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

8 June 2022

ECIS commends the co-legislators in reaching an agreement on NIS 2

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. For further information, please see ECIS' website at www.ecis.eu and LinkedIn.

The 2016 EU Network Information Security Directive ("**NIS**") set baseline requirements for a high common level of network and information security across the European Union. ECIS has been engaging with stakeholders on the topic of cybersecurity through position papers and webinars since 2016. In November 2021 we hosted an online event on digital sovereignty and cybersecurity involving different stakeholders and earlier in 2021 we provided our initial feedback on the NIS revision.

We support the EU's wide ranging efforts to modernise EU law and bolster the cyber-resilience from critical infrastructures to consumer Internet of Things devices. The industry has had to step up resilience activities related to recent experiences: during the COVID-19 pandemic critical infrastructures were attacked by cybercriminals using ransomware for financial gain and during the recent nation state attacks on Ukraine critical facilities were targeted to disrupt and disable societies further.

ECIS strongly supports the following elements in the agreed NIS 2 text:

- introducing voluntary cyber threat sharing between both governments and companies;
- broadening the scope of entities that are required to raise their resilience compared to NIS 1 – which is an important step to raising cybersecurity resilience in Europe;
- boosting the powers and international cooperation of national Computer Security Incident Response Teams ("**CSIRT**");
- using comprehensive risk management principles based on international standards.

On the last point, ECIS believes that setting a basis in international cybersecurity and information security standards such as, *e.g.*, the ISO 27000 series of standards, is crucial. Cybersecurity policy measures should not be used by geographical regions to pursue digital sovereignty objectives. Systemic risk and the need for resilience in Europe's strategic sectors do not begin and end at the geographical borders of the EU. Europe should remain open and strengthen partnerships with trusted players to ensure that companies and governments in the EU have the flexibility needed to pursue their business and digital transformation journeys. Moreover, we welcome the decision by the EU to continue to use and rely on the established international Common Vulnerabilities and Exposures system and reflect this in an EU database as opposed to creating a duplicative registry which would run the risk of creating additional cost and complexity without additional resilience.

Furthermore, measures to increase the uptake of open standards and open source solutions in cybersecurity services should be welcomed. Open standards and open source solutions allow users better interoperability between services which are otherwise siloed for cybersecurity operations. ECIS welcomes the reference in draft Recital 26/c to on one hand Open Standards and their important role in facilitating interoperability between security tools. And on the other hand the recognition of open source software in making community vulnerability and thread sharing easier. ECIS published a paper on the importance of openness and interoperability in cybersecurity in 2019, supporting this approach.[1]

Additionally, we welcome the effort to increase cyber resilience across member states, and the legal recognition that security research activities undertaken to enhance the security of cyberspace are permitted under the General Data Protection Regulation.

[1] http://www.ecis.eu/wp-content/uploads/2019/10/White-paper-on-The-importance-of-openness-and-interoperability-in-cybersecurity-and-cloud-services.pdf

ECIS believes the following matters would still need to be addressed:

- Incident notification and timelines

  We believe that a blanket 24-hour notification window as an early warning of an incident would prove ineffective without related guidance on the substance and form of the initial “light” notification. A notification without relevance or context provides no valuable or actionable information. On the contrary, such a notification without actionable content potentially overwhelms competent authorities or CSIRTs. ECIS supports a compromise that clarifies what is to be reported in the early window of an incident.

- Information sharing

  Cybersecurity is a shared problem; therefore, information sharing is crucial. Threat-information is the lifeblood of cyber defence. ECIS strongly supports robust, real-time information sharing of threat-data through voluntary Information Sharing and Analysis Centres to help protect citizens and organizations from cyber-attacks. Governments should facilitate efforts to establish more sector specific initiatives of this kind.

- Future regulatory collaboration to ensure optimal cyber-resilience

  In light of the large number of existing and future cybersecurity related regulatory activities (from Cybersecurity Act schemes and Radio Equipment Directive delegated acts to the Digital Operational Resiliency Act) it is critical that the European Commission ("**Commission**") ensures a fully coordinated regulatory approach to create synergies and thus avoid unnecessary regulatory overlap or operational confusion. Moreover, much of the implementation detail of the NIS 2 will be driven by delegated acts and implementation acts, as such, we urge the Commission to ensure that technical and operational expertise is sought throughout the process to ensure best available technology and operational practices are reflected. ECIS remains concerned that national and European cyber certification interests are often prioritised over the actual operational collaboration and the development of an international cyber-security community to actually fight off ever more complex attacks.