REQUEST INFORMATION	
Title of Proposed Pilot Project	DNS Abuse – The End-User Perspective
Community Requestor Name	**Chair**
ALAC – At-Large Advisory Committee	Maureen Hilyard
ICANN Staff Community Liaison	
TBC	

REQUEST DESCRIPTION
Purpose: To facilitate advisory activities by ALAC in the area of DNS abuse

ICANN's mission is to ensure the stable and secure operation of the Internet's unique identifier systems, including the Domain Name System (DNS), and which it carries out by ensuring the operational stability of a critical, shared global resource.

Since 2013 and more so in recent years, the ICANN community has seen, raised and continue to experience and combat activities and behaviours that threaten the stability, security and resilience, and by extension, the viability of a single, trusted, interoperable DNS.

The GAC in its 2013 Beijing Communique identified several DNS security threats in its advice the ICANN Board which led to the incorporation of provisions into the base Registry Agreement in the form of Section 3(b) of Specification 11. ICANN Org has also implemented 2 initiatives in an effort to understand security threats which impact the DNS; these being the Domain Abuse Activity Reporting (DAAR) project and the Contractual Compliance Audit Program.

The Competition, Consumer Choice and Consumer Trust Review Final Report of 2018 included a lengthy chapter on DNS infrastructure abuse and recommendations, some of which are still being contemplated. According to the review of the last round of new TLDs by the CCT Review Team, the safeguards put in place during the last round were not effective, and the compliance operation within ICANN does not have the necessary mandate nor probably the ideal tools to combat DNS Abuse effectively. Discussions continue about how to define DNS Abuse, but there are also settled consensus definitions that could be employed for immediate reform - not to regulate content, but to exercise enforceability against DNS Abuse.

As recently as ICANN66 in Montreal, the At-Large Community organized a policy session on "DNS Abuse – End User Concerns", with a panel presentation by Drew Bagley, Secure Domain Foundation / CrowdStrike and Graeme Bunton, Chair, Registrar Stakeholder Group, during which we summarized how At-Large can enhance Internet end user protection against DNS Abuse.

At-Large believes DNS Abuse is one of the biggest challenges faced by individual Internet end users and remains a key factor eroding confidence in a single, trusted, interoperable Internet. Systemic abuse is a persistent problem. In taking on the important fight against DNS Abuse from the end-users' perspective, it is timely for the ALAC to undertake this pilot project with the goal of facilitating and enhancing the effectiveness and efficiency of the At-Large's performance of its

advisory work and participation in ICANN policy and technical work in this area. It is a pilot project which is not budgeted for in FY2020.

Scope: Capacity Building - Research/Study, Training/ICANN Learn; Outreach & Engagement

This pilot project primarily touches on the following strategic goals outlined in the Draft FY21-25 Strategic Plan:

1. Strengthen the security of the Domain Name System and the DNS Root Server System
- While technical aspects of DNA Abuse may be best explored by SSAC (for eg), we should not discount the end-users' perspectives on what end-users opine makes the DNS secure

2. Improve the effectiveness of ICANN's multi-stakeholder model of governance
- Capacity building for facilitating and enhancing the effectiveness and efficiency of the At-Large's performance of its advisory work and participation in ICANN policy and technical work in this area

3. Evolve the unique identifier systems to continue to serve the needs of the global Internet user base
- The global Internet user base is best served with the maintenance of a trusted unique identifier systems, thus it is in the global public interest to keep all forms of DNS abuses in check
- Forms of DNS abuses (have and) can foreseeably evolve over time – it is crucial to monitor and analyse developments in this area

4. Address geopolitical issues impacting ICANN's mission to ensure a single and globally interoperable Internet
- The proliferation of DNS Abuse – if not kept in check – may well lead to 'justified' fragmentation of the Internet which in turn runs counter to ICANN's mission to ensure a single and globally interoperable Internet

It is expected to comprise a broad-based education/awareness aspect as well as a data collection element, involving and/or addressing:
- An analysis/review of existing materials pointing to the current consensus definitions of DNS Abuse, from which to draw up a layperson's description of such abuses
- Reliance on not only At-Large Structures (ALSes) but also other partners and interested parties for outreach and engagement on the topic
- A survey, then onward analysis, of regular Internet end-users' understanding and knowledge of such consensus definitions, frequency of incidence, challenges in taking action etc
- Call for reports of 'severe' DNS abuse cases – party involved, role of law enforcement, method of resolution (if any)
- A determination, with recommendations (where possible), on whether an amendment (or evolution) of the current consensus definitions of DNS Abuse is needed
- Current as well as downstream capacity building (in the form of training, ICANN Learn course) to not only increase At-Large expertise in the area but also to improve general awareness of end-users in this topic

Proposed Timelines/Schedule: 12months
- Pilot project detailed timeline to be developed under the direction of the ALAC

Resources Required: Consultancy, translation services, web services

Under the direction of the ALAC,

- <u>Consultancy</u> for various aspects of the pilot project, including:
    - o Review of current consensus definitions of DNS Abuse to draw up a layperson's description
    - o Strategy formulation – to cover a sufficiently wide scope of inquiry to include the current consensus definitions to test awareness and identify incidences of DNS Abuse, especially of DNS infrastructure abuse, but excluding regulation of content
    - o Selection of location and ideal numbers of target respondents – eg in not more than 3 countries across each of the 5 ICANN regions, and based criteria such as size of population, Internet penetration rates, number of Registry Operators and Registrars
    - o Selection and development of data collection tools – eg survey
    - o Retention, storage and presentation of collected data – eg portal or website
    - o Data analysis, drawing of conclusions, reporting, recommendations
- <u>Translations services</u> – for data collection tool (as required) and reports
- <u>Web services</u> – for portal or website & data capture/repository development/hosting
- <u>Training services</u> – for downstream training, ICANN Learn

Estimated Cost: USD500,000.00 (TBC)

- Breakdown of costs is subject to negotiation with contractors

Deliverables: TBD

- While the nature of final deliverables is to be determined with consultant(s), we envisage these **must include**:
- (1) A manual-like document describing the pilot project, tools and methodology used in implementing the pilot, as well as in analysing and reporting on the data collected;
- (2) Retention, storing and presentation of the data collected in some easily accessible form; and
- (3) A report on the findings on which to base ALAC's preliminary advisory on the topic.

Success Metrics:

- A rate of response which allows reasonable conclusion(s) to be drawn for each target region
- Each of the deliverables mentioned above