Submitted by Germany

"Clean" version of informal document GRVA-03-13 (tracked changes)

Informal document **GRVA-03-13**
3rd GRVA, 3-4 June 2019
Provisional agenda item 3

Proposal for an Informal Working Group on Cyber Security and (Over-the-Air) Software-Updates

A) Terms of Reference

1. The Informal Working Group on Cyber Security and (Over-the-Air) Software-Updates is established as a subgroup of GRVA.

2. Members of the group shall have the relevant technical or regulatory expertise to contribute to the delivery of its task.

3. The Informal Working Group shall:

- Address Cyber Security and (Over-the-Air) Software-Update issues, relevant for the automotive industry (Conventional and Automated / Autonomous vehicles). This shall include the following activities:
  - Agree common terms and definitions for "Cyber Security" and "Software-Updates"
  - Develop and agree a common understanding of the terms "lifetime" and "lifecycle" of a vehicle with respect to unresolved issues on providing safety and security of a vehicle taking into account the longevity of vehicles, identifying and agreeing on principles and solutions on handling older vehicles in traffic.
  - Identify and consider key risks and threats
  - Agree and define principles/objectives to be obtained to address the key risks and threats and measures to assure vehicle safety in case of cyber-attacks
  - Consider the implications related to type approval for software updates, including technical and administrative provisions
  - Consider the implications related to post-registration regulatory compliance and conformity to the type approved
  - Take into account the document titled "Guideline on cybersecurity and data protection", developed by the former IWG on ITS/AD, to avoid duplications/deficiencies
  - Consider existing and developing standards, practice(s), directives and regulations concerning cyber security and their applicability to the automotive industry
  - Identify competencies that authorities/technical services need to have in order to be able to review and objectively assess the proof and measures taken by the respective entities that seek compliance or type approval (qualitative requirements).
  - Define the process in case Cyber Security incidents occur (obligations for manufacturers)
- Address Data protection issues. This shall include the following activities:
  - Consider the implications of data protection legislation and privacy legislation
  - Agree common terms and definitions, including defining "Data protection" and "Data privacy" in the context of the automotive industry
  - Consider what data might be stored in a vehicle or transmitted from it
  - Consider and identify key risks and threats for the protection of data including personal data, stored data and transmitted data
  - Develop recommendations or guidance to address the key risks and threats identified

- Consider existing and developing standards, practice(s), directives and regulations concerning data protection and data privacy and their applicability to the automotive industry
- Consider and develop provisions with regard to the property of data (manufacturers, suppliers, maintenance providers, vehicle owners and Contracting Parties) stored or transmitted from the vehicle.
- Consider and develop provisions for the use and right of use of data stored or transmitted from the vehicle.

- Develop relevant recommendations, regulations, provisions or documentation for both the 1998 Agreement and the 1958 Agreement; The decision whether to adopt the work as regulation, guidelines or best practices will be taken by WP.29.
- Submit its outcome to GRVA.

4. The group shall conduct a test phase on the relevant recommendations, provisions or documentation in cooperation with the respective administrations and technical services and OEMS and present the results to the November 2019 session of GRVA.

5. Draft UN-Regulations for Cybersecurity and Software-Updates to supplement the new UN Regulation for the automated lane keeping function on highways are expected until [March 2020].

6. Review of draft set of technical requirements for the 1998 Agreement and present the results until March 2021.

B) Rules of Procedure

1. The Informal Working Group is a sub group of the IWG on ITS/AD GRVA, and is open to all participants of WP.29 and its subsidiary bodies.

2. The Informal Working Group will be chaired by [the United Kingdom Department for Transport and Japan]. The [Technical] Secretariat will be provided by [OICA].

3. The working language of the Informal Working Group will be English.

4. All documents and/or proposals shall be submitted to the [Technical] Secretary in a suitable electronic format at least one week before the meeting. The group may refuse to discuss any item or proposal which has not been circulated one week in advance.

5. An agenda and related documents will be circulated to all Informal Working Group members in advance of all scheduled meetings.

6. All Informal Working Group documents will be made available on the dedicated UNECE website by the Secretary (https://www2.unece.org/wiki/pages/viewpage.action?pageId=40829521).

7. The Informal Working Group decisions will be reached by consensus. When consensus cannot be reached, the Informal Working Group Chairmen shall present the different points of view to GRVA and seek guidance as appropriate.

8. The IWG progress will be routinely reported at sessions of GRVA by the Chair(s) or representative(s).