ICANN’s Contribution to the European Commission's Draft Implementing Regulation

on Cybersecurity risk management & reporting obligations for digital infrastructure, providers and ICT service managers

25 July 2024

1. Introduction

Founded in 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit, public-benefit global organization, dedicated to coordinating and managing the Internet's unique identifiers. Its responsibilities include overseeing domain names, allocating IP addresses, setting protocol parameters, and managing the root server system. These efforts ensure the Internet remains stable, secure, and interoperable. By coordinating the Internet's unique identifier systems, ICANN plays a crucial role in guiding the Internet's expansion and evolution.

This comment on the Draft Implementing Regulation on Cybersecurity Risk Management & Reporting Obligations is submitted by the ICANN Organization in accordance with its charter for engagement with governments and standards bodies.

ICANN welcomes the opportunity to contribute to the European Commission's consultation on the Draft Implementing Regulation laying down the rules for the application of Directive 2022/2055[1] (NIS2 Directive) regarding technical and methodological requirements for cybersecurity risk management measures, hereafter referred to as "Annex", and further specifying the cases in which an incident is considered to be significant within the meaning of Directive 2022/2055.

First, ICANN supports further specifying the cases in which an incident is considered significant for Domain Name System (DNS) service providers and top-level domain (TLD) name registries. This aims to capture incidents that could have a significant impact on the availability and resilience of the DNS and the entities providing domain name services. To achieve the aforementioned objective, ICANN supports further clarifications in Article 5 and Article 6 of the Draft Implementing Regulation regarding the unavailability of a service, service degradation, and cybersecurity breaches in backend systems.

Second, ICANN supports clarifications regarding the criteria used to determine the existence of a considerable reputational damage of an incident set out in Article 3, and those used to determine a recurring incident set out in Article 4.

Third, with respect to the proposed technical and methodological requirements of cybersecurity risk management measures referred to in the Annex, ICANN suggests that the considerable development of best practices by the international multistakeholder community regarding the security of the DNS should be reflected and incorporated into the Annex.

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, p. 80–152.

2. Clarifications to Significant Incidents with regard to DNS Service Providers (Article 5)

I. Service Unavailability - Article 5, Point (a)

ICANN suggests that the prescribed timeframe for service unavailability adds complexity to incident assessment, as limiting the duration of the incident does not enhance the evaluation of its significance. Typically, DNS service providers use monitoring tools to achieve 100% uptime. Once a service is deemed unavailable, the provider's operations team will work on triaging and resolving the event. Therefore, a service that is unavailable for 10 minutes, as specified in Article 5, point (a), is likely to remain unavailable for a longer period.

ICANN supports the language used in Article 6, point (a), as it is clearer and more operative. Therefore, ICANN suggests **omitting the time limitation on the duration of the event**.

II. Service Degradation - Article 5, Point (b)

ICANN believes that the language used to capture service degradation does not align with the intended objective of capturing such incidents. To illustrate this, it is important to understand that name servers and TLD service infrastructure are distributed across the Internet, much like the end users who are attempting to reach the services. Therefore, factors beyond the control of a DNS service provider or a TLD name registry, such as connectivity issues at the local network or the ISP level, the intermediary or transit network, or the quality of the endpoint device or hardware, can negatively impact the perceived quality of service.

ICANN believes that approaching service degradation from the end user perspective could indirectly transfer the responsibility for upholding service quality to DNS service providers and TLD name registries for factors beyond their control.

To illustrate the above, consider an end user in one Member State using a personal computer to perform a DNS lookup on a name server located in another Member State. If the DNS lookup is not resolved within 10 seconds, as prescribed in Article 5, point (b), the event could be classified as a significant incident. However, factors such as the end user's device lacking connectivity to the local network or the network lacking connectivity to the DNS service provider's network in the other Member State may be the root causes of the delay, not the quality of service provided by the DNS service provider.

ICANN proposes **removing point (b) from Article 5,** considering that DNS service providers and TLD name registries cannot take responsibility for connectivity issues outside their network. From the service provider's perspective, the DNS infrastructure may be operational, accessible, and on standby to respond to DNS queries. However, if there are significant delays for such queries to reach the infrastructure, the DNS service provider or TLD name registry should not be held responsible for issues along the connectivity chain, nor should they report incidents that would otherwise not be considered significant.

III. Cybersecurity Breaches - Article 5, Point (c)

Considering the divergent levels of criticality of domain names, ICANN recommends distinguishing between different types of incidents to capture the granularity of significant incidents beyond the quantitative parameters prescribed in Article 5, point (c). To illustrate the importance of this distinction, consider a breach of the systems of a provider hosting essential services; the potential damage, whether material or non-material, may be substantial despite the total number of affected domains being low. Conversely, if the DNS services of 10,000 randomly generated domain names used for less critical purposes are breached, the resulting damage may be negligible despite the high number of affected domains.

3. Clarifications to Significant Incidents with regard to TLD Name Registries (Article 6)

I. Service Unavailability - Article 6, Point (a)

ICANN supports the phrasing of this point, which does not impose a specific timeframe to the unavailability of the authoritative domain name resolution service.

II. Service Degradation - Article 6, Point (b)

ICANN supports the notion that, similar to the justification provided for point (b) of Article 5, the language used to capture service degradation may indirectly lead to DNS service providers and TLD name registries absorbing responsibility for connectivity issues outside their network. This could result in an increase in the reporting of incidents that would otherwise not be considered significant. ICANN proposes **removing point (b) from Article 6.**

III. Cybersecurity Breaches - Article 5, Point (c)

ICANN believes that the text is clear, reasonable, and operative.

4. Clarifications to Determining Considerable Reputational Damage (Article 3)

ICANN believes that the reference to “media” in point (a) of paragraph 2 of Article 3, which is a determining criterion as regards the existence of considerable reputational damage of an incident in accordance with paragraph 1, point (b) of Article 3, is non-operative. ICANN understands the intent but cautions against using such a generic term that may include verified, unverified, and user-generated content.

Therefore, ICANN recommends that the language is clarified to reflect widely reported incidents in official media to determine considerable reputational damage, and thus, a significant incident.

Against this backdrop, ICANN supports **exploring the use of terms with a legal basis grounded in applicable EU law**, such as Regulation 2024/1083[2] (European Media Freedom Act). In particular, ICANN recommends using the terms *"media service provider"* and *"public service media provider"* as defined in point (2) and point (3) of Regulation 2024/1083.

5. Clarifications to Recurring Incidents (Article 4)

ICANN supports the objective of capturing significant incidents that, while not considered significant in isolation, may collectively be interpreted as significant due to their recurrence, as outlined in Article 3 of the Draft Implementing Regulation.

ICANN believes it is important to clarify point (b) of Article 4 regarding the apparent root cause of a recurring incident. In alignment with the comments provided above concerning point (b) of Article 5 and Article 6 of the Draft Implementing Regulation, an incident may be considered significant despite its cause being rooted outside the control of the impacted entity. Therefore, ICANN suggests adding language to this point to clarify that an apparent root cause outside the control of the affected entity **should not be considered a recurring - and therefore significant - incident**.

6. Comments on the Technical and Methodological Requirements (Annex)

The Draft Implementing Regulation makes direct reference to network security measures that entities falling within the scope of Directive 2022/2055 should adopt, particularly focusing on implementation plans and best practices regarding (i) a secure and full transition to the latest generation network layer communication protocols, (ii) the deployment of internationally agreed and interoperable modern e-mail communications standards to secure e-mail communications, and (iii) Internet routing security and routing hygiene of traffic.

ICANN welcomes the European Commission's proposed measures to protect network and information systems from cyber threats and proposes adding an additional point to section 6.7.2 of the Annex to include DNS security as a fundamental measure for enhancing network security.

ICANN recommends using language similar to that of point (l) of section 6.7.2 of the Annex to **incorporate the application of best practices in the security of the DNS**, calling relevant entities to apply best practices for the security of the DNS without specifying those practices as they can evolve over time. Such practices should be agreed upon by the relevant communities. An example of such practices emerging from the relevant communities themselves is ICANN's Knowledge-sharing and Instantiation Norms for DNS and Naming Security (KINDNS)[3] initiative

[2] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act), OJ L, 2024/1083, 17.4.2024.

[3] "ICANN Launches the KINDNS Initiative to Promote DNS Security Best Practices", September 2022, ICANN Announcements, https://www.icann.org/en/announcements/details/icann-launches-the-kindns-initiative-to-promote-dns-security-best-practices-06-09-2022-en

which engages with the DNS technical community, DNS service providers, software vendors, registrants, and others, to catalog, document, and develop a program to promote DNS operational best practices within various communities and ecosystems. As a result, KINDNS developed a framework for the most critical security norms for DNS operations, including those for authoritative and recursive resolvers and software.

7. ICANN Cybersecurity and Business Continuity Requirements and Enforcement

ICANN follows a multistakeholder approach to policymaking in which individuals, non-commercial stakeholder groups, industry, civil society, the technical community, and governments play important roles. Collectively, they make up the ICANN community, which develops policies for the DNS through a consensus-driven, bottom-up process. The consensus policies developed through the ICANN multistakeholder community are incorporated into agreements with generic top-level domain (gTLD) registries[4] and ICANN-accredited registrars. Separately, ICANN can also negotiate further obligations to the agreements with gTLD registries and ICANN-accredited registrars. ICANN works closely with gTLD and country code top-level domain (ccTLD) operators to ensure the security and stability of the DNS. Although all TLDs are delegated through ICANN's Internet Assigned Numbers Authority (IANA), ccTLDs are independently managed according to the relevant oversight and governance mechanisms within their respective countries.

ICANN's contractual agreements with gTLD registries include requirements regarding registry data escrow procedures, interoperability and continuity specifications, as well as an emergency transition procedure, which - in the event that any of the emergency thresholds for registry functions is reached - allows ICANN to designate an emergency interim registry operator of the registry for the TLD in accordance with ICANN's registry transition process[5]. One of the objectives of ICANN's agreements with gTLD registries is to ensure their overall resilience by ensuring higher levels of redundancy and continuity, higher availability and the swift restoration of the critical functions of the registry in cases of extraordinary events beyond the control of the registry operators. ICANN's contractual agreements include obligations to conduct registry operations using network and geographically diverse, redundant servers (including, among others, network-level redundancy, end-node level redundancy) to ensure continued operation in the case of technical failure or an extraordinary occurrence or circumstance beyond the control of the registry operator. ICANN enforces these obligations, which also include performance requirements for critical functions, such as DNS and Registration Data Directory Services (RDDS). I

The ICANN multistakeholder model breeds optimal, inclusive solutions for the DNS, globally applied, which are essential for a stable DNS and a global, single, and interoperable Internet. In that respect, the ICANN multistakeholder model is essential to the unified operation of the DNS and as such, is the appropriate place for the development of policies related to it, including cybersecurity and business continuity related policies for the DNS. Besides, this approach is

[4] Base generic top-level domain (gTLD) Registry Agreement (Base RA), January 2024, https://itp.cdn.icann.org/en/files/registry-agreements/base-registry-agreement-21-01-2024-en.pdf

[5] Emergency Back-end Registry Operator (EBERO), https://www.icann.org/resources/pages/ebero-2013-04-02-en

consistent with the commitment to the multistakeholder model of Internet governance that the EU champions.

ICANN policies and requirements are not static; they are continually revisited by the ICANN community and evolve to adapt to the changing digital landscape and enhance the ability of stakeholders to better serve the Internet community.

In late 2022, ICANN's registrars and gTLD registries requested a negotiation to enhance the obligations related to DNS abuse in both the Registrar Accreditation Agreement (RAA) and the Base gTLD Registry Agreement (RA). They sought to ensure ICANN has the right to terminate registrars and registries that do not adequately mitigate DNS abuse in their platforms. In 2023, ICANN and the Contracted Parties agreed to new terms and followed the procedures to amend the agreements. On 5 April 2024, the new provisions came into effect and ICANN's Contractual Compliance function began enforcing the new DNS abuse obligations applicable to registries and registrars. These requirements include obligations to take appropriate mitigation actions that are reasonably necessary to stop or disrupt DNS abuse. The successful effort to develop and enforce binding obligations to combat DNS abuse is a model of how ICANN and its stakeholders can address other emerging and challenging issues with a globally unified solution that is not bound by any specific jurisdiction.

8. Conclusion

ICANN welcomes the opportunity to contribute to the European Commission's consultation and remains committed to providing expertise regarding the technical functioning of the Internet and the multistakeholder model of Internet governance.

Considering the broad scope of Directive 2055/2022, especially concerning DNS service providers and TLD name registries, ICANN recommends clarifications to the European Commission's proposed framework for classifying significant incidents in cases where a service is rendered unavailable or degraded.

Moreover, ICANN recommends clarifying the European Commission's framework for determining considerable reputational damage and the recurrence of incidents. ICANN suggests incorporating best practices in the security of the DNS into the Annex to reflect significant developments by the global, multistakeholder community in this field.

ICANN

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

soundcloud/icann

instagram.com/icannorg