An industry call for a clear, proportionate and risk-based European Trusted ICT Supply Chain Framework under the revised Cybersecurity Act (CSA2)

Executive summary: We call on the co-legislators to ensure that every measure under the CSA2 Trusted ICT Supply Chain Framework starts from a prior, evidence-based risk assessment conducted with industry. The revised framework should guarantee graduated and proportionate mitigation, with prohibition only as a last resort, as well as legal certainty, fair treatment of compensation and realistic and feasible timelines.

Dear Rapporteur, Shadow Rapporteurs and Member State representatives,

The undersigned associations represent Europe's strategic industries: connectivity, electricity distribution and digital infrastructure, including cloud and data centres, energy, automotive and manufacturing, health technology, and finance. We support the objective of the revised Cybersecurity Act. Stronger cybersecurity, greater resilience and genuine simplification are goals we advance every day.

However, there are several areas of concern which need to be raised and further addressed during the institutions' negotiations on the Trusted ICT Supply Chain framework in Title IV. Introducing targeted adjustments would help avoid unnecessary complexity while preserving the core EU objectives of resilience, innovation and competitiveness, the Union's cloud and AI capacity objectives under the Cloud and AI Development Act, and the energy transition.

Our shared recommendations are the following:

➤ **High-risk designation must rest on clear evidence-based criteria, while also considering the broader cybersecurity, resilience, and strategic dependency context relevant to critical infrastructure.** High-risk status should follow a genuine risk assessment of the technology concerned, considering technical cybersecurity criteria and demonstrable security risks within the context of the specific critical infrastructure. This should also account for existing strategic dependencies, including those dependencies that would be caused in the event of ICT technology prohibitions.

➤ **Clarity on the notion of 'ICT component'.** Supplier-based restrictions should apply only where a genuine supplier relationship exists, i.e. where the supplier retains the ability to update, access or influence the component once deployed. This should apply both to software and hardware. As a consequence, any reference in CSA2 proposal to

"components that include ICT components to be used in key ICT assets" should be clarified or deleted to ensure the legal certainty.

➤ **Mitigation before prohibition.** The framework provides excessive discretion to the Commission and allows prohibitions to be triggered far too quickly, without genuine consideration of the existing catalogue of risk mitigation measures affected sectors and entities already apply and without any previous consultation with Member States and stakeholders. Consultation of, and assessment of the implications on, the impacted industry stakeholders is paramount from the outset of any EU risk assessment to ensure it duly considers the practicalities and realities of the market. This includes effective impact assessments and timelines to replace suppliers designated as 'high-risk'. Such impact assessments should explicitly evaluate the consequences for supply chain resilience, product availability, continuity of critical services, and the competitiveness of European industry. In particular, certain critical dependencies cannot realistically be replaced in the short to medium-term without the risk of significant societal, economic and operational implications including disruption to critical services.

➤ **Proportionality and legal certainty.** Title IV overregulates, or conflicts with, principles that already exist within horizontal and sector-specific regulation, including the Network and Information Security Directive II (NIS2), the Digital Operational Resilience Act (DORA), the Cyber Resilience Act (CRA), the AI Act, the European cybersecurity certification schemes, UN Regulation 155 on vehicle cybersecurity or the Medical Devices Regulations (IVDR/MDR). For several already heavily regulated sectors, this creates duplication, legal uncertainty and a disproportionate burden. Any additional requirements should be designed to complement existing sectoral frameworks rather than create parallel compliance expectations or duplicate existing obligations. Furthermore, risk assessments need to be driven by sector-specific considerations. More broadly, adding a new layer of regulation runs contrary to the simplification the Union has promised.

➤ **Fair competition and consistent obligations.** The CSA2 would apply only to entities carrying out their activities in the EU, creating a disproportionate advantage for non-EU entities in the sectors concerned, who can serve the EU market without bearing the same obligations as European entities. Any CSA2 obligations applicable to products, services or software within the defined scope should therefore be applied consistently to those placed on the EU market, regardless of origin, while preserving the ability of authorities to take proportionate risk-based measures where justified by security assessments. Fair competition also means preserving alignment with international standards, which allows European companies to serve customers in the EU and third countries without duplicating compliance.

➤ **Market openness and supplier resilience.** Supplier restrictions should carefully consider operational feasibility, service continuity, existing technological dependencies, and asset lifecycles. Across all sectors, restrictions should be implemented in a manner that strengthens security while avoiding the creation of new dependencies, concentration risks or unintended impacts on long-term supply chain resilience.. Restricting data-centre operators' access to hardware and AI components, in particular excluding openly released AI models by origin, would raise costs, slow the capacity build-out the Union seeks to accelerate under the Cloud and AI Development Act, and leave Europe reliant on a handful of proprietary non-EU models.

➤ **Governance, consultation and legal certainty.** Where the framework relies on secondary legislation to designate high-risk suppliers, such measures should rest on three safeguards: a prior risk assessment, meaningful consultation of Member States and affected industry stakeholders, as well as transparent governance and oversight mechanisms. Given their geopolitical nature, the designation of third countries and of high-risk suppliers and the identification of key ICT assets should be endorsed by Member States, through the Council or at minimum under the examination procedure. Such safeguards are essential to ensure proportionality, predictability and legal certainty, while supporting a coordinated European approach and preserving the integrity and consistent functioning of the Single Market.

➤ **A responsible use of public money.** Mandatory removals and replacements of ICT technologies across supply chains will inherently require substantial technical, operational and financial resources from companies. Whether such costs are borne by the entities concerned or by national budgets, they risk undermining the competitiveness of European companies or straining public finances already under pressure from an ageing population and the financing needs of the digital and green transitions.

To that end, we ask co-legislators to ensure that every measure under the CSA2 Trusted ICT Supply Chain Framework starts from a prior, evidence-based risk assessment conducted with industry. The revised framework should guarantee graduated and proportionate mitigation, reserving prohibition for cases where less restrictive measures cannot adequately address the identified risks. It should also provide legal certainty, fair treatment of compensation and realistic and feasible timelines, while avoiding regulatory overlap and unnecessary administrative burdens. This approach is essential to support European innovation, competitiveness and cybersecurity resilience.

We would welcome the opportunity to share our operational expertise with you. Given the advanced status of the proposal an exchange before the file progresses further would be timely.

Yours faithfully,

Signatories

- **Connect Europe**, representing European telecommunications operators *(connectivity)*
- **GSMA Europe**, representing European mobile network operators *(mobile telecoms)*
- **ACEA**, representing Europe's 17 major car, van, truck and bus manufacturers *(automotive)*
- **CISPE** – Cloud Infrastructure Services Providers in Europe, representing European cloud infrastructure providers *(cloud and data-centre infrastructure),*
- **EuroISPA,** representing Europe's Internet Services Providers *(internet services / digital infrastructure)*
- **E.DSO**, representing 37 of Europe's leading distribution system operators (DSOs), electricity only, which jointly serve the majority of Europe's electricity customers (*energy*)
- **MedTech Europe,** representing the medical technology industry, including diagnostics, medical devices and digital health (*medtech*)
- **COCIR**, representing the medical imaging, radiotherapy, health ICT and electromedical industries (*medical devices and equipment*)