Submitted by the IWG on CS/OTA

Informal document **GRVA-16-15**
16th GRVA, 22 - 26 May 2023
Provisional agenda item 5(a)

Based on TFCS-25-03

Proposal for an update of Recommendations for Automotive Cyber Security and Software Updates

To align the contents of regulations and documents for different agreements the IWG on CS/OTA reflected the amendments to UN R155 and R156 in the recommendation document (ECE/TRANS/WP.29/2022/60) ready for the 1998 Agreement. The amendments are based on GRVA-15-05 and GRVA-15-06. The changes proposed to the current text of the document are indicated in ~~strikethrough~~ for deleted and **bold** for new text.

I. Proposal

Part I - Introduction, amend to read:

"1. Individuals and organizations involved in the design, manufacturing, or assembly of a motor vehicle have a role to play with respect to vehicle cybersecurity.

2. This document is provided as guidance for Contracting Parties to the 1998 Agreement when formulating regulation or legislation on cyber security for automotive vehicles and/or regulation or legislation on software updates and the processes for updating a vehicle's software. The aim of the guidance is to enable a harmonized approach to the adoption of such regulation or legislation. As such, the technical requirements herein are aligned to the furthest extent possible with the requirements from UN Regulations Nos. 155 and 156 that pertain to the 1958 Agreement's Contracting Parties regarding cyber security and software updates, respectively. Parenthetical references have been added pointing to corresponding section(s) in the corresponding regulation.

The document lists technical requirements for the vehicle and technical requirements for management systems. The technical requirements for the management systems list requirements that are external to the vehicle but need to be in place to effectively manage the cyber security of a vehicle over its lifetime and to ensure software updates will be sufficiently appraised and protected before they are sent to a vehicle.

It is recommended that, as a minimum, the technical requirements relating to the vehicle are adopted *en masse* when formulating regulation or legislation. Where possible the requirements for the management system should also be adopted. Where it is not possible to adopt the management system requirements within regulation or legislation, it is suggested they are adopted as national guidance for manufacturers of automobiles to follow.

The document does not define acceptance criteria nor test criteria for these requirements.

The vehicle phases mentioned in this document are not defined herein and are left to regulation or legislation. Industry guidance on all vehicle phases can be found in international standards e.g. ISO/SAE 21434, **ISO PAS 5112** and ISO 24089. However, it should be noted that the "post-production phase" encompasses all aspects after a vehicle has been produced, where the two most important aspects to be considered are end of life of a vehicle (also known as "decommissioning") and end of cybersecurity support of a vehicle. Due to the fact that the 1998 Agreement is intended to be applicable to diverse regulatory and enforcement systems, the Informal Working Group on cyber security and over the air updates has not defined a minimum length of time for vehicle cyber security support in this document.

This document provides a method by which information about the software and hardware configurations, particularly those relating to systems of a vehicle specified in regulation or

legislation, can be managed and understood with respect to the vehicle's certification. Through the use of a dedicated identifier (e.g. R_xSWIN as defined in UN Regulation No. 156), representing the configuration of a given system's software and hardware, it can be understood when a software update affects the certification of that system as the dedicated identifier should change when this happens. For this method to work, a vehicle manufacturer needs to be able to provide information about the hardware and software represented by a given dedicated identifier. For a given vehicle it must be possible to determine what software is present on the vehicle in order to verify that the software conforms to that represented by the dedicated identifier."

Annex 1, Part A, Table A1, amend to read:

4.3.2 Threats to vehicles regarding their communication channels	4	Spoofing of messages or data received by the vehicle	4.1	Spoofing of messages by impersonation (e.g. ~~802.11p~~ V2X ~~during platooning~~ **cooperative awareness or manoeuvre coordination messages**, GNSS messages, etc.)

Annex 1, Part B, Table B1, amend to read:

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	*Mitigation*
4.1	Spoofing of messages (e.g. ~~802.11p~~ V2X ~~during platooning~~ **cooperative awareness or manoeuvre coordination messages**, GNSS messages, etc.) by impersonation	M10	The vehicle shall verify the authenticity and integrity of messages it receives

II. Justification

1. To reference all relevant and current standards it is proposed to include ISO PAS 5112 in the introduction.

2. The Informal Working Group previously agreed that using "802.11p" to refer to Vehicle to Everything (V2X) communications is out of date: 802.11p is properly referred to as 802.11-OCB and other direct communication methods are in use. The experts consider "V2X" a more up-to-date and appropriate term than "802.11p". Furthermore, the experts note that platooning is a niche V2X operation and not widely used and suggest the use of more mainstream examples such as cooperative awareness or manoeuvre coordination and are therefore proposing to change the relevant text as already agreed by GRVA for UN Regulation No. 155.