ECIS European Committee for Interoperable Systems

ECIS ivzw-aisbl
Louizalaan 65 avenue Louise Box 2
B-1050 Brussels, Belgium

T/F +32 (0)2 706 24 15
info@ecis.eu
www.ecis.eu

18 March 2021

FEEDBACK ON THE EUROPEAN COMMISSION'S

PROPOSAL FOR A REVISED DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS

1. BACKGROUND ON ECIS

1. The European Committee for Interoperable Systems ("**ECIS**") is an international, non-profit association of information technology companies founded in 1989 which endeavours to promote a favourable environment for interoperable ICT solutions. For three decades ECIS has actively represented its members on issues relating to interoperability and competition before European, international and national fora, including the EU institutions and WIPO. ECIS' members include both large and small information and communications technology hardware and software providers, including IBM, McAfee, Opera, Oracle, and Red Hat.

2. FEEDBACK ON THE PROPOSAL FOR A REVISED DIRECTIVE ON SECURITY OF NETWORK AND INFORMATION SYSTEMS

2. ECIS welcomes the European Commission's ("**Commission**") proposal to revise the Directive on Security of Network and Information Systems ("**NIS2 Proposal**"). The fast-changing digital landscape, accelerated further by the COVID-19 pandemic, necessitates a revised regulatory framework to provide a new approach to cybersecurity and critical infrastructure protection.

3. Cyber threat intelligence information-sharing between public and private entities is indispensable for both "essential" and "important" entities (as defined in Article 4 NIS2 Proposal) to maintain digital operational resilience. Ensuring the interoperability of threat intelligence feeds is critical for successful threat intelligence as it allows for: (i) the sharing and receiving of cyber-threat intelligence; and (ii) the rapid detection of, and preparedness to, respond to imminent attacks by cybersecurity experts.

4. Interoperability enables cybersecurity communities to communicate using a common language which, in turn, enables a better understanding of cyber-attacks. Interoperability and cooperation between public and private entities on threat intelligence feeds has clear benefits for businesses, as they deploy cloud services and cybersecurity solutions and seek to protect against existing and prospective threats.

Scope and classification of entities

5. The scope of the current NIS Directive is expanded considerably by the Commission's proposal, which adds new sectors based on their criticality for the economy and society, and introduces a size cap, such that all medium and large companies in selected sectors will be in scope. By expanding the scope and number of service providers which are "essential" entities, the NIS2 Proposal does not account for common practices in the enterprise cloud environment, whereby one essential service provider is the user of another essential service provider's services. This could lead to legal ambiguity and overlap in reporting obligations.

6. The NIS2 Proposal expands the extra-territorial effect of the current regime, and will now apply to some entities, including cloud computing service providers, who offer services within the European Union, but do not have a European establishment. This means that cloud computing service providers, among others, will have to designate a representative in the European Union (Article 24(3) NIS2 Proposal), which may increase the administrative and regulatory burden on these entities.

Coordinated vulnerability disclosure

7. The NIS2 Proposal aims to encourage coordinated vulnerability practices, requiring the European Union Agency for Cybersecurity ("**ENISA**") to develop a European vulnerability registry. ECIS supports a coordinated approach to cybersecurity at the European level. It is vital ENISA's efforts build on coordinated vulnerability disclosure work already undertaken at international level, notably the CVE programme[1].

Security requirements and risk management approach

8. Article 18 of the NIS2 Proposal introduces numerous, and significant, cybersecurity risk management measures, including risk analyses, business continuity and crisis management, and testing and auditing procedures, among others. While ECIS is supportive of a comprehensive risk management approach, the current proposals, as drafted, would add a significant administrative burden on entities without any demonstrative proportional benefit. Further, the minimum requirements for appropriate risk management at Article 18(2) of the NIS2 Proposal should be further clarified to ensure legal certainty, and where relevant, reference should be made to minimum technical standards (such as ISO27001).

Supply-chain assessment

[1] https://cve.mitre.org/

9. ECIS welcomes the Commission's aim to address the security of supply chains and supplier relationships by tackling cybersecurity risks. In order to align with existing industry initiatives, ECIS recommends that the Commission aligns its approach in this area with existing industry recommendations for baseline security requirements (such as those of the Charter of Trust).

Incident Reporting

10. According to the NIS2 Proposal, essential and important entities should report any incident having a significant impact on the provision of their services. The NIS2 Proposal introduces a two-stage incident reporting approach. Entities should submit an initial notification within 24 hours of becoming aware of the incident, and produce a final report, not later than one month after the initial notification. This is a very short timeframe in which to make a notification to the competent authorities and may not be workable for all players. In addition, ECIS is concerned that this approach to incident reporting would require entities to report incidents before operations are effectively resumed, potentially exposing them to further risk. While ECIS recognises that a prompt incident reporting framework is vital to ensure robust oversight of breaches by competent authorities, this timeframe should be extended to 72 hours. Not only would this timescale align with many regulatory timeframes required by European Union legislation (such as that required under Article 33 General Data Protection Regulation), it would also ensure that entities are in a better position to meet, and coordinate, various reporting requirements.

11. The NIS2 Proposal also introduces a requirement to report "*any significant cyber threat that* […] *entities identify that could have potentially resulted in a significant incident*" to competent authorities or the computer security incident response team ("**CSIRTs**") (Article 20(2) NIS2 Proposal). Similarly, entities are required to notify the recipients of their services of cybersecurity threats and of any measures that the entities can take in response to the threat. While ECIS supports a stringent and coherent cybersecurity regime, it is concerned that these new requirements are too burdensome, speculative, and will ultimately lead to a lack of clarity. Additionally, the increased incident reporting obligation may also be unnecessarily burdensome for the competent authorities and CSIRTs and lead to decreased efficiency.

Supervision, enforcement and penalty regime

12. The NIS2 Proposal introduces more stringent supervisory measures for national authorities, and stricter enforcement. Under Article 31(4) NIS2 Proposal, EU Member States would be required to ensure that infringements are subject to administrative fines "*up to a maximum of at least*" EUR10 million or 2% of the total worldwide turnover (at an undertaking level), whichever is higher. Further, NIS2 Proposal leaves open the opportunity to impose criminal penalties at national level for infringements. It is important that the sanction and oversight regime remains proportionate to encourage service providers to operate. As such, any proposed criminal sanctions are discouraged, as these are disproportionate and could also lead to reluctance from market players to offer services in the European Union.

Interaction with other legislation / proposals

13. Recital 13 of the NIS2 Proposal states that its provisions relating to ICT "*risk management measures, management of ICT-related incidents and notably incident reporting, as well as on digital operational resilience testing, information sharing arrangements and ICT third party risk*" should not apply to financial entities covered by overlapping legislation. However, ECIS believes that this could lead to a fragmented approach and ultimately create an increased regulatory burden on entities falling under the scope of the NIS2 Proposal. In order to effectively coordinate and strengthen Member States' responses to cybersecurity and resilience, it is necessary that the NIS2 Proposal is aligned with other legislation, does not create double reporting obligations, and clearly outlines the new notification procedures which are not already covered by other existing European Union legislation.

Encryption

14. Recital 54 of the NIS2 Proposal posits that use of encryption, and in particular end-to-end encryption, should be promoted and, "*where necessary, should be mandatory for providers of such services and networks*." The recital then goes further to state that the use of such encryption "*should be reconciled with the Member State' powers to ensure the protection of their essential security interests and public security, and to permit the investigation, detection and prosecution of criminal offences in compliance with Union law*" but that such "[s]*olutions for lawful access to information in end-to-end encrypted communications should maintain the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime*."

15. ECIS appreciates the Commission's recognition of the important role of encryption in data protection and cybersecurity. It is an important tool in the risk management framework adopted by Member States. As with other security tools, organisations should consider when the use of encryption is required to mitigate a particular set of risks, and respond accordingly. It should not, however, be required in all circumstances. Moreover, the attempt to address law enforcement access in the recital is confusing and inappropriate in this context, as discussion on this complex and sensitive topic are taking place in other venues. We urge the recital be removed.