ICANN Organization’s Comments on Public Consultation on “Powers in Relation to U.K.-Related Domain Name Registries”

1. About the Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN is a nonprofit public benefit corporation that, on behalf of the Internet community, oversees the technical coordination of the top-most level of the Internet’s Domain Name System (DNS). ICANN's mission is to help ensure a stable, secure, and unified global Internet. To reach another person on the Internet, you need to type an address – a name or a number – into your computer or other device. That address must be unique so computers know where to find each other. ICANN helps coordinate and support these unique identifiers across the world. ICANN was formed in 1998 with a global community of participants.

ICANN follows a multistakeholder model in which individuals, non-commercial stakeholder groups, industry, and governments play important roles in its community-based, consensus-driven, policy-making approach. Together, they produce policies for the DNS. The multistakeholder model of policy development is instrumental in governing generic top-level domains (gTLDs). Although ICANN does not directly manage country code top-level domains (ccTLDs), which are generally governed by an independent manager according to local laws, ICANN works closely with ccTLD operators to ensure the security and stability of the DNS.[1]

The consultation and feedback-seeking process that the Department for Science, Innovation and Technology (DSIT) is undertaking also resonates with the ICANN multistakeholder model’s emphasis on involving relevant stakeholders in decision making.

ICANN Contractual Compliance (“Compliance”) enforces the policies developed by the community and incorporated into the ICANN organization’s (org) agreements with gTLD registries and registrars. Compliance ensures these obligations are implemented to preserve and enhance the security, stability, and resiliency of the DNS. Compliance undertakes enforcement actions resulting from complaints received from external users, proactive monitoring, and audit-related activities. Contracted parties that fail to cure breaches of their obligations are subject to remedies up to and including termination.

ICANN's Bylaws expressly prohibit ICANN from imposing rules and restrictions on services that use the Internet's unique identifiers or the content that such services carry or provide.

This comment is submitted by the ICANN organization (ICANN org) in accordance with its charter for engagement with governments and standards bodies.

[1] “About ccTLD Compliance,” ICANN website, accessed 31 August 2023, https://www.icann.org/resources/pages/cctld-2012-02-25-en#:~:text=ICANN%20works%20 cooperatively%20with%20ccTLD,and%20 operability%20of%20the%20Internet.

2. ICANN’s Approach to DNS Abuse

ICANN org supports the definition in the upcoming proposal DSIT is considering that delineates five broad categories of harmful Internet activity as malware, botnets, pharming, phishing, and spam. ICANN has developed a cross-functional DNS Security Threat Mitigation Program that supports several initiatives and projects devoted to thwarting these specific activities.[2]

ICANN’s response to DNS abuse is multifaceted, reflecting the need to address abuse within the constraints of ICANN’s Bylaws and policies as defined by the ICANN community, and by obeying local law and regulatory requirements.

ICANN org's cross-functional DNS Security Threats Mitigation Program supports a number of projects, initiatives, and programs to mitigate DNS abuse. These include the following:

- ICANN is working to enhance the contractual obligations for ICANN-accredited registrars and gTLD registry operators related to DNS abuse.

- The Domain Abuse Activity Reporting System (DAAR), through which ICANN monitors and reports on potential threats and abusive domains. The aim is to facilitate and inform ICANN community discussions and provide factual data to policy makers so they can make informed policy decisions. The monthly DAAR reports show security threat concentrations of domain names via visuals and statistics. DAAR tracks reputation data for phishing, malware, botnet command and control domains, and spam as a vector for other security threats.

- The ICANN-funded project, Inferential Analysis of Maliciously Registered Domains (INFERMAL), analyzes one of the methods cybercriminals use to actively register domains to launch Internet-scale attacks, such as phishing, malware, or spam campaigns. There are many theorized reasons why bad actors may prefer to use certain registrars over others. For example, there is some evidence that suggests that bad actors may prefer registrars that provide low registration prices or specific payment methods. They also may look for registrars offering free application programming interfaces for bulk registrations or avoid registrars or top-level domains (TLDs) that require certain information in the purchasing process.

- The Domain Name Security Threat Information Collection and Reporting (DNSTICR) project of ICANN’s Office of the Chief Technology Officer identifies domain names that appear to have been used for malicious purposes and are related to the COVID-19 pandemic or the Russia-Ukraine war. It provides well-evidenced reports of these abuses to sponsoring registrars who can take appropriate action to mitigate the DNS abuse. After ICANN analyzes these domain names and reports the phishing

[2] “DNS Security Threat Mitigation Program (Last updated 8 May 2023),” ICANN website, accessed 31 August 2023, https://www.icann.org/dns-security-threat.

attacks, the registrar has the evidence needed to take the appropriate mitigation action.

In addition, ICANN Contractual Compliance enforces the contractual obligations set forth in ICANN's policies and agreements, including the Registry Agreement (RA) and the Registrar Accreditation Agreement (RAA). Examples of the abuse-related provisions enforced by ICANN Compliance include Specification 6 4.1, Specification 11 3(a) and 3(b) of the RA, as well as Section 3.18 of the RAA. For example, both registrars and registries must publish on their website information about how to submit a report of abuse about a domain name and an email address to collect reports of abuse. Registrars are required to investigate and respond appropriately to reports of abuse.

ICANN has worked with its accredited registrars and gTLD registries to develop new contractual obligations for dealing with DNS abuse.[3] The requirements are based on the actions that registrars and registry operators, respectively, can take to minimize the scope and intensity of the harm and victimization caused by DNS abuse. These requirements also consider that registrars and registry operators represent only a portion of the DNS ecosystem, which is composed of many actors. Depending on the specific circumstances of an instance of DNS abuse, the most appropriate actor to detect, assess, verify, and stop the abusive activity may vary, and sometimes may be an actor other than a registrar or registry operator.

Finally, ICANN org notes that some uses of domain names are outside of registrars' and registries' technical expertise and in many cases beyond ICANN's remit. For example, intellectual property disputes regarding the use of domain names can be complex, involving considerations such as fair use, free speech, and laws from multiple jurisdictions. Registrars and registries are not the proper venue to adjudicate these disputes.

The Organisation for Economic Co-operation and Development (OECD) recently produced a report,[4] noting that:

"...what is often labeled as 'addressing DNS abuse' should rather be understood as DNS-level action to address abuses online, i.e., leveraging the DNS ecosystem to solve issues that neither affect nor are caused by the DNS specifically. In fact, most forms of DNS abuse relate to content and services that belong to the 'content layer'…"

The findings of the OECD report echo ICANN's approach to mitigating DNS abuse.

[3] Sally Costerton, "ICANN and Contract Negotiations Update: Improved DNS Abuse Requirements," 30 May 2023, ICANN Blog, https://www.icann.org/en/blogs/details/icann-and-contract-negotiations-update-improved-dns-abuse-requirements-30-05-2023-en.

[4] OECD (2022), "Security of the Domain Name System (DNS): An introduction for policy makers," OECD Digital Economy Papers, No. 331, https://doi.org/10.1787/285d7875-en.

4. ICANN Relations With gTLDs, .london .scot, .wales/.cymru

For the purpose of this consultation, ICANN highlights that the registries which will fall under the upcoming amended legislation include gTLD registries that have an existing RA with ICANN, i.e., .scot, .wales/.cymru and .london. It is also noted that the ICANN community is working on the introduction of new gTLDs. Any new gTLDs introduced with a nexus to the United Kingdom of Great Britain and Northern Ireland (U.K.) would also be subject to the upcoming amended legislation. They will also have an RA with ICANN according to the policies for new gTLDs that the ICANN community is currently developing.

ICANN does not directly manage ccTLDs, which are generally governed by an independent manager according to local laws. ccTLDs are delegated through ICANN's Internet Assigned Numbers Authority (IANA) and there are existing processes on the initial delegation and subsequent transfers of the management of ccTLDs.[5]

For gTLD registries and ICANN accredited registrars, ICANN enforces the obligations of the RA and RAA respectively, which include ICANN Consensus Policies developed through the multistakeholder ICANN community in accordance with documented processes and procedures. Requirements from national legislation that create conflicts with the rules created within the ICANN ecosystem pose significant challenges for the registries and registrars, and for the multistakeholder Internet governance model more generally.

In particular, ICANN highlights that the ICANN community has been tasked with setting global policies for the gTLDs through its multistakeholder process. Those policies, developed by the multistakeholder community, are incorporated into the ICANN org's agreements with generic gTLD registries and registrars. Trust in ICANN's multistakeholder model has been reaffirmed multiple times, including by the government of the U.K. in the course of the IANA transition and afterwards.

As it is not the intention of this reform to interfere with ICANN's role and processes, ICANN org welcomes a continuous dialogue with the DSTI to preserve ICANN's multistakeholder community role in developing global policies related to the Internet's unique identifiers and the DNS. Keeping an open dialogue would also ensure that U.K. registries will not be subject to conflicting requirements to their detriment and to the detriment of the expansion of U.K.-specific TLDs.

Finally, given the high volatility of the current geopolitical landscape and the interest of some countries to defer Internet governance to nation states, preserving the multistakeholder model of governance of the DNS remains critical at this time. In light of upcoming processes at the United Nations' level (World Summit on the Information Society (WSIS+20)) that will look into the current model of Internet governance, ICANN counts on the support of the U.K. government to uphold the multistakeholder, bottom-up approach to the governance of the DNS.

[5] "Delegating or transferring a country-code top-level domain (ccTLD)," IANA website, accessed 31 August 2023, https://www.iana.org/help/cctld-delegation.

5. Conclusion and Next Steps

ICANN org is pleased that the U.K. government recognizes ICANN’s role. It takes note of the objective to avoid interfering with the ICANN’s community responsibility for the policies of gTLDs and trusts the multistakeholder model of Internet governance will also be recognized and respected in the final regulations to be introduced. ICANN org welcomes future dialogue with the DSIT and remains at the disposal of the DSIT during the development of the proposal.