BUSINESS CONSTITUENCY

13 February 2026

BACKGROUND

This document provides input from the ICANN Business Constituency (BC), from the perspective of business users and registrants. The BC is the representative body within the Internet Corporation for Assigned Names and Numbers (ICANN) for business users of the internet and advocates for authoritative policy that promotes end-user confidence in internet-based commerce and prevents fraud and abuse.

BC COMMENT

The BC strongly supports the Commission's intention to develop an action plan to combat online fraud. The BC has been a vocal advocate for anti-fraud and -abuse measures as a way to help prevent reputational and financial injury to the businesses we represent and to those businesses' customers.

The following observation by the Commission is correct:

> *"abuse of the Domain Name System (DNS) is often how online fraud is committed. However, phenomena such as phishing, farming, botnet attacks and spam distribution are also growing in scale and frequency."*

We're pleased that participants in the ICANN policymaking process have begun to address these forms of DNS abuse. However, the BC remains very concerned that:

- ICANN's definitions of what constitute DNS abuse soon will be or already are inadequate in terms of recognizing other, rapidly developing forms of abuse, which are going unaddressed;
- ICANN's policymaking procedures are too slow and cumbersome and thus are incapable of dealing with abuse vectors that develop and strike quickly; and
- The application of artificial intelligence (AI) will intensify the frequency and sophistication of abuse.

Accordingly, the BC is in favor of the proposed action plan. While ICANN remains ideally positioned as the internationally recognized steward of the domain name system, it has become more apparent in recent months and years that ICANN's efforts must be supplemented by anti-abuse measures from governments and other authorities.

Accordingly, the BC is grateful to see the type of cross-border cooperation aimed at "increasing efficiency at every stage of the anti-fraud cycle by supporting complementarity between anti-fraud actors in the prevention, detection, investigation, correction and prosecution of fraud". The BC also concurs with identified problems 6 and 7, which indicate:

- “current efforts to combat online fraud suffer from a lack of coordination and collaboration between the various public and private-sector stakeholders involved”; and
- “relevant information is not necessarily shared between the private sector and public authorities, making it more difficult to identify and prosecute fraudsters, conduct investigations and carry out effective prevention.”

Therefore, it is critical that authorities with stakes in the safety and stability of online infrastructure, such as the DNS, assertively move forward in a coordinated and cooperative manner to deal with the rising tide of fraud and abuse. The Commission’s proposal for an action plan is a worthy step in such a process.

The BC also has identified, in various fora, the need for DNS operators to adhere to the tenets of Article 28 of the NIS2 Directive. Since the advent of GDPR, a critical investigatory tool – the database of domain name registrant data (also known as “WHOIS” data) – has been sidelined. Article 28 intends to reverse that unintended consequence by liberalizing access in a manner that is consistent with EU privacy law.

The BC accordingly strongly supports the intention in Article 28 to permit legitimate requestors (IP right holders, law enforcement agencies, consumer and child protection investigators etc.) to access accurate domain name registrant data. However, to date, most Member States have not, or have not correctly, implemented Article 28. Further, despite NIS2 mandating TLD name registries and entities providing domain name registration services to ensure the accuracy, completeness, and accessibility to legitimate access seekers of domain name registration data, legitimate requests are routinely ignored, or refused.

The BC calls on the Commission to move forward decisively with a framework of anti-abuse and -fraud measures that will help combat this growing online threat.

Thank you for the opportunity to comment.