

CoESS-Euralarm Joint Statement

On the proposal for a Cybersecurity Act 2

Brussels, 13 October 2026

The European security industry, represented by Euralarm and the Confederation of European Security Services, supports the objectives of the European Commission's proposal for a Cybersecurity Act 2 and the establishment of a Trusted ICT Supply Chain Framework under Title IV. Europe's critical entities must be able to rely on secure and resilient technologies, and dependencies creating genuine cybersecurity risks need to be addressed.

The security industry would be one of the sectors affected by this new regime. Euralarm and CoESS therefore want to contribute to making this framework a success and ensure that it is also workable and effectively applicable across the entire security chain of NIS2 entities - from technology developers and manufacturers to integrators, installers and private security service providers. To achieve this, we call on the co-legislators to strengthen Title IV in four key areas:

- 1. Ensure structured consultation of all affected stakeholders in ICT supply-chain risk assessments;***
- 2. Ensure transparent, evidence-based and proportionate risk assessments and mitigation measures;***
- 3. Assess operational and economic impacts across the full affected value chain; and***
- 4. Ensure realistic alternatives and transition periods that safeguard continuity of security operations.***

These principles are important because restrictions imposed on ICT products may have significant consequences beyond the NIS2 entities directly subject to them. In our industry, they can affect manufacturers, integrators, installers and security service providers and, ultimately, the continuity and availability of security systems protecting critical and essential entities.

A cybersecurity mitigation measure should therefore not inadvertently create new operational or physical-security risks that undermine the resilience it is intended to strengthen. In this sense, we also underline that the Cybersecurity Act 2 should avoid creating unnecessary overlaps or redundancies with existing requirements stemming from EU law: the current NIS2 framework already imposes, albeit indirectly, cybersecurity-related obligations on security service providers operating for entities within the scope of the Directive. In addition, the Cyber Resilience Act already establishes cybersecurity requirements for cybersecurity products and equipment.

The security industry is part of the operational security chain of NIS2 entities

The European security industry provides technologies, systems and services to a broad range of entities covered by Annexes I and II of the NIS2 Directive. This includes the development and manufacture of security technologies, their integration and installation at client sites, as well as operational services such as access control, video surveillance, alarm monitoring and response. Increasingly, these services and solutions depend on connected security technologies.

The Cybersecurity Act 2 proposal itself recognises this relevance. Recital 133 explicitly identifies detection equipment, drones and counter-drone systems and surveillance equipment among the critical ICT supply chains in which cybersecurity risks may arise. The operational reality of the security industry, and the possible impact of the Trusted ICT Supply Chain Framework across the security value chain, should therefore be fully reflected in the Regulation.

Security technologies deployed at an NIS2 entity are not necessarily developed, purchased, owned, integrated, maintained or operated by that entity itself. Different parts of the security industry may be responsible for manufacturing the equipment, integrating and installing systems, maintaining them throughout their lifecycle, or operating them as part of a long-term security service contract.

Restrictions or phase-out measures under Article 103 could therefore have consequences throughout this chain. They may require manufacturers and integrators to adapt product portfolios and system architectures, installers to replace and recommission equipment, and security service providers to replace equipment before the end of its economic lifecycle, redesign integrations, source alternative solutions, retest systems, retrain personnel and renegotiate existing contracts - potentially under significant time pressure. This may create stranded investments and, where suitable alternatives cannot be deployed in time, risks to the continuity of security operations themselves.

Our recommendation: a full security value chain and operational continuity approach

We therefore recommend that the co-legislators strengthen Title IV in four areas to ensure that the Trusted ICT Supply Chain Framework takes account of impacts across the full security value chain and can be implemented effectively in practice:

1. Consult all affected stakeholders when assessing ICT supply chains.

Article 99 entrusts the NIS Cooperation Group with Union-level coordinated security risk assessments, including the identification of key ICT assets, threat actors, risks and vulnerabilities. Yet there is no general obligation to consult the European businesses that develop, manufacture, integrate, install, maintain or operate the technologies concerned at NIS2 entities.

The NIS Cooperation Group should therefore be required to consult relevant affected stakeholder groups throughout the security value chain as part of security risk assessments and before key ICT assets and mitigation measures are determined. This is essential to understand actual deployment models, technical dependencies, replacement possibilities, product lifecycles and operational consequences.

2. Make risk assessments transparent, predictable and strictly security-based.

Articles 99 and 102 provide an important starting point, but businesses need greater transparency on how individual ICT supply chains and assets will be assessed and how the criteria in Article 102(2) will be applied in practice.

Assessments should identify concrete and demonstrable cybersecurity risks, based on transparent and objective evaluation criteria and a consistent methodology. Decisions under the Trusted ICT Supply Chain Framework should remain grounded in the cybersecurity and supply-chain security objectives of the Regulation and be based on clearly defined, objective and consistently applied criteria. Greater

transparency and predictability are essential for businesses across the value chain to anticipate possible measures, plan future investments and adapt product and service strategies in good time.

3. Assess economic impacts along the entire affected value chain – not only at NIS2 entities.

Article 103(4)(b) requires the Commission to assess the potential economic and societal impact of mitigation measures on entities covered by Annexes I and II of the NIS2 Directive. Recital 144 rightly requires consideration of implementation costs and the lifecycle of components.

However, neither provision sufficiently reflects the costs that may arise elsewhere in the security value chain as a direct consequence of obligations imposed on NIS2 entities. These may affect European manufacturers, integrators, installers and service providers that have invested in, supplied, installed, maintained or operate the technology concerned.

Economic assessments should therefore cover the full affected value chain and take account of the actual allocation of ownership, investment and contractual responsibility. Costs resulting from regulatory replacement requirements should not simply be transferred from NIS2 entities to their European suppliers and service providers. Where mandatory accelerated replacement creates substantial stranded investment that cannot reasonably be absorbed through normal investment cycles, appropriate EU or national financial support should be considered.

4. Guarantee realistic alternatives and transparent transition plans.

We strongly support the requirement in Article 103(4)(c) to assess the availability of alternative suppliers. For security technologies and services, however, this must mean more than the theoretical presence of another supplier on the EU market.

Alternative solutions must be technically suitable, interoperable, available at the necessary scale, deployable within the required timeframe and capable of maintaining the required level and continuity of security operations.

Article 103(1) already requires appropriate transition and phase-out periods, while Recital 144 requires account to be taken of component lifecycles and continued service provision. These principles should be translated into transparent migration, transition and phase-out plans developed with affected stakeholders across the security value chain. Developers, manufacturers, integrators, installers, service providers and their NIS2 clients need sufficient time to identify and validate alternatives, adapt products and systems, replace and test equipment, adjust contracts, train personnel and ensure uninterrupted security operations.

Secure ICT supply chains are indispensable for Europe's resilience. The European security industry supports this objective and wants to help make the new framework a success. Achieving this requires a full value-chain approach. Cybersecurity measures should be based on transparent and demonstrable risk assessments, proportionate to the risks identified, informed by the expertise of affected stakeholders and accompanied by realistic implementation and transition arrangements.

Euralarm and CoESS therefore call on the European Parliament and the Council to strengthen Articles 99-103 by embedding stakeholder consultation, proportionality, full value-chain impact assessment and operational continuity into the Trusted ICT Supply Chain Framework.

We also encourage the European Commission and the NIS Cooperation Group to establish a structured dialogue with affected sectors when developing coordinated security risk assessments and subsequent mitigation measures.

About CoESS

CoESS acts as the voice of the private security industry, covering 23 national associations across Europe and representing 45,000 companies with 2 million security officers. Private security provides a wide range of services for private and public clients, ranging from Critical Infrastructure to public spaces – including guarding, remote surveillance, alarm monitoring and response. CoESS is member of multiple EU Expert Groups and recognised by the European Commission as the EU employers' organisation representative active in EU Sectoral Social Dialogue with UNI Europa.

About Euralarm

Euralarm represents the electronic fire and security industry, providing leadership and expertise for industry, market, policy makers and standards bodies. Our Members make society safer and secure through systems and services for fire detection and extinguishing, intrusion detection, access control, video monitoring, alarm transmission and alarm receiving centres. Founded in 1970, Euralarm represents over 5000 companies within the fire safety and security industry valued at 67 billion Euros. Euralarm Members are national associations and individual companies from across Europe.