ICANN BUSINESS CONSTITUENCY

October 28, 2019

ICANN Board of Directors

Goran Marby, ICANN President and CEO

Keith Drazek, GNSO Council Chair

ICANN Community

Dear Colleagues:

Domain Name System abuse and security threats are critical public policy issues, as is the ICANN community's role in addressing and mitigating them effectively. As such, the Business Constituency (BC) welcomes the heightened attention given this important matter and looks forward to what we hope will be a robust and productive conversation about DNS abuse at ICANN66.

Accordingly, the BC submits the attached for the broader community's consideration prior to our meeting in Montreal. Our remarks represent the BC's current position on the many aspects of domain name abuse, our aspirations regarding the community's exchanges, and our specific requests. Via this communication, we hope to contribute in advance to a useful and informed community discussion.

Thank you for your consideration of these remarks.

Sincerely,

ICANN Business Constituency

ICANN BUSINESS CONSTITUENCY

Statement Regarding Community Discussion on DNS Abuse

ICANN's Business Constituency (BC) thanks ICANN Org and the community for discussions thus far regarding the issue of DNS abuse. The purpose of this statement is to contribute, in advance, to the framing of and our participation in the planned discussion of this issue at ICANN66. We look forward to the opportunity to constructively engage on this topic.

As the Governmental Advisory Committee (GAC) recently said about the importance of addressing DNS abuse, "Protecting the public from security threats and DNS Abuse is an important public policy issue." The BC concurs, and urges the community to take a proactive footing toward combating this increasing problem.

In that light, while the BC appreciates the need for actionable definitions of abuse, we are concerned about recent efforts to limit or otherwise over-restrict discussion about the serious issue of domain name system abuse. Such a subject deserves fulsome consideration by the entire community -- we therefore outline our requests, with additional context and background to follow.

BC statements and requests

- ICANN has a responsibility to enforce its contracts in the areas of DNS-related abuse. This community dialogue cannot delay or defer ICANN's commitments or operations related to DNS abuse.
- The BC encourages a definition of abuse that is not artificially restricted to the functioning of the DNS infrastructure.
- A PDP is unnecessary because the GNSO has already produced consensus definitions of "abuse" and "malicious use of domain names" that are appropriately more expansive. According to that definition, "abuse" is an action that:
    - Causes actual and substantial harm, or is a material predicate of such harm; and
    - Is illegal or illegitimate, or is otherwise considered contrary to the intention and design of a stated legitimate purpose, if such a purpose is disclosed.

  The GNSO also recognized that "malicious use of domain names" include, *but are not limited to*:
    - Spam
    - Malware distribution
    - Online child sexual exploitation and imagery abuse
    - Phishing
    - Botnet command-and-control
- ICANN should clarify the purposes and applications of "abuse" before further work is done to define DNS abuse.
- Once those purposes are identified, ICANN should determine whether abuse definitions used by outside sources can serve as references for the ICANN community, or whether a new, outcomes-based nomenclature could be useful (including impersonation, fraud, or other types of abuse) to accurately describe problems being addressed.
- While endorsing the adoption and use of registry and registrar best practices, as outlined in the recent webinar on the subject of abuse, the BC supports stronger contractual obligations related to DNS abuse, in order to ensure they apply to all registrars and registries.

- The BC further underlines its support for recommendations from the Competition, Consumer Trust and Consumer Choice Review Team (CCTRT) recommendations in the area of abuse, particularly Recommendation 15.[1]
- ICANN should collect and post more abuse-related data (i.e. DAAR) and update that work as abuse definitions evolve to keep pace with abuse involving the internet's unique identifier system.
- Because the issue of abuse falls squarely into the remit of the Security and Stability Advisory Committee (SSAC) and the GAC, the ICANN Board should seek advice from those two bodies about building on the GNSO's existing definitions, or about any questions generally regarding the definition of DNS abuse, and how contracts with registries and registrars can be strengthened to fight DNS abuse.
- Input from the SSAC and GAC (via the Public Safety Working Group) should form the basis of advisories to be issued by ICANN Org regarding interpretation and enforcement of existing contractual provisions.

Context

The implementation of the European Union's General Data Protection Regulation (GDPR) has driven an increase in the incidences of DNS abuse, as it has become severely problematic to leverage Whois and/or other parts of the DNS for the purpose of mitigating abusive behavior.

Increases in abuse are well documented and, regrettably, show no signs of abating, so long as investigatory capability is hampered and DNS coordinators do not widen their engagement in combating them:

- The global cost of cybercrime is rising, and reached an estimated $600 billion in 2018, according to the Center for Strategic and International Studies, in partnership with McAfee.
- The Anti-Phishing Working Group (APWG) reported a total number of detected phishing sites in the second quarter of 2019 of 182,465, up sharply from the 138,328 reported in the fourth quarter of 2018.
- Akamai reports a strong uptick in phishing attacks against consumers.
- Global insurance giant AIG reports that phishing attacks have now outpaced ransomware as the most frequent instances of fraud, alarming the business community and security experts.

DNS abuse has not gone without community notice. ICANN Org has facilitated at least three separate discussions on abuse in 2019, and there is a major cross-community discussion scheduled for ICANN66 in Montreal.

Abuse has occupied the community's attention for many years, even preceding GDPR; more recently, however, discussions on the subject have become more urgent:

- The community concluded, in 2010, a wide-ranging and comprehensive review of DNS abuse as a topic, producing a final report that would be useful as building blocks for the current discussion (particularly in the realm of definitions of abuse).
- The PSWG conducted comprehensive sessions at ICANN57 (Hyderabad), ICANN58 (Copenhagen) and ICANN60 (Abu Dhabi), including cross-community discussions.

[1] Recommendation 15 states: ICANN Org should, in its discussions with registrars and registries, negotiate amendments to the Registrar Accreditation Agreement and Registry Agreements to include provisions aimed at preventing systematic use of specific registrars or registries for DNS Security Abuse. With a view to implementing this recommendation as early as possible, and provided this can be done, then this could be brought into effect by a contractual amendment through the bilateral review of the Agreements. In particular, ICANN should establish thresholds of abuse at which compliance inquiries are automatically triggered, with a higher threshold at which registrars and registries are presumed to be in default of their agreements. If the community determines that ICANN org itself is ill-suited or unable to enforce such provisions, a DNS Abuse Dispute Resolution Policy (DADRP) should be considered as an additional means to enforce policies and deter against DNS Security Abuse. Furthermore, defining and identifying DNS Security Abuse is inherently complex and would benefit from analysis by the community, and thus we specifically recommend that the ICANN Board prioritize and support community work in this area to enhance safeguards and trust due to the negative impact of DNS Security Abuse on consumers and other users of the Internet.

- Between 2015-2017, registries, registrars, the GAC and ICANN Org responded to community concern by developing a Framework for Registry Operator's Response to Security Threats. However, these voluntary measures, likely formulated as a demonstration of self-policing, while welcomed, are narrowly focused, and their effectiveness is unmeasured.
- Further, the Competition, Consumer Trust and Consumer Choice Review Team (CCTRT) made a specific recommendation (#19) in its 2018 final report -- specifically, that the next CCTRT should review the registry framework to assess whether it is a "clear and effective mechanism" for mitigation of abuse.
- The GAC, in its most recent communication, urged the community to adopt the CCTRT's and others' recommendations for addressing DNS abuse.

While ICANN Org has contributed to the discussion (for example, with the introduction of DAAR), much work remains to be done. In the aggregate, ICANN Org and the community have worked on the fringes of abuse mitigation but have yet to meaningfully address it with impactful action. Accordingly, abuse has been -- and still is -- very much on the mind of the community, and must be addressed through contractual revisions (as recommended by the CCT Review Team and the Registration Directory Services (RDS) Review Team), as well as with enhanced enforcement of the existing language in the contracts.

The BC looks forward to contributing to these discussions in Montreal.

--

This statement was drafted by Mason Cole, Claudia Martinuzzi, Denise Michel, Chris Wilson, John Berard, Fred Felman, Ben Wallis, Statton Hammock, and Tola Sogbesan.

It was approved in accord with the BC Charter.