BMW Group Position on the Cybersecurity Act II (CSA 2)

Executive Summary

- The BMW Group supports the EU's objective of strengthening cybersecurity and enhancing the resilience of ICT supply chains.
- Cybersecurity for motor vehicles is already comprehensively and bindingly regulated under a mature and globally recognized sector-specific framework, in particular UNECE Regulation No. 155 within EU type-approval legislation.
- The key challenge lies not in the absence of rules, but in the effective and coherent enforcement of the existing vehicle cybersecurity framework.
- CSA 2 follows a horizontal, entity-based regulatory approach that is structurally unsuited to product-based systems such as motor vehicles. As a result, manufacturing activities within the EU are disproportionately affected, while comparable products placed on the EU market by non-EU entities remain out of scope.
- CSA 2 would neither achieve its overarching political objective of ensuring cyber-secure vehicles on European roads -since imported vehicles would not be covered- nor would it provide additional cybersecurity benefits beyond existing regulations such as UN R155.
- Additional requirements under CSA 2 would lead to regulatory duplication, legal uncertainty, and inconsistent interpretation and application of existing frameworks.
- Non-technical and geopolitical considerations, such as supplier dependencies, should be clearly distinguished from cybersecurity risks and carefully assessed, as trade-restrictive measures risk triggering countermeasures, increasing regulatory fragmentation, and undermining free and fair trade.

Solution: Instead of introducing additional regulation for vehicle cybersecurity, an effective enforcement mechanism should be established based on the existing regulatory framework.

1. Cybersecurity in Vehicles: A Mature Sector-Specific Framework

Modern vehicles are highly complex, software-defined, and increasingly connected systems. Cybersecurity is therefore an integral element of vehicle design, development, production, and operation throughout their lifecycle. In the EU, vehicle cybersecurity requirements are comprehensively regulated under UN R155, which is legally anchored in EU type-approval legislation and applies to all vehicles placed on the EU market, regardless of origin.

UN R155 establishes a binding, risk-based, and lifecycle-oriented framework based on two pillars: certification of a Cybersecurity Management System (CSMS) and cybersecurity type approval for each vehicle type. The regulation already explicitly addresses the supply chain. Annex 5 requires consideration of a comprehensive threat catalogue, including supplier- and component-related compromise scenarios, malicious software or hardware manipulation, and risks associated with remote updates.

Vehicle cybersecurity cannot be assessed solely on the basis of individual components. It must be evaluated at the vehicle level, treating the vehicle as an integrated system. Given the existence of this comprehensive sector-specific framework, introducing additional horizontal requirements under CSA 2 would result in regulatory duplication. This would create inconsistencies in interpretation, uncertainty regarding responsibilities and competencies, and an increased risk of misapplication, ultimately leading to heightened litigation risks. Furthermore, the distinction between "technical" and "non-technical" risks does not justify a separate horizontal regime, as UN R155 already requires governance structures, supplier risk management, and organizational controls that inherently address such risks at system level. Vehicles and vehicle manufacturing should therefore be excluded from the 'Trusted ICT Supply Chain Framework' under CSA 2 in order to avoid overlapping obligations.

2. Structural Mismatch of CSA 2 for Automotive Products

CSA 2 introduces a Trusted ICT Supply Chain framework under Title IV that applies to entities listed in Annexes I and II of the NIS 2 Directive carrying out activities within the Union. By design, this entity-based framework applies only to activities conducted within the EU.

As a result, vehicles manufactured outside the EU by non-EU entities and placed on the EU market would not be subject to CSA 2 supply chain obligations. EU-based manufacturers, by contrast, would face additional requirements not imposed on non-EU competitors offering comparable products on the same market. This creates an inherent and unavoidable competitive asymmetry and raises questions regarding the effectiveness of a cybersecurity regulation that lacks a comprehensive market-based approach.

This imbalance is intrinsic to the horizontal design of CSA 2 and cannot be remedied without transforming it into a product-based market-access framework. For globally traded products such as vehicles, CSA 2 is therefore not an appropriate regulatory instrument.

From an automotive perspective, the only coherent solution is to exclude manufacturing activities under point 5 of Annex II of NIS 2 from the Trusted ICT Supply Chain framework, thereby avoiding one-sided disadvantages for EU manufacturers.

3. Enforcement as the Critical Bottleneck and Key Lever

Experience with the implementation of UN R155 in the EU clearly demonstrates that the main challenge lies not in the absence of rules, but in their effective and consistent enforcement. In practice, assessments currently focus primarily on CSMS process reviews, while type-approval test cases often remain high-level and insufficiently concrete.

Competent authorities and technical services frequently face capacity and expertise constraints when assessing complex cybersecurity risks. Risk assessments for connected and automated vehicles explicitly identify these limitations as a major challenge. Introducing additional regulatory layers will not resolve this bottleneck if enforcement capabilities are not strengthened.

By contrast, other jurisdictions such as China, and increasingly the Republic of Korea - which also applies UN R155 - rely on clearly defined, concrete, and verifiable test cases integrated into the type-approval process. Translating identified risks into harmonized EU-wide test cases, derived directly from Annex 5 threat scenarios, would significantly strengthen enforcement, legal certainty, and real-world security outcomes without creating regulatory duplication.

4. Distinguishing Cybersecurity Risks from Non-Technical Objectives

Effective and proportionate regulation requires a clear conceptual distinction between cybersecurity risks and geopolitical considerations. Cybersecurity risks relate to the technical integrity, resilience, and safety of vehicles and related systems. These risks are already comprehensively addressed through UN R155 and UN R156 within the type-approval framework.

Non-technical considerations - such as dependencies on suppliers potentially subject to governmental or military influence - are policy-driven issues that extend beyond technical cybersecurity. From a broader policy perspective, trade-restrictive regulatory measures inevitably trigger countermeasures. Such actions risk increasing fragmentation and prompting retaliatory responses, with negative impacts on global value chains, resilience, and competitiveness. The BMW Group therefore strongly supports free and fair trade, open markets, and proportionate, risk-based regulation. Cybersecurity policy should enhance resilience without introducing unnecessary trade barriers or undermining long-standing international cooperation. Where perceived gaps exist, they primarily relate to enforcement challenges and specific supply chain scenarios—not to a structural absence of regulation.

5. Governance, Legal Certainty and Proportionality

Measures with significant economic and strategic implications, such as the identification or exclusion of high-risk suppliers, should not be introduced or substantially modified through implementing acts. Such decisions require robust governance safeguards, transparency, and meaningful involvement of Member States and the European Parliament, for example through qualified majority voting in the Council. Interventions in supply chains have substantial impacts on development cycles for connected vehicles and may delay innovation.

Unilateral national approaches must be avoided. Only uniform EU-wide rules can safeguard the integrity of the Single Market. Adequate implementation periods and a strict limitation of new obligations to new vehicle types are essential to ensure regulatory stability and planning certainty.

6. Focusing on Core Activities and Excluding Ancillary Activities

In practice, large industrial groups may fall under multiple NIS 2 sectors due to ancillary or purely internal activities that are not system-relevant from a cybersecurity perspective, such as internal charging infrastructure. To ensure legal certainty and proportionality, the application of CSA 2 should be strictly limited to core business activities. Ancillary or supportive activities that are not system-relevant should not trigger regulatory obligations. This clarification should be explicitly included in both CSA 2 and NIS 2.

A clear focus on core activities prevents an unnecessary expansion of scope, reduces administrative burden, and supports the EU's simplification agenda, including the Omnibus and Digital Fitness Check initiatives, while maintaining the protection of essential services.

Some Member States have already begun to reflect this approach in their national transposition of NIS 2. However, without a clear EU-level legal basis, there is a risk of divergent interpretations. Anchoring this principle at EU level is therefore essential to ensure harmonized application and a level playing field.

Conclusion

The BMW Group supports strengthening ICT supply chain resilience but considers CSA 2 unsuitable as an instrument for regulating vehicle cybersecurity. Cybersecurity risks in vehicles are already comprehensively addressed through UN R155 and should be reinforced through improved enforcement and harmonized type-approval test cases.

Non-technical concerns, where relevant, should be carefully assessed and addressed separately through dedicated, sector-specific product regulation subject to full legislative scrutiny. Maintaining this distinction is essential to ensure legal certainty, avoid regulatory duplication, and preserve Europe's competitiveness while achieving robust cybersecurity outcomes.