

OCTOBER 2026

Cybersecurity Act 2 and mobility: ensuring proportionate and workable ICT supply-chain rules for connected vehicles

Executive summary

The proposed **Cybersecurity Act 2** would establish a binding EU framework for addressing non-technical risks in critical ICT supply chains. DIGITALEUROPE supports the objective of a **harmonised, evidence-based** approach. Its application to mobility must, however, account for the sector's existing mandatory cybersecurity framework, integrated vehicle architectures, long development and service lifecycles, and global manufacturing networks. The relevance and proportionality of any future measure should depend on the presence and criticality of the ICT functions concerned. Vehicles and manufacturers differ in their levels of connectivity, remote-access capabilities and exposure to ICT supply-chain risks; measures should be targeted accordingly.

This paper identifies **four priorities** for ensuring that the Trusted ICT Supply Chain Framework is effective and workable for the mobility sector:

- ▶▶ **Build on the existing automotive cybersecurity framework.** CSA2 should complement the requirements already established under UN Regulation No. 155 and the EU vehicle type-approval framework. Additional measures should focus on clearly identified risks that are not already adequately addressed, without duplicating technical controls, supplier oversight or existing evidence.
- ▶▶ **Treat comparable risks consistently across the EU market.** CSA2 should not impose additional requirements on EU manufacturing while leaving equivalent cybersecurity risks unaddressed in comparable imported vehicles. Where its entity-based structure cannot ensure equivalent treatment, measures affecting vehicle design or functionality should be addressed through appropriate product-based rules applying to all vehicles placed on the EU market.
- ▶▶ **Prioritise proportionate mitigation and treat prohibition as a last resort.** Restrictions and phase-out periods must reflect the technical substitutability and maturity of alternatives, as well as automotive development, validation, production, type-approval and service lifecycles.



- 
- **Target supplier-information requests to critical assets and suppliers.** Transparency requirements should be linked to clearly identified key ICT assets and specific risks. They should reuse existing information where possible, remain proportionate and feasible across complex multi-tier supply chains, and protect confidential and security-sensitive information.

Together, these recommendations would make the Trusted ICT Supply Chain Framework more precise, proportionate and workable for the mobility industry. They would support stronger cybersecurity while preserving regulatory coherence, the integrity of the Single Market and the **competitiveness** of European manufacturing.

DIGITALEUROPE seeks a framework that applies proportionately, without duplicating existing vehicle rules, disrupting validated vehicle programmes, or creating an uneven playing field between EU-manufactured and comparable imported vehicles. The following **suggested safeguards** would make the Trusted ICT Supply Chain Framework more precise, more implementable and more likely to strengthen security without unintended industrial consequences.

Table of contents

Executive summary.....	1
Table of contents.....	3
Build on Europe's existing automotive cybersecurity framework	4
CSA2 should complement, rather than duplicate, established vehicle-security rules	4
Existing UN R155 evidence should be the starting point for additional assessments	4
Ensure equivalent risks are treated consistently across the EU market.....	4
An entity-based framework must not disadvantage EU manufacturing	4
Align transition periods with automotive development and vehicle lifecycles	5
Supplier restrictions must reflect validation, type approval and long service lives	5
Replacing a connected-vehicle platform involves more than changing suppliers	6
Target transparency requirements to the suppliers and assets that matter.....	6
Information requests must be proportionate, feasible and appropriately protected	6
Connected-vehicle supply chains show the need for targeted requests	7
A targeted framework can strengthen both cybersecurity and industrial resilience.....	7

Build on Europe's existing automotive cybersecurity framework

CSA2 should complement, rather than duplicate, established vehicle-security rules

DIGITALEUROPE calls for measures that are proportionate, evidence-based and applied only where identified non-technical risks cannot be adequately addressed under existing applicable rules.

The mobility sector already operates under a mandatory and audited cybersecurity framework. **UN Regulation No. 155** requires vehicle manufacturers to maintain a certified Cybersecurity Management System, assess and manage cybersecurity risks throughout the vehicle lifecycle, including risks linked to suppliers, and monitor vehicles after production. Compliance with these requirements is embedded in the EU vehicle type-approval framework.

Automotive cybersecurity is assessed at the level of the integrated vehicle and its systems. Measures targeting individual ICT components or suppliers may therefore interact with an established **system-level architecture** covering safety, cybersecurity and type approval. Connected vehicles should not be subject to **overlapping** cybersecurity frameworks pursuing the same objectives. CSA2 should focus on residual risks not already adequately covered and should avoid duplicate assessments, parallel evidence requirements, overlapping technical controls or additional compliance obligations that would increase complexity and costs without necessarily improving security.

At the same time, regulatory approaches should recognise the distinction between technical cybersecurity vulnerabilities and broader strategic or geopolitical considerations. In the automotive sector, cybersecurity risks affecting vehicles and their systems are already systematically addressed through the existing regulatory framework, notably UN Regulation No. 155, which requires manufacturers to identify, assess and mitigate risks across the vehicle lifecycle, including those linked to suppliers. Concerns related to supplier dependencies, foreign state influence or similar **non-technical** factors raise important policy questions, but differ in nature from technical cybersecurity risks and should therefore be assessed through appropriate policy instruments rather than additional cybersecurity obligations.

Existing UN R155 evidence should be the starting point for additional assessments

Annex 5, point 5.1.1(a), of UN Regulation No. 155 requires manufacturers to collect and verify information throughout the supply chain so that supplier-related risks are identified and managed.

Where a future CSA2 measure concerns a vehicle connectivity or control system, the Commission should first draw on relevant Cybersecurity Management System documentation and type-approval evidence, subject to appropriate confidentiality safeguards. Any additional requirement should be limited to residual non-technical risk, such as exposure to third-country influence, and should not duplicate supplier mapping, technical testing or mitigation controls already demonstrated under the automotive framework.

Ensure equivalent risks are treated consistently across the EU market

An entity-based framework must not disadvantage EU manufacturing



DIGITALEUROPE warns that an **entity-based approach** may create competitive distortions if obligations apply to manufacturing activities carried out in the Union while comparable vehicles manufactured outside the EU and placed on the same market are not subject to **equivalent measures**.

The automotive industry is organised around global vehicle platforms, integrated supply chains and manufacturing networks. The same vehicle model, architecture or ICT component may be used across several production sites. Depending on the scope of a future implementing act and the corporate structures concerned, an EU manufacturing entity could be required to replace a supplier, provide additional information or introduce mitigation measures, while a comparable imported vehicle could continue to contain the same component.

Such an outcome would be problematic for both **competitiveness** and **security**. It would concentrate, for example compliance costs on **EU manufacturing** without necessarily addressing the equivalent cybersecurity risk in vehicles imported into and used within the Union, ultimately preventing the necessary level playing field for market competitiveness.

The implementation of CSA2 should therefore ensure that comparable risks are treated consistently across the EU market. The place of final assembly should not, by itself, determine whether a vehicle presenting a particular cybersecurity risk is subject to regulatory intervention.

However, where the entity-based structure of CSA2 cannot ensure equivalent treatment of imported vehicles, any measures directly affecting vehicle design, components or functionality should be implemented through appropriate product-based legislation applying equally to all vehicles placed on the EU market, regardless of where they are manufactured. This would preserve the integrity of the EU type-approval framework and ensure a level playing field between EU-manufactured and imported vehicles.

Align transition periods with automotive development and vehicle lifecycles

Supplier restrictions must reflect validation, type approval and long service lives

DIGITALEUROPE calls for sufficient **transition and phase-out periods**, robust economic and operational **impact assessments**, and proper consideration of the availability and maturity of **alternatives** before restrictions are imposed.

Replacing an automotive supplier is not comparable to changing a conventional IT vendor. Vehicle hardware and software architectures are typically defined and validated years before market launch. Replacing a safety- or cybersecurity-relevant component may require structural engineering redesign, hardware and software integration, component requalification, cybersecurity and functional-safety assessments, production changes and, where applicable, updates to type-approval documentation.

The practical consequences also differ between new vehicle programmes, vehicles already in production and the installed fleet. Vehicles remain in service for many years, during which manufacturers must maintain software support, replacement parts and repairability. Transition and phase-out periods designed around conventional ICT replacement cycles may therefore be unworkable and could create additional safety, continuity and compliance risks.





Article 103 already requires appropriate transition and phase-out periods and consideration of alternative suppliers. For mobility, however, the existence of another supplier on the market is not sufficient. The assessment must determine whether the **alternative** is:

- ▶▶ technically substitutable;
- ▶▶ sufficiently mature and validated;
- ▶▶ available at the required production scale;
- ▶▶ compatible with the relevant vehicle architecture; and
- ▶▶ ready to meet applicable safety, cybersecurity and type-approval requirements.

Prohibitions should consequently remain a measure of last resort, used only where the identified risk cannot be adequately addressed through less restrictive mitigation measures. Where a prohibition is necessary, its implementation timeline must reflect automotive development, production and service lifecycles.

Replacing a connected-vehicle platform involves more than changing suppliers

Replacing a telematics control unit or central compute platform can affect the vehicle gateway, remote diagnostics, emergency-call functions, over-the-air updates and interfaces with safety-relevant systems.

Even where an alternative supplier is available, introducing a replacement may require changes to the vehicle's electronic architecture, new hardware and software integration, component qualification, renewed cybersecurity and safety validation, updates to approval documentation and new spare-parts and maintenance arrangements.

Where the identified risk can instead be **reduced through measures** such as network segmentation, restricted remote access, continuous monitoring or independently audited operational controls, these measures may improve security more quickly and with less disruption than an immediate supplier prohibition.

Target transparency requirements to the suppliers and assets that matter

Information requests must be proportionate, feasible and appropriately protected

DIGITALEUROPE supports **structured consultation** with affected companies and **clear guidance on supplier-information requests**. Any such requirements should be necessary, proportionate and subject to robust confidentiality safeguards.

Article 103(2)(a) would allow the Commission to introduce supplier-transparency requirements concerning key ICT assets. In mobility, these requirements would apply to highly complex and multi-tier ecosystems





encompassing vehicle manufacturers, control-unit suppliers, semiconductor manufacturers, embedded and open-source software, connectivity providers, cloud services and AI-enabled computing platforms.

An unbounded requirement to map every supplier involved in every component containing ICT could therefore generate large volumes of information that are difficult to maintain, quickly become outdated and may have limited relevance to the identified risk.

Information requests should consequently be linked to:

- ▶▶ the key ICT asset identified under Article 102;
- ▶▶ the specific non-technical risk under assessment;
- ▶▶ suppliers materially involved in the functioning, control or security of that asset; and
- ▶▶ information that is necessary, relevant and reasonably available to the affected entity.

Requirements should reuse relevant information already collected, while recognising that additional information may be necessary to assess matters such as supplier ownership, control or exposure to third-country influence.

The framework must also protect **trade secrets, intellectual property, commercially sensitive information and security-relevant details**. Guidance should clearly identify the information required, the relevant supplier tier, the recipient authority, the permitted use of the information, the reporting format, applicable deadlines and the expected frequency of updates.

Early **industry consultation** is essential. Manufacturers and suppliers can help the Commission determine whether the requested information exists, which supply-chain actor holds it, how it can be provided securely and whether it would meaningfully support the relevant risk assessment.

Connected-vehicle supply chains show the need for targeted requests

A connected-vehicle function may involve an OEM, a Tier 1 controller, semiconductor and firmware suppliers, open-source software libraries, a cellular communications module and a cloud-service provider.

A request to **identify every contributor** to every electronic component would be costly to implement, difficult to keep current and unlikely to provide a clear picture of the risk under assessment.

A more targeted request could focus on suppliers that exercise privileged access, remote-update capabilities, operational control or another material influence over a key connectivity or vehicle-control function. This would provide information that is more relevant to the identified non-technical risk while avoiding indiscriminate mapping of the entire vehicle supply chain.

A targeted framework can strengthen both cybersecurity and industrial resilience

As the mobility sector is operating cross border, the EU framework should be fully **harmonised** across the Single Market.





The CSA2 will be most effective if intervention is focused on clearly identified key ICT assets and risks that are not already adequately addressed through existing requirements, taking into account the presence and criticality of the relevant ICT functions. Decisions should be evidence-based, reflect the technical and regulatory realities of the automotive sector, and be developed through early and structured engagement with the companies expected to implement them.

The recommendations set out in this paper would support preserving the security objectives of CSA2 while ensuring that its implementation:

- ▶▶ builds on existing automotive cybersecurity and type-approval requirements, including UN Regulation No. 155, rather than duplicating technical controls or evidence;
- ▶▶ addresses comparable cybersecurity risks consistently across EU-manufactured and imported vehicles via product-based regulation;
- ▶▶ prioritises proportionate mitigation and treats prohibition as a last resort, with transition and phase-out periods reflecting vehicle development, validation, production and service lifecycles; and
- ▶▶ targets supplier-information requests at the key ICT assets, suppliers and information relevant to the identified risk, while protecting confidential and security-sensitive information.

Together, these safeguards would make the Trusted ICT Supply Chain Framework more precise, proportionate and workable for mobility. They would support stronger cybersecurity while preserving regulatory coherence, the integrity of the Single Market and the competitiveness of European manufacturing.



FOR MORE INFORMATION, PLEASE CONTACT:

 Francesco Alemani

Policy Officer for Mobility and Sustainability

francesco.alemani@digitaleurope.org / +32 490 44 20 68

THE VIEWS EXPRESSED IN THIS STUDY ARE THOSE OF DIGITALEUROPE AND DO NOT NECESSARILY REFLECT THE POSITIONS OF ITS INDIVIDUAL MEMBER ORGANISATIONS OR CONTRIBUTORS.

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory and investment environment that enables European digitalising businesses across multiple sectors and citizens to prosper from digital technologies. We wish for Europe to grow, attract and sustain the world's best digital talents, investment and technology companies. Together with our members, we shape industry positions on all relevant policy matters, and contribute to their development and implementation. Our membership represents over 56,000 businesses who operate and invest in Europe. It includes corporations and scaleups who are global leaders in their field of activity, as well as national trade associations from across more than 30 European countries.