

EN

P-003058/2026

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(3.9.2026)

Under Directive (EU) 2022/2555¹ (the NIS2 Directive), Member States must ensure that certain public administration entities take cybersecurity risk-management measures and report significant incidents. However, the Commission is not a recipient of such reports, since significant incidents have to be reported to a computer security incident response team (CSIRT) or a competent authority at national level. At the request of a member of the CSIRTs network, the CSIRTs network can discuss information in relation to a specific incident. Further, a Member State may request the European Union Agency for Cybersecurity (ENISA) to provide support in relation to ex-post technical inquiries into significant incidents under Regulation (EU) 2019/881². The EU Cybersecurity Reserve, established under the Cyber Solidarity Act³, can support Member States in addressing significant or large-scale cybersecurity incidents by offering a pool of trusted providers for incident response.

Since the entry into force of the NIS2 Directive, the Commission has been actively supporting Member States in their transposition efforts. Romania has notified the Commission of the complete transposition of the Directive. The Commission is currently evaluating the level of completeness and compliance of the national transposition measures. The Commission remains fully committed to assisting Member States' efforts in transposition and implementation of the Directive.

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 (NIS 2 Directive), OJ L 333, 27.12.2022, pp. 80-152.

² Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, pp. 15–69.

³ Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), OJ L, 2025/38, 15.1.2025.