NGPC's response directs ICANN to solicit community participation (including conferring with the GAC) in a task force or through a policy development process in the GNSO, as appropriate, to develop the framework for Registry

> Operators to respond to identified security risks that pose an actual risk of harm, notification procedures, and appropriate consequences, including a process for suspending domain names until the matter is resolved, while respecting privacy and confidentiality.
>
> The proposed implementation of the GAC's advice is phased to account for the commenters' concerns. The proposed language in the PIC Specification will provide the general guidelines for what registry operators must do, but omits the specific details from the contractual language to allow for the future development and evolution of the parameters for conducting security checks."

2. Framework serves to help operators respond to identified security risks. The Framework is not intended as detailed in-depth manual. However, for these purposes, we suggest Framework documentation to be expanded by building on technical part as follows:

- Providing specific examples of the most common threats
- Connecting listed actions to the use cases

3. Also request for "respecting privacy and confidentiality" is not clearly addressed within the proposed Framework.

Conclusions

Overall we recognize the Framework as very welcome initiative. At the moment the Framework is not ready for publication, but is a work in progress that needs more elaboration and clarification. The information in insufficient within the intended scope.

We thank SFDT for conducting a public comment for broader community feedback prior to finalization of the Framework, even though it was not required. We are looking forward to addressing the points of this comment.