RySG Submission on the European Commission Consultation on *Fighting Online Fraud - Action Plan*

13 February, 2026

The gTLD Registries Stakeholder Group (RySG) welcomes the opportunity to comment on the European Commission's initiative *Fighting Online Fraud – Action Plan* (Ref. Ares(2026)783547 - 23/01/2026).

The RySG shares the European Commission's commitment to addressing DNS Abuse and focuses this submission on outlining intricacies of the topic of DNS Abuse and on DNS Abuse mitigation actions available to top-level domain (TLD) registry operators. Understanding the role of registries in the Internet ecosystem and in DNS Abuse mitigation supports effective and proportionate measures in the future Union-level counter-fraud frameworks.

About the RySG

The gTLD Registries Stakeholder Group (RySG) is a part of the Internet Corporation for Assigned Names and Numbers (ICANN) community. Our role is to represent the interests of generic top-level domain (gTLD) registries who are currently under contract with ICANN to provide gTLD Registry Services. As gTLD registry operators, RySG members provide important internet infrastructure and domain name registry services and enable internet navigation for gTLDs, including some of the world's largest.

The RySG is committed to engaging in ICANN policy development and other collaborative efforts to address DNS Abuse at the registry level, and to contribute to a secure, stable, and resilient DNS and internet.

Defining DNS Abuse

A secure, safe, and reliable Domain Name System (DNS) is critical for a secure and safe internet experience – something that is becoming increasingly critical as more of our daily lives move to the digital world. While different stakeholders may have different perspectives on how to define "DNS Abuse," the ICANN community has reached a consensus definition of this phrase. It is important to understand this definition in the context of other types of harms that fall under the broader category of abuse via the DNS[1], namely illegal and abusive content.

- **DNS Abuse:** defined as being "composed of five broad categories of harmful activity [where] they intersect with the DNS: malware, botnets, phishing, pharming, and spam when [spam] serves as a delivery mechanism for those other forms of DNS Abuse."
- **Illegal Content:** content that is unlawful and hosted on websites that are accessed via domain names in the global DNS. Examples might include the illegal sale of controlled substances or the distribution of child sexual abuse material (CSAM), and proven intellectual property infringement.
- **Abusive Content:** is content hosted on websites using the domain name infrastructure that is deemed "harmful," either under applicable law or norms, which could include scams, fraud, misinformation, or intellectual property infringement, where illegality has yet to be established by a court of competent jurisdiction.

The distinction between different types of abuse is critical to understanding and effectively addressing and mitigating online harms. It underscores the need for different parties to assume responsibility for developing targeted responses, from TLD registry operators to registrars, online platforms, hosting companies, and content providers.

DNS Abuse Mitigation Actions Available to Registry Operators

While TLD registry operators are central to the management of domain names, their influence is primarily technical and administrative, and they have very limited ability to directly address content hosted on services accessed by way of the DNS. Below is a list of actions available to TLD registry operators:

- **Contact the registrant:** Registry Operators that collect registrant contact data may contact the registrant directly to request the owner investigate, take a specific action

[1] For additional information on different categories of online abuse, please see "Unpacking DNS Abuse: Understanding 'Abuse of the DNS' and 'Abuse via the DNS,'" available here.

(e.g., cleaning up a hacked site), or inform the owner of one of the following actions to be implemented.

- **Refer to the sponsoring registrar:** Registrars have a direct contractual relationship with the registrant and should be given a time-bound opportunity to investigate the purported DNS Abuse. If a registrar does not take action on the abuse, the registry maintains the right to directly take action.
- **Suspend the domain:** This is the most commonly used method for mitigating DNS Abuse. Suspending, or applying the status of serverHold to, the domain removes the domain name from the TLD zone file and the domain will no longer resolve. This disrupts access and email will be disabled. The content of the website may still exist on a server and could be available via the IP address directly or via other domain names, including in other TLDs.
- **Lock the domain:** Locking the domain on its own does not affect the content on the site or affect mail servers; it does however mean that the domain cannot be transferred, deleted or have its registration details modified. Locking the domain may aid in the investigation of the domain by third parties.
- **Redirect:** A registry can redirect a domain by changing the nameservers. This is often done as part of a government seizure (where the domain is redirected to a splash page along the lines of "This page has been seized by [governmental agency]") or for "sink-holing." A sink-holed domain logs traffic to help identify victims affected by DNS Abuse such as malware.
- **Transfer:** A registry has the ability to transfer the domain, which may allow for the prevention of DNS Abuse, while still allowing the management of lifecycle, EPP status codes, and expiration of the domain. This action is typically only done in response to a court order.
- **Delete:** Deletion is both ineffective since the domain can be re-registered and put to the same abusive purpose and extreme in that it is irreversible. For both of these reasons, suspension is almost always the better option to address DNS Abuse.

These actions are blunt instruments; they can disrupt or restrict user access to abusive content but do not actually remove the content itself. The harmful content could easily reappear on a different domain or otherwise be accessed directly via an IP address. Suspending or deleting a domain name also may inadvertently impact legitimate users and activities associated with the domain, such as when a website has been compromised to include illegal content on some parts of the site but not others. While these actions can serve to disrupt malicious activity like cybercrime and fraud by interrupting access, because they do not remove the harmful content itself, they should be considered as one of multiple possible actions that can be taken by different providers, some of which can address the harmful content much more precisely.

The Broader Internet Ecosystem

In contrast to TLD registry operators, online platforms, hosting and content providers have much more decisive control over the content, resources and broader services hosted on their infrastructure. They can take targeted actions to remove specific content that violates legal standards or their own policies, suspend individual user accounts or implement more nuanced filtering techniques to combat abusive content. For example, a hosting provider can identify and shut down a single malicious webpage or URL hosted on a domain name without impacting other legitimate services using the same domain name.

While there is clearly an important role for TLD registries to continue to refine their approaches and technologies to detect abuse and take appropriate mitigation steps in accordance with the actions available to them, it is also incumbent upon online platforms, hosting and content providers to implement robust measures to take speedy and precise action on abusive content that is hosted on their platforms. Any truly effective approach to mitigating DNS Abuse must be collaborative across the internet ecosystem and place each service provider in the position to take appropriate action based on their role and skillset.

DNS Abuse Mitigation Work within ICANN

The ICANN community has undertaken various efforts to analyze, measure, and develop requirements to mitigate DNS Abuse in recent years. In 2023, the RySG and the Registrar Stakeholder Group (RrSG, the RySG's counterpart representing the interests of ICANN-accredited registrars) voluntarily adopted new requirements to mitigate DNS Abuse in their contracts with ICANN, which took effect early in 2024. These amendments were the first step in a broader bottom-up community effort to create new obligations for DNS Abuse mitigation for gTLD registries and registrars, in accordance with their technical roles and capabilities and within ICANN's technical remit. The Generic Names Supporting Organization (GNSO), the body primarily responsible for developing policies for domain names in gTLDs, has initiated the first of multiple targeted policy development processes that each aim to address specific aspects of DNS Abuse. Taken together, these policy development efforts aim to increase the security of the DNS and help to mitigate the harms internet users face as a result of DNS Abuse.

Input for the European Commission

As the European Commission considers future action to fight online fraud and the role DNS Abuse plays in committing such fraud, we would encourage the Commission to keep the following principles in mind:

- Delineate categories of threats: infrastructure abuse, DNS Abuse, illegal vs. harmful content, etc.
- Understand the unique roles and responsibilities of the various service providers across the internet ecosystem
- Understand the precise operational and technical capabilities of various types of providers across the internet ecosystem
- Determine the necessary safeguards around liability, due process, and transparency to ensure innocent domain name registrants have recourse if infrastructure providers take erroneous action to address DNS Abuse
- Support ICANN's important role in coordination and facilitation, particularly as a centralized source of data, tools, and resources to help and hold accountable those parties responsible for managing and maintaining the internet's unique identifiers