Submitted by the expert from IMMA

Informal document **GRVA-17-06**
17th GRVA, 25-29 September 2023
Provisional agenda item 5(a)

Proposal for a new supplement to UN Regulation No. 155

This informal document is aimed at including Category L in the scope of UN Regulation No. 155.

I. Proposal

Paragraphs 1.1. and 1.2., amend to read:

"1.1. This Regulation applies to vehicles, with regard to cyber security, of the Categories M and N.

This Regulation also applies to vehicles of Category O **and L** if fitted with at least one electronic control unit.

~~1.2. This Regulation also applies to vehicles of the Categories L6 and L7 if equipped with automated driving functionalities from level 3 onwards, as defined in the reference document with definitions of Automated Driving under WP.29 and the General Principles for developing a UN Regulation on automated vehicles (ECE/TRANS/WP.29/1140).~~"

Paragraphs 1.3. and 1.4., renumber as paragraphs 1.2. and 1.3., respectively.

Paragraph 7.3.1., amend to read:

"7.3.1. The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved. However, for type approvals **of vehicles of categories M, N and O** first issued before 1 July 2024, **for type approvals of vehicles of categories L6 and L7 which are equipped with automated driving functionalities from level 3 onwards, as defined in the reference document ECE/TRANS/WP.29/1140, first issued before 1 July 2024, and for type approvals of other vehicles of category L first issued before 1 July 2029,** and for each extension thereof, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned."

Paragraph 7.3.4., amend to read:

"7.3.4. The vehicle manufacturer shall protect the vehicle type against risks identified in the vehicle manufacturer's risk assessment. Proportionate mitigations shall be implemented to protect the vehicle type. The mitigations implemented shall include all mitigations referred to in Annex 5, Part B and C which are relevant for the risks identified. However, if a mitigation referred to in Annex 5, Part B or C, is not relevant or not sufficient for the risk identified, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented. In particular, for type approvals **of vehicles of categories M, N and O** first issued before 1 July 2024, **for type approvals of vehicles of categories L6 and L7 which are equipped with automated driving functionalities from level 3 onwards, as defined in the reference document ECE/TRANS/WP.29/1140, first issued before 1 July 2024, and for type approvals of other vehicles of category L first issued before 1 July 2029,** and for each extension thereof, the vehicle manufacturer shall ensure that another appropriate mitigation is implemented if a mitigation measure referred to in Annex 5, Part B or C is technically not feasible. The respective assessment of the technical feasibility shall be provided by the manufacturer to the approval authority."

II. Justification

1. After WP.29 adoption of UN Regulation No. 155 on Cybersecurity for four-wheeled vehicles (categories M, N and O, as well as L6 and L7 with automated driving functionalities from level 3 onwards) in June 2020 (ECE/TRANS/WP.29/2020/79), the discussion to extend the scope of the Regulation with L-category was postponed in GRVA. L1-L5 category vehicles are considered to currently have limited risk for cybersecurity abuse.

2. Meanwhile, in the European Union, the recently proposed EU Cyber Resilience Act (CRA) will introduce a set of horizontal requirements aimed at strengthening cyber resilience for products across a large number of sectors. While the CRA is a significant legislative initiative, its generic nature might not fully address the specific needs of the automotive industry, in particular for L-category vehicles. UN Regulation No. 155 is already available, proven for the automotive industry, and fully compatible with the EU CRA requirements, making it a more suitable and focused solution for these vehicles. Fundamentally, this would ensure that the complex cybersecurity requirements are met through a sector-specific regulation. This targeted approach mitigates potential mismatches and gaps that could arise from a horizontal application of generic standards.

3. UN Regulation No. 155 already covers all the CRA requirements for motorcycles, considering the complete exemption granted for cars. This demonstrates that the regulation is not only in line with existing legal frameworks but also anticipates the future trajectory of cyber resilience legislation within the EU.

4. Similar to what was granted to categories M and N in the original version of the regulation (paragraphs 7.3.1. and 7.3.4.), an adequate lead time is also necessary for L-category vehicles, to allow manufacturers to demonstrate adequate cybersecurity measures for the approval of vehicle types whose development phase started prior to the implementation of the Cyber Security Management System.