Submitted by the experts from
CITA, EGEA, ETRMA, FIA and FIGIEFA

Informal document **GRVA-04-04**
4th GRVA, 24-27 September 2019
Agenda item 5

Proposal for amendments to the Recommendation on Cyber Security (ECE/TRANS/WP.29/GRVA/2019/2 as revised)

(Proposal for amendments to the draft GRVA-03-02e_TF CS-OTA_Overview of the recommendations on cyber security)

The text reproduced below aims at proposing improvements to the text of the main text and the draft new UN Regulation on uniform provisions concerning the approval of cyber security. The modifications to the existing text of the proposed Recommendation on Cybersecurity (ECE/TRANS/WP.29/GRVA/2019/2) are marked in **bold** for new text and strikethrough for deleted text.

I. Proposed amendments

Proposal for a Recommendation

II. Definitions

Paragraph 2.1., **amend** to read:

"2.1. "*Aftermarket*" means the secondary market of the automotive industry, like repairers who provide repair and maintenance services for vehicles, independent operators who are directly or indirectly involved in the repair and maintenance of vehicles, and include repairers, manufacturers or distributors of diagnostic and repair equipment, tools or spare parts or **lubricants**, as well as publishers of technical information, **remanufacturers**, automobile clubs, roadside assistance operators, fleet management solution providers, operators offering inspection and testing services, operators offering training for installers, manufacturers and repairers of equipment **for electric and** alternative-fuel vehicle and independent service providers."

III. Cyber security principles

*Insert **new** paragraph 3.3.11.,* to read:

"3.3.11. When designing a Cyber Security Management System, vehicle manufacturers should ensure the highest level of protection against security threats and attacks while at the same time safeguarding access to the vehicle, its data, functions and resources for authorised parties."

VII. Conclusion and recommendation for further proceedings

*Insert **new** paragraph 7.6.6.,* to read:

"7.6.6. This Regulation should be supplemented by a technical authorisation concept, as part of type-approval, in order to allow national or regional legislations to regulate the authorised remote access to in vehicle data, functions and resources in a technology neutral manner."

Annex A, draft new UN Regulation on uniform provisions concerning the approval of cyber security

*Insert **new** paragraph 1.2.,* to read:

"1.2. This Regulation is without prejudice to other UN Regulations, regional or national legislations governing the access by authorised parties to the vehicle, its data, functions and resources, and conditions of such access."

II. Justification

Proposal for a Recommendation

II. Definitions

*Paragraph 2.1., **amended***

The submitted proposal to change the definition of "aftermarket" was accepted by the Task Force and adopted in the Cyber Security proposal (see TFCS 15-23 and TFCS 15-35 ECE/TRANS/WP.29/GRVA/2019/2e).

In order to ensure that all aftermarket participants are covered by this definition, the inclusion of lubricants, remanufacturers and manufacturers and repairers of equipment for electric vehicles is also required.

III. Cyber security principles

*Paragraph 3.3.11., **new***

The inclusion of this cyber security principle results from the three overarching cyber security principles - availability, confidentiality and integrity -.

It intends to clarify the balance between a high level of protection of the vehicle against security threats whilst at the same time guaranteeing authorised access to the vehicle, its data, functions and resources for authorised parties.

VII. Conclusion and recommendation for further proceedings

*Paragraph 7.6.6., **new***

An authorisation concept is needed to keep the technical solution for the remote access to the vehicle, its data, functions and resources, technology neutral. It defines basic specifications for the remote communication with the vehicle to be implemented at the moment of design and construction of the vehicle. Whilst doing so, it is without prejudice from any UNECE legislation possible for national and regional legislators to determine who is authorised, at which level, to access vehicle-data, functions and resources; to which appropriate level authorised parties can access in-vehicle-data, functions and resources; how in greater details the implementation is done.

Annex A, draft new UN Regulation on uniform provisions concerning the approval of cyber security

*Paragraph 1.2., **new***

In the current proposal for a UN Regulation on Cybersecurity, vehicle manufacturers submit their own proprietary cybersecurity management strategies for a type-approval (audit-process instead of testing to standard or target values), which may include proprietary access control techniques, practices and designs for remote communication channels with the vehicle. Due to this procedure, there could be a conflict with wired or wireless network communication to the vehicle for authorised parties. This is why this Regulation should be without prejudice to other UN Regulations, regional or national legislations governing the access by authorised parties to the vehicle, its data, functions and resources, and conditions of such access.