Submitted by the experts from France and the United Kingdom of Great Britain and Northern Ireland

Informal document **GRVA-17-13**
17th GRVA, 25-29 September 2023
Provisional agenda item 5(a)

Proposal for a new supplement to UN Regulation No. 155

The text below was prepared by the experts from France and the United Kingdom of Great Britain and Northern Ireland. The modifications to the existing text of the Regulation are marked in **bold** for new or ~~strikethrough~~ for deleted characters.

I. Proposal

Paragraph 1.1., amend to read:

"1.1. This Regulation applies to vehicles, with regard to cyber security, of ~~the~~ Categories **L,** M ~~and,~~ N**, O, R, S and T, if fitted with at least one electronic control unit.**

~~This Regulation also applies to vehicles of Category O if fitted with at least one electronic control unit~~."

Paragraph 1.2., shall be deleted:

"~~1.2. This Regulation also applies to vehicles of the Categories L_6 and L_7 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. (former) and 1.4., renumber as paragraphs 1.2. and 1.3.

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**, and for type approvals of vehicles of Categories L, R, S and T first issued before 1 July 2027**, 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**, and for type approvals of vehicles of Categories L, R, S and T first issued before 1 July 2027**, 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. At the 16th session of GRVA in May 2023, the subsidiary Working Party accepted the Chair's proposal to finalise the discussion of the inclusion of all categories of vehicles in UN Regulation No. 155 at its 17th session in September.

2. The purpose of UN Regulation No. 155 is to offer an international framework for the homologation of road vehicles with regard to cyber security. Therefore, GRVA should strive to offer the broadest scope possible to its Contracting Parties, and to allow manufacturers of vehicles of any relevant category to apply for a type approval.

3. During the previous sessions of GRVA and of its informal working group on cyber security and software updates, no technical argument was put forward to justify the exclusion of vehicles of Categories L, R, S and T from the scope of the Regulation. Not including these categories thus forces Contracting Parties and regional organisations to use national or regional laws on cyber security for these categories of vehicles. This could lead to unique requirements and a level of divergence that could be onerous on the industry.

4. The scope of UN Regulation No. 156 already includes all categories of vehicles: this current discrepancy between the two Regulations is an implicit statement that some vehicles, while able to receive over-the-air software updates, should not be type approved with regard to cyber security. Aligning the scope of UN Regulation No. 155 with that of UN Regulation No. 156 is a logical step towards a comprehensive regulatory environment for connected vehicles.

5. Similarly 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 necessary for manufacturers of vehicles of the categories introduced in this proposal to demonstrate adequate cybersecurity measures for the approval of vehicle types whose development phase started prior to the implementation of the manufacturer's Cyber Security Management System. Category L vehicles that were already in scope of the Regulation have been included in this lead time to simplify the drafting and remove reference to SAE levels of automation. As the provisions still require demonstration that cyber security was adequately addressed and any alternative mitigations are appropriate, there should be no issues in allowing additional time in this case.