Submitted by the expert from FIGIEFA

Informal document **GRVA-03-16**
Third GRVA, 3-4 June 2019
Agenda item 4(a)

United Nations Economic Commission for Europe -
Inland Transport Committee -
World Forum for Harmonization of Vehicle Regulations

Draft UN Regulation on uniform provisions concerning the approval of cyber security (GRVA-02-37 dated 28.1. – 1.2.2019)

FIGIEFA comments

Dear Madam, dear Sir,

FIGIEFA brings together 20 national associations representing independent automotive aftermarket distributors across Europe. FIGIEFA is part of the wider independent multi-brand automotive aftermarket of vehicle parts, diagnostics, servicing, maintenance, roadworthiness testing and repairs, which provides 4,3 million jobs in the EU through over 500.000 predominantly SME companies. All these operators ensure that the 284 million vehicles on European roads fulfil the regulatory standards in terms of safe and sustainable mobility, at an affordable cost for consumers, through innovative and competitive services and solutions.

The independent operators in the automotive aftermarket have a key role to play in the deployment of connected and automated mobility, by contributing to the continuous safety and security of the connected and automated vehicles once on the road, through their lifetime. Their position, enabling them to independently detect and fix many issues affecting the quality and safety of mobility, should be taken into account.

FIGIEFA fully supports cybersecurity measures as being absolutely necessary to build confidence in and support the uptake of connected and automated mobility.

The way that the GRVA Cybersecurity Recommendations and the ensuing type-approval regime are currently conceived is that they leave the design of the cybersecurity schemes to the entire discretion of vehicle manufacturers, who are becoming vehicle related service providers. This deviates from the classical type-approval approach where functional requirements or limit values are set by the legislator, and each type-approval applicant (e.g. vehicle manufacturers, parts producers etc.) must demonstrate that their products can achieve them. If such a change of paradigm is adopted, which consists in auditing vehicle manufacturers' proprietary cybersecurity schemes, **then Contracting Parties should make sure that there are no negative consequences on other market operators**.

This is however now the problem: If vehicle manufacturers are becoming vehicle related service providers and are also free to design their cybersecurity schemes without any scrutiny of the legislator, this has the potential to completely close the vehicle for competing independent service providers in the name of "cybersecurity". Today, all vehicle related service providers communicate with the vehicle, its data and functions in order to offer competitive services and products.

FIGIEFA
International Federation of Automotive Aftermarket Distributors
Boulevard de la Woluwe 42, Box 5
BE-1200 Brussels

Tel.: +32 2 761 95 10
Fax: +32 2 762 12 55
E-mail: figiefa@figiefa.eu
Web: www.figiefa.eu

EC Transparency Register ID:
69678928900-56

Consequently, **Contracting Parties must ensure that cases of "legitimate use" of vehicle related service providers will be included into the GRVA Recommendation and its type-approval regime to** make sure that these crucial stakeholders are not excluded from the connected and automated vehicles. Having legitimate service providers excluded from future vehicles would put these vehicles at risk, be detrimental to innovation and competition and affect negatively the benefits of their potential users.

Therefore, FIGIEFA, after having consulted cybersecurity experts through the entire automotive sector, in the manufacturing as well as in the aftermarket, recommends to adopt the following amendments:

Amendment 1: In the chapter "Definitions" (2), to add the following definitions:

2.4.1. **'Authorised parties'** are authorized by national approval authorities for general access rights, e.g. confirming that the company is a legitimate vehicle related service provider.

2.4.2. **'Vehicle related services providers'** means undertakings which are directly or indirectly involved in the repair and maintenance of motor vehicles, in particular repairers, manufacturers or distributors of repair equipment, tools or replacement parts, publishers of technical information, automobile clubs, roadside assistance operators, operators offering inspection and testing services, operators offering training, manufacturers and repairers of equipment for alternative fuel vehicles and mobility service providers."

2.4.3. **'Vehicle diagnostics, repair and maintenance operations'** mean wired or wireless network communication with the vehicle and the accessibility to its data and functions for diagnosis, servicing, maintenance, inspection, road worthiness testing, repair, software updates, re-programming or re-initialising of the vehicle, including the fitting and coding of systems, components, parts or equipment on vehicles, during the lifetime of the vehicle."

Amendment 2: in the chapter "Approval" (5), to introduce a new article:

5.5. To ensure neutrality and compliance with the requirements for the authorisation of vehicle related service providers, an approval authority body that is independent of the vehicle manufacturer, will be responsible for authentication and certification of authorized parties.

Amendment 3: In the chapter "Specifications" (7), to introduce a new article:

7.2.3. Vehicle manufacturers, when designing and implementing their Cyber Security Management System shall put in place functions and processes that allow all authorised parties access to data, functions and resources inside the vehicle required to support competing vehicle related services in comparison to those provided by the vehicle manufacturer in a safe and secure way during the lifetime of the vehicle.

The operations on the vehicle depend on the vehicle state; which are stationary, driving or parking.

Cybersecurity management system must enable the following type of functions calls:

- Function calls that Read Data from the vehicle
- Function calls that Write Data to the vehicle
- Function calls that request ECUs to activate routines
- Function calls that implement new routines from a third party
- Function calls that trigger software updates
- Function that enables the installation of replacement parts

The amount and degree and depth of accessible functions depends on the level of certification for authorized parties as well as the current state of the vehicle.

Amendment 4: Through the entire proposal, to replace “life cycle” with “lifetime”

* * *

FIGIEFA kindly invites you to include these amendments into the and would be pleased to offer additional details and discuss any questions you may have.