ICANN 57: Summary of High Interest Topic Cross-Community Session – Mitigation of Abuse in gTLDs

To follow is a summary of the High Interest Topic (HIT) session held at ICANN57, Hyderabad (on Saturday 5 November, 2016).

This summary has been prepared by the independent ACIG GAC Secretariat, for the information of ICANN’s Governmental Advisory Committee (GAC).

It is not a formal record of the meeting.


Panellists

GAC Representatives who are interested in finding out more about this topic may wish to approach the session panellists.

**Session Chaired by** Alice Munyua, African Union Commission GAC Representative, PSWG co-Chair

**Discussion Moderated by** Robert Flaim, GAC PSWG Member, Executive Office Liaison, Science and Technology Branch Executive Office Federal Bureau of Investigation, United States of America

**Abuse of the DNS:**

- Robert Flaim (GAC PSWG, US FBI)
- Drew Bagley (Secure Domain Foundation)

**Mitigation of Abuse - Current industry practices:**

- ICANN - Allen Grogan, Carlos Alvarez (SSR)
- gTLD Registries: Brian Cimbolic (PIR), and Statton Hammock (Rightside)
- ccTLD Registries: Giovanni Seppia (EURid, .eu)
- Registrars: Michele Neylon (Blacknight)
- Business: Denise Michel (Facebook)

**Summary of Discussions**

Throughout the session, participants shared information and views. No formal position, or possible next steps (action items), were agreed or discussed.

Some of the challenges discussed included:
• The difficulty of defining DNS abuse. Abuse takes many different forms and no single, agreed definition exists. Lacks even a common vocabulary.

• DNS abuse has enormous financial implications – examples include ransomware and business email compromise. Potentially more than a billion dollars in losses.

• Ongoing community debate about ICANN’s role in combating abuse.

• Registries and Registrars lack uniform abuse mitigation policies – much variation between them in terms of how strict they are.

• Reports of DNS abuse often lack clarity.

• Lack of relevant international laws means legal jurisdiction is often unclear.

• The system fails if Registrars fail to undertake basic verification at the point of registration.

Some of the approaches to preventing and mitigating DNS abuse included:

• Increased sharing of information about ‘bad’ WHOIS data between Registries and Registrars may mitigate some forms of abuse. Some sharing occurs currently, but only on an informal basis.

• Overview of ICANN’s activities, including ‘expedited registry security requests’; outreach; and the provision of training to law enforcement agencies.

• Systems are in place to flag unusual registration patterns.

• Outreach by Registries to Registrars, and by Registrars to Registrants, although there is much variation in policies.

• Technical protections around IDNs, to prevent lookalike registrations.

• Important to have education, co-operation and dialogue among all stakeholders.

**Document Administration**

<table>
<thead>
<tr>
<th>Title</th>
<th>Summary of High Interest Topic (HiT) – Mitigation of Abuse in gTLDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>GAC Brief No.</td>
<td>16-142</td>
</tr>
<tr>
<td>Distribution</td>
<td>GAC</td>
</tr>
<tr>
<td>Distribution Date</td>
<td>13/12/16</td>
</tr>
</tbody>
</table>