Submitted by the IWG on Cyber Security and OTA issues

Informal document **GRVA-15-05**
15th GRVA, 23 – 27 January 2023
Provisional agenda item 5(a)

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

Proposed amendments are indicated in bold for new characters, and strikethrough for deleted characters.

I. Proposal

Annex 5, Part A, second major row of 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.)
			4.2	Sybil attack (in order to spoof other vehicles as if there are many vehicles on the road)

Annex 5, Part B, first row of 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. The Informal Working Group agreed that using “802.11p” to refer to V2X communications is out of date: 802.11p is properly referred to as 802.11-OCB and other direct communication methods are in use.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.

2. This proposal therefore includes amendments that are suggested to be more appropriate and, in practical terms, would lead to less interpretation requests from implementers as the new examples would fit with mainstream implementers’ expectations.

_____