Feedback on the Cybersecurity Act (CSA2) and Network Information Security (NIS2) simplification proposals

The RIPE NCC is a not-for-profit membership organisation and the Regional Internet Registry (RIR) for Europe, the Middle East and Central Asia. We operate one of the world's 13 global DNS root servers (K-root) and act as the secretariat for the RIPE community, which is an inclusive forum open to all parties interested in wide area IP networks.

We aim to provide feedback on the proposal for a Directive amending the NIS2 Directive and the proposal for a Regulation revising the Cybersecurity Act (CSA2). In summary, we recommend the following: 1) Reduce the administrative burden, particularly under the NIS2 framework, for small and micro DNS service providers and small to mid-cap enterprises. 2) Provide clearer justification for the collection of IP ranges of the entities involved. 3) Ensure a strong multistakeholder approach to maintaining the core technical functions of the Internet, especially in relation to the CSA2 draft proposal.

1. NIS2 simplification

The RIPE NCC has already expressed concerns about the risks associated with subjecting the Domain Name System (DNS) to government oversight.[1] We highlighted the potential for unintended consequences resulting from overreach and retaliatory measures, which would complicate the functioning of this key component of the Internet's global infrastructure.

We also emphasised the high level of distribution and diversity within the DNS ecosystem, which includes both commercial and non-commercial operators, as essential for ensuring the overall stability and resilience of the DNS. We are concerned that imposing excessive regulatory burdens and compliance costs could jeopardise this stability and resilience, and could encourage some DNS operators to cease their operations or withdraw their services from the EU, resulting in increased centralisation among larger commercial companies.

We therefore welcome the ongoing efforts to reduce the regulatory burden on micro and small DNS providers, as well as the introduction of the small mid-cap enterprises category under Recommendation 2025/1099, qualifying these entities for the ex-post regime. Such adjustments represent a positive step toward a more proportionate and risk-based approach.

2. Registration of IP ranges

Regarding the role of ENISA, which is tasked to maintain and create a registry based on information provided by Member States (including the newly required IP ranges), the new proposals mandate essential and important entities to notify competent authorities of any changes within two weeks of their occurrence. We recommend regulators to provide more explanation of how these IP ranges should be used for security purposes. We also suggest providing more details about what information is appropriate for subject entities to report and make sure that registration obligations remain guided by the principle of proportionality.

---

[1] RIPE NCC Response to the European Commission's Proposed NIS2 Directive (March 2021): https://www.ripe.net/media/documents/RIPE_NCC_Response_to_the_European_Commissions_Proposed_NIS_2_Directive_March_2021.pdf

Since the accompanying documents and impact assessments do not provide any rationale for collecting IP ranges, nor explanation for the need to centralise all information in a registry maintained by ENISA, we question whether requiring systematic reporting and updating of IP ranges is the most efficient use of resources to address security risks and respond to cyber incidents. A cost-benefit analysis and additional explanation would be appropriate to prevent possible duplicative efforts, explain what mechanisms or security approaches will be implemented to monitor that IP space, and ensure security benefits outweigh the administrative burden of collecting and updating IP ranges.

3. Technical Core of the Internet

We note the reference to the multistakeholder approach in Recital 14 of the CSA2 proposal: *"[...] ENISA should support the security and resilience of the public core of the open internet and the stability of its functioning, including, but not limited to, the secure deployment and operation of key protocols [...] by promoting best practices, guidance, and cooperation, in accordance with established global, multistakeholder Internet governance arrangements and the respective roles and responsibilities of relevant international technical and operational bodies".* In addition, the new proposal suggests that "*ENISA shall contribute to the implementation of Union policy and law [...] by assisting Member States and relevant Union entities in developing and promoting cybersecurity policies related to sustaining the general availability and integrity of the public core of the open internet" (*Article 5(1)(e)*).*

While we welcome the reference to multistakeholder Internet governance arrangements in the recital, we encourage the Commission and ENISA to apply this approach consistently when addressing the Internet's core technical functions. This means working with the relevant technical community actors in accordance with their respective roles and responsibilities. The IETF remains the leading standards body for open Internet standards, while registration services for key Internet identifiers are carried out by non-profit and non-governmental organisations and their respective communities through inclusive, bottom-up governance models, including the RIPE NCC as secretariat for the RIPE community, ICANN and Public Technical Identifiers (PTI), among others. The Commission and ENISA should work with these stakeholders in accordance with their respective roles and responsibilities, ensuring that they continue to play a central role in maintaining a secure, resilient and globally interoperable Internet.