

EN

E-003112/2026

Answer given by Executive Vice-President Virkkunen
on behalf of the European Commission
(2.10.2026)

The proposal for revision of the Cyber Security Act¹, currently under negotiation by co-legislators, sets out an objective and risk-based framework to address risks related to foreign interference and dependencies in the ICT Supply Chain in NIS 2 sectors².

For charging infrastructure specifically, the Risk Assessment on Connected and Automated Vehicles (CAV³) recommends that Member States apply the ICT Supply Chain Security Toolbox to ‘CAVs and related charging infrastructure’, including assessment of critical suppliers, multi-vendor strategies, reducing dependencies on high-risk suppliers and, where appropriate, restricting or excluding high-risk suppliers from critical supply chains. Risk assessments are legally of non-binding nature.

The proposal for revision of the Cyber Security Act⁴ sets out that the high-risk suppliers, as defined in the proposed act, shall not be entitled to participate in any activities under EU funding programmes and instruments implemented in direct and indirect management in accordance with Article 136 Regulation (EU, Euratom) 2024/2509 and EU sector-specific rules as well as in any EU funding activities implemented in shared management in relation to the provision of ICT components or components that include ICT components to be used in key ICT assets as identified in accordance with the Regulation.

¹ <https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act>.

² <https://digital-strategy.ec.europa.eu/en/news/ict-supply-chain-security-eu-adopts-toolbox-mitigate-risks>.

³ <https://digital-strategy.ec.europa.eu/en/library/toolbox-improve-ict-supply-chain-security>.

⁴ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0011>.