RIPE NCC response to the consultation on the draft law implementing NIS2 in the Netherlands

The *Réseaux IP Européens* Network Coordination Centre (RIPE NCC) is one of the five Regional Internet Registries (RIR) that allocate and register IP addresses and Autonomous System Numbers (ASNs) worldwide. Collectively, the RIRs form the Joint Internet Number Registry system and coordinate their activities via the Number Resource Organization (NRO). Headquartered in the Netherlands, the RIPE NCC is a not-for-profit membership organisation with more than 20,000 members in 76 countries across Europe, the Middle-East and parts of Central Asia. Our main role as RIR is to allocate and register Internet number resources to organisations in our service region that run networks.

The RIPE NCC welcomes the opportunity to provide a response to the online consultation on the draft law implementing the NIS2 Directive in the Netherlands. Our response offers considerations and recommendations related to definitions of DNS services, risk management and reporting requirements, and cooperation with competent authorities.

Definitions of DNS operations and services

The RIPE NCC actively participated in discussions on the proposed revision of the NIS2 Directive at the EU level.[1] Among the main concerns, we pointed to the potential unintended consequences of the draft legislation on global DNS operations. One of the main issues we raised was that subjecting root servers to EU regulatory oversight could encourage foreign governments to reciprocate with their own legislation that undermines or interferes with the operation of this fundamental component of the Internet's infrastructure. Other issues were related to regulatory overreach and the risks of undermining the resilience of the global Internet. As a result, the root name servers are excluded from the scope of the EU Directive.

Article 6(20) of the NIS2 Directive defines “DNS service provider” as an entity that provides: “*(a) publicly available recursive domain name resolution services for internet end-users; or (b) authoritative domain name resolution services for third-party use, with the exception of root name servers.”* While the RIPE NCC does not provide DNS registration services as defined under Article 6(21)(22) of the NIS2 Directive, we do provide DNS coordination and support activities. This includes providing global secondary services to some country code top-level domain (ccTLD) operators who are in the start-up phase of their operations, as well as reverse DNS (rDNS) services for the IPv4 and IPv6 address space we manage. For the address space managed by other RIRs, we provide secondary DNS services to support the reliability of these reverse lookups. We also operate, as a public service, one of the Internet's 13 root name servers (K-Root), which is managed as a set of globally-distributed nodes. It is important to note that while the RIPE NCC operates a root server funded by our 20,000 members for the good of the Internet, several other organisations active in Internet coordination activities also manage certain DNS functions on a voluntary basis and for no financial benefit.

Part of the stability of the DNS comes from the extremely high distribution and diversification of operators offering commercial and non-commercial services. If regulatory requirements, compliance costs and oversight are applied in a way that makes it too demanding, non-

[1] See RIPE NCC Response to the European Commission’s Proposed NIS2 Directive

commercial DNS operators may decide to halt or withdraw their operations from the EU, leading to more centralisation by commercial companies, which may affect the stability and resilience of the DNS system. We urge competent authorities to adopt a case-by-case approach and ensure a proportionate level of implementation and enforcement.

To prevent potential negative impacts on important Internet operations, we recommend Dutch authorities provide guidance to DNS operators and align their definitions with the terminology commonly used within the Internet technical community. Of particular relevance is RFC 9499 “DNS Terminology”, which provides detailed information and represents the consensus definitions of the DNS community.[2]

Cybersecurity risk management and alignment with international standards

The “duty of care” as described under Chapter 7 of the draft cybersecurity act requires essential and important entities to take appropriate and proportionate technical, operational and organisational measures to control risks to the security of the network and information systems, which it uses for its operations or to provide services. It shall also take these measures to prevent incidents or mitigate the effects of incidents on recipients of its services and on other services. The draft then states that measures should be commensurate with the risks and that entities should take into account “state-of-the-art” implementation costs, and European and international standards, where relevant.

While we welcome the recognition of both European and international standards in the draft law, we recommend more explicit language to encourage national authorities, ENISA and other EU member states to strongly align their guidelines and assessment with internationally recognised standards in the area of cybersecurity risk management. For example, ISO/IEC 27001 is referred to by other EU member states. This is paramount for entities when implementing the requirements of the law in their operations and ensuring legal harmonisation across the EU and beyond.

Incident reporting requirements and thresholds

The “duty to report” described in the draft law requires entities to report any “significant incidents”, and an “early warning” should be sent to the competent authority and CSIRT within 24 hours of becoming aware of a significant incident (Article 28). We understand that further guidance based on the draft cybersecurity act (Article 37) will be provided at a later stage, including definitions of what constitutes an incident and the thresholds to determine its existence and significance. We recommend that thresholds to assess the significance of an incident are carefully tied to the service providers and not the recipient of the service. The main reason is that providers may lack key information needed to determine an incident’s significance, such as the exact number of users affected, the severity of service disruption, and financial loss. Moreover, the level of significance of an incident might change over time as the incident is investigated and its impact further assessed. This means the reporting framework should be flexible and focused on realistic and measurable parameters.

Regarding double reporting, we note that entities must report to both the CSIRT and the competent authority. We appreciate ongoing efforts to provide a single way of sharing information as described in the accompanying Explanatory Memorandum. We encourage

[2] See https://www.rfc-editor.org/rfc/rfc9499

national authorities to further harmonise and streamline reporting obligations, for instance by aligning timeframes and processes across regulatory regimes in order to limit the administrative burden and costs for network operators.

We also encourage CSIRTs to actively share relevant threat information with essential and important entities in order to balance some of the additional burden of the regulatory requirements with an added value of two-way operational collaboration to prevent and resolve incidents, in order to ensure a higher common level of cybersecurity across the EU.

Cooperation with competent authorities

The Netherlands is recognised for its world-class Internet infrastructure and exceptional talent pool, making it a hub for technology and innovation in Europe. While NIS1 applied to approximately 300 organisations, NIS2 is expected to apply to more than 5,000, with higher administrative and financial burdens for these entities. The RIPE NCC supports the aim of NIS2, which is to ensure a higher common level of cybersecurity across the EU. However, requirements under NIS2 may pose challenges and constitute disproportionate charges, especially for small and medium-sized organisations and entities with complex business models and operating environments as described in recitals 16 and 21 of the NIS2 Directive.

Enhanced cooperation between competent authorities and these entities will be paramount for effective implementation of the new law. It is equally important that national authorities, including ministries and relevant departments, share expertise and knowledge relevant to their respective sectors and sub-sectors in order to ensure a proportionate level of implementation and enforcement.

Finally, the Netherlands is a strong advocate of a single, open, free and secure global Internet, and has always supported the multistakeholder approach in Internet governance. As described in its national and international cyber security strategy, Dutch authorities aim to protect the public core of the Internet – meaning its technical operations and functions – from unnecessary interference.[3] We believe that organisations responsible for the administration of the global Internet, such as the RIPE NCC (as secretariat to the RIPE community), the IETF and others, should remain in the lead for developing the technical standards, protocols and procedures governing the Internet's core functionality. The Dutch authorities have consistently pledged to prevent scenarios where national or regional regulations could contribute to Internet fragmentation, and we fully support this stance.

[3] See Netherlands Cybersecurity Strategy 2022-2028 and International Cyber Strategy 2023-2028