Proposal for a Directive on Measures for a High Common Level of Cybersecurity Across the Union, Repealing Directive (EU) 2016/1148 ("NIS2")

Public Consultation

ISC's Submission: DNS and Root Name Servers

March 2021

Internet Systems Consortium, Inc, (ISC) is grateful for the opportunity to comment on the NIS2 proposal.

ISC is a member of a limited and special group. We are one of the world's 12 globally recognized operators of authoritative Internet DNS root name servers. As one of the world's trusted Root Server Operators (RSO) we wish to maintain a stable root for the Internet's global non-fragmented DNS system.

ISC is a not-for-profit company, incorporated in Delaware, resident in New Hampshire, USA, and registered under US IRC § 501(c)(3). ISC's wholly owned subsidiary, Internet Systems Corporation, is also incorporated in Delaware and resident in New Hampshire, USA. ISC and its wholly owned subsidiary collectively comprise a "small enterprise," having fewer than 50 staff and less than €10 million annual turnover.

We make this submission for one purpose only: to comment on the potential impact of NIS2 on the operation of DNS root name servers.

Except as noted, our comments relate to COM(2020)823 final, 16.12.2020, 2020/0359 (COD) and Annexes 1 to 3.

1. Executive summary

1.1. Operating a root name server system is an inherently global process.

1.2. Operating a root name server system involves significant cost while generating no revenue.

1.3. We question whether NIS2 should extend to the operation of root name servers at all. The global DNS root server system is technologically resilient, well-maintained, and globally trusted. This trust is due to both the technological expertise and dedication of those who operate root servers, the diverse identities of root server operators, and the fact that no single root server operator – or small group of operators – can destabilize the Internet's authoritative DNS root name system.

1.4. We believe in a global non-fragmented DNS addressing system.[1] We believe that bringing root server operators into the remit of NIS2 is unnecessary and brings the potential to destabilize the Internet's global unitary DNS system.

2. The technical nature and significance of root name servers

2.1. Root name servers fulfil an important, but limited, function in maintaining a global non-fragmented DNS for the Internet. They answer a single question: what are the hostnames and IP addresses of the authoritative DNS servers operated by each of the domain name Registries that administer the world's 1500+ Top Level Domains (TLDs). Each TLD has one authoritative Registry. The organization managing a TLD Registry then empowers multiple domain name Registrars. The Registrars, in turn, manage requests from Registrants to register domain names in the TLD.

2.2. If a computer connected to the Internet wishes to connect to a previously unknown domain name (e.g., **`example.com`**) that computer consults an online DNS server in an effort to locate the relevant DNS records. The DNS server consulted is typically (but not necessarily) maintained by the customer's Internet service provider and supplied as a matter of course with the Internet service. If this DNS server does not recognize the domain name, it will consult with the relevant TLD Registry (e.g., **`.com`** TLD Registry). That TLD Registry returns information that enables the DNS server to find authoritative information concerning that domain name.

2.3. If the relevant DNS server does not have current information concerning the network address of the requested TLD Registry (**`.com`**), it then consults a root name server. The root name server (in effect) answers this question: "What is the hostname of the DNS server where I can find information about domain names registered in this TLD?" The root name server does not provide information about the requested domain itself (**`example.com`**). The root name server does not play a role in registering domain names. The root name server does not provide DNS services to domain name Registrants.

2.4. The database containing the list of TLD name servers is known as the "root zone". RSOs do not control the content of this database. This task is the responsibility of IANA/ICANN, which operates through the global multistakeholder process. The RSOs merely replicate, and repeat with authority, the root zone information pursuant to that multistakeholder governance process.

2.5. The root name servers are operated under the control of 12 RSOs. No single RSO is capable of subverting the system. DNS servers that seek authoritative TLD Registry addresses can (and do) consult with multiple servers operated by multiple RSOs. If a server operated by an RSO disagrees about the authoritative DNS address of a TLD Registry this disagreement is discovered through technical means. The relevant RSOs then work to remedy whatever caused the disruption and reinstate authoritative TLD address data as assigned by IANA/ICANN. The massive redundancy in the system limits

[1] We note this same goal reflected in the "**Draft** Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade" 6722/21, 9 March 2021. This draft includes the following at paragraph 17:

> "The Council… LOOKS FORWARD to discussions with the Commission, ENISA, the two EU DNS Root Server Operators and the multi-stakeholder community to assess the role of the two EU DNS Root Server Operators when it comes to guaranteeing that the Internet remains **globally accessible and non-fragmented**." (emphasis added)

the opportunity for mischief if one machine is suborned. Furthermore, the contents of the root zone are cryptographically authenticated and protected from unauthorized modifications using DNSSEC.

3. Root name server operations lose money

3.1. The tens of thousands of network operators and other DNS service providers who consult root name servers from time to time to validate TLD addresses do not pay for that privilege. These TLD addresses are published to the world. Anyone, anywhere, can look them up when necessary. This availability to the world without transaction cost is an important part of the system's design and engineering efficiency.

3.2. Although it does not generate revenue, operating a root server system involves significant expense. The RSO must secure and maintain a diversity of technical equipment, residing in multiple locations around the world and often colocated at Internet exchange points (IXPs) or other major traffic interchange points. While some IXPs make small payments to RSOs to defray costs of installing additional root server nodes, such payments are by no means certain and they do not address the operating expenses of the root server system.[2]

3.3. In the world of Internet domain names, money tends to flow as follows:

a. **Revenue collected by DNS service providers.** Domain name Registrants typically pay a commercial service provider for DNS service. This service answers network questions about how to find online resources related to a given domain name.

b. **Revenue collected by domain name Registrars.** Domain name Registrants make recurring payments to Registrars for the privilege of maintaining a domain name registration. A percentage of this revenue is paid by the Registrar to the relevant TLD Registry.

c. **Revenue collected by TLD Registries.** Domain name Registrars typically pay a TLD Registry for the privilege of operating as a Registrar, as well as a percentage of registration fees.

d. **Revenue collected by ICANN.** Both gTLD and ccTLD Registries make payments to ICANN. The gTLD Registries pay ICANN pursuant to a variety of commercial arrangements and ccTLD Registries make varying levels of contribution on a voluntary basis.

e. **No revenue collected by RSOs.** No part of these various revenues is paid routinely to Root Server Operators, as such. To the extent that any RSOs collect money from this system (e.g., ICANN and Verisign) it is because of some other activity they undertake (e.g., acting as a TLD Registry) and not because they are operating a root server.

[2] In ISC's annual report for 2019, we reported to the world that payments received to defray some root server equipment costs generated 1% (one per cent) of all funds received in the year. In that same year, root server operations were responsible for 11% (eleven per cent) of all expenses incurred. (Financial data not audited.)

3.4. Most RSOs (including ISC and ICANN) are managed by organizations that operate on a not-for-profit basis. Some are operated by and funded by government agencies (e.g., NASA). Some are operated by academic institutions or consortia.

3.5. In common with all RSOs we find other funding sources, including contributions and grants, so that we can fulfil our mission to the world: maintaining stability and trust at the root of the world's global DNS system.

3.6. There have been some discussions within the RSO community of establishing an arrangement in which IANA/ICANN would remit payments to Root Server Operators in consideration of RSO services. These discussions are at an early stage.

4. There is no demonstrated need to extend the scope of NIS2 to root name server operations

4.1. We believe strongly in the need for cyber security and trust in Internet infrastructure. We understand that trust in global DNS is important to the good functioning of the Internet. Our very existence as a company is founded on this principle.

4.2. Although there have been a number of cyberattacks against various DNS-related service providers, there is little or no evidence that attacks on the root server system are a significant part of the problem. Threat actors who seek to subvert the authenticity of domain name records often attack systems that provide (paid-for) DNS services to domain name Registrants. If a criminal can take control of the DNS records of the **`example.com`** domain, this allows that attacker to use that domain name for its own nefarious purposes. Such attacks have become common, sometimes aided by poor security practices of the Registrants themselves.

4.3. By contrast, attacks on root name servers historically have focused on denial-of-service attempts. Such attempts have been thwarted routinely and have become increasingly rare as the RSO community has invested in massively parallel equipment in multiple locations, with the root DNS servers' IP addresses announced globally. This reduces the impact of DDoS attacks against the root system and helps ensure that the effects of any such attack are limited.[3]

4.4. The RSO community currently enjoys a good reputation for having built and maintained a robust and resilient system that does one important thing and does it well: reporting the addresses of the authoritative DNS servers of the TLD Registries.

5. Trust in the root server system is founded on diversity of infrastructure and unity of purpose

5.1. The world at large reposes trust in the root server system because it is diverse. Root name servers operate on the basis of:

a. Diversity of control (twelve RSOs with a variety of goals – mostly not-for profit)

b. Diversity of equipment (thousands of nodes operating in hundreds of locations)

[3] We are unaware of any DDoS attack that has succeeded in destabilizing the root server system such that any effects were visible to end users.

c. Diversity of implementations (different operating systems and DNS software)

d. Diversity of geography and sovereignty (the operators are located in a variety of sovereign states, and each operator in turn locates its equipment in multiple sovereign states around the world)

5.2. What all RSOs have in common is this: an abiding desire and a passionate mission to maintain a global, unitary, resilient DNS system. This is a passion driven by the understanding that a single global DNS system has enabled the global success of the Internet today. It enables ubiquitous connectivity. It allows equipment manufacturers and network service operators to function secure in the knowledge that standards-based networking will empower them to innovate and deliver services.

5.3. This combination of unity of purpose and diversity of infrastructure is the foundation on which the world has built trust in the global DNS addressing system. Anything that threatens either of these, threatens that global trust.

6. Extending NIS2 to RSOs could destabilize the entire RSO system and DNS as we know it

6.1. The current draft NIS2 appears, on its face, to extend to all RSOs[4] without regard to their size[5] or where they are established in the world.[6] While this global extension may have been unintentional in the case of root name servers,[7] it is hard to escape the logic that regulating one RSO would mean regulating them all.

6.2. All 12 RSOs (including ICANN and three agencies of the US government) maintain root server equipment in the European Union. Even if all such equipment of non-resident RSOs were to be withdrawn from the European Union (which would, itself, disrupt the resilience and stability of the system), network operators and others resident in the Union would continue to consult equipment that is resident outside of, and managed by organizations that are not established within, the European Union.

6.3. If it is really the goal of NIS2 to bring all 12 RSOs under its regulatory remit, this could produce significant additional challenges for both EU and non-EU resident RSOs. We fear that any move by a single sovereign state to regulate the RSOs as a group could produce similar regulation by other sovereign states in response. If all RSO operations become regulated simultaneously by multiple sovereign states, the resulting

[4] The function of an RSO appears to fall within the definition of "DNS service provider" in Art 4(14) and Recital 15 specifically calls out "root name servers" as a subject of regulation.

[5] Although NIS2 normally would not apply to a small enterprise like ISC, Article 2(2)(a)(iii) makes a specific exception to include any enterprise of any size that operates as a "(DNS) service provider[]."

[6] Article 24(3) speaks of extending coverage to "DNS service providers" that are "not established in the Union, but offer[] services within the Union." As discussed above, data maintained by all 12 RSOs can be consulted by any person anywhere in the world at zero charge. It is unclear whether making this information available to the world, for free, is intended to fall within the definition of "offering a service" within the Union.

[7] The Impact Assessment Report prepared by Commission Staff accompanying NIS2 refers repeatedly only to the **"two root name servers"** that are **"located in Netherlands and Sweden."** Commission Staff Working Document – Impact Assessment Report, SWD(2020)345 final, 16.12.2020, Part 1/3 at p.62, footnote 175, Part 2/3 at p.24, footnote 14, and Part 2/3 at p.44. It is therefore unclear to us whether the 10 RSOs established outside the Union are a purposeful target of NIS2 regulation, or they have been unintentionally swept up into NIS2 by the inherently global nature of their operation. See also a similar reference to "two" root name servers in the Draft comments from the Council cited in footnote 1, above.

compliance and reporting burdens and the increasing risk of conflicting regulatory requirements could easily fracture or destroy the root server system as we know it. With its destruction, we fear the destruction of the global unitary DNS addressing system and the fragmentation of the Internet that would inevitably follow.

6.4. RSOs already work in close cooperation with IANA/ICANN, which in turn is governed globally through the multistakeholder process. We believe that the multistakeholder process is the most appropriate method for the European Union, as well as other sovereign and non-sovereign interest groups interested in the smooth and efficient operation of the Internet, to influence RSO operations.

7. Recommendations

7.1. We ask that NIS2 is amended specifically to dis-apply the Directive to operation of the Internet’s global root name severs.

7.2. If NIS2 is dis-applied to root name servers, we ask that NIS2 is also amended specifically to limit the ability of Member States to extend any similar Member State regulation (including the transposition of NIS2) to the operation of such root name servers.

7.3. If NIS2 is specifically intended to apply to all RSOs in the world, including those that have no establishment in the EU,[8] we recommend modifying the jurisdictional allocation mechanism in Article 24(2). In circumstances where an RSO has no establishment in the Union, and cyber security decisions are taken outside the territory of the Union, the current mechanism would award NIS2 regulatory jurisdiction to the Member State in which the RSO has the “highest number of employees.” We suggest that this is not the most appropriate means of allocating regulatory jurisdiction among and between the several Member States, especially as such employees may have little or nothing to do with RSO operations. We ask that any such extraterritorial RSO be allowed to elect an appropriate Member State to act as NIS2 regulator so as to enable better chances of productive communication between regulator and RSO.

[8] See comments in paragraph 6.1, especially footnotes 6 & 7.