Submitted by the experts from OICA and CLEPA

Informal document **GRVA-10-12**
10th GRVA, 25-28 May 2021,
Agenda item 5 (a)

Proposal for amendments to UN Regulation No. 155 (Cyber Security and Cyber Security Management System)

The additions and deletions are shown in **bold** text to facilitate identification of these proposed changes within the existing Regulation.

I. Proposal

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 ~~**prior to**~~ **first issued before** 1 July 2024 **and for extensions 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 ~~**prior to**~~ **first issued before** 1 July 2024 **and for extensions 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. Currently, paragraphs 7.3.1. and 7.3.4. define specific requirements for type approvals "prior to 1 July 2024". The question of extensions of those type approvals has been discussed within the UN Task Force on Cyber Security and OTA issues at its 21st session. The Task Force considers that the current wording is ambiguous because those requirements are not part of any transitional provision.

2. From a technical point of view, it will be necessary to obtain extensions of those type approvals after 1 July 2024.

3. As a consequence, OICA and CLEPA believe that the wording proposed above, which is in line with the General Guidelines ECE/TRANS/WP.29/1044/Rev.2, would clarify the correct application of paragraphs 7.3.1. and 7.3.4.