

EN

E-002367/2025

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(1.8.2025)

The Commission monitors closely the cybersecurity situation in relation to critical infrastructure. Under the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)¹, essential and important entities must report any significant cyber incidents to their national Computer Security Incident Response Team (CSIRT) or competent authority without undue delay and within 24 hours of becoming aware.

The EU has strengthened the legislative framework regarding the cybersecurity of critical infrastructure. The NIS2 Directive increases the overall level of cybersecurity across 18 critical sectors, by requiring critical entities to implement cybersecurity risk-management measures, such as incident handling and business continuity. Among these critical sectors are the public administration and water transport sector, including managing bodies of ports and entities operating works and equipment contained within ports or operators of vessel traffic services.

Finally, the Commission has started preparations for an EU Ports Strategy², which includes cybersecurity as an area of focus, and is inviting stakeholders to participate in the process.

¹ Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).

² See: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14659-EU-Ports-Strategy_en.