

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

### A) Terms of Reference

1. The ~~Task Force~~ **Informal Working Group on Cyber Security and (Over-the-Air) Software-Updates** is established as a subgroup of GRVA ~~the Informal Working Group on Intelligent Transport Systems / Automated Driving (IWG on ITS/AD) of WP.29.~~

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

3. The ~~Task Force~~ **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”

~~This shall include the following definitions:~~

- ~~▪ “Cyber Security” in the context of the automotive industry shall be defined as:~~

~~“The use of technologies, processes and practices designed to protect networks, devices, services and programs—and the information and data on them—from theft, damage, attack or unauthorized access”~~

- ~~▪ “The automotive industry ” shall be considered to include:~~

~~“Manufacturers, suppliers, maintenance providers and providers of systems and services that interact with the vehicles (e.g. back-end systems and 3<sup>rd</sup> party systems)”~~

~~This definition may be further refined were needed.~~

- 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 ~~and any associated timelines for achieving them~~
- 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
- ~~Define detailed guidance or measures for how to meet the objectives/principles. This may include processes and technical approaches~~
- ~~Consider what assessments or evidence may be required to demonstrate compliance or type approval with any requirements identified~~
- **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)**
- ~~Outputs to be presented to the IWG on ITS/AD of WP.29 for their consideration. This shall include recommendations on the outputs use as a regulation or a resolution and, if applicable timelines, for delivery~~
- 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.**
  - ~~Outputs to be presented to the IWG on ITS/AD of WP.29 for their consideration. This shall include recommendations on the outputs use as a regulation or a resolution and, if applicable timelines, for delivery~~
- ~~Address software updates. This shall include the following activities:~~

- ~~○ Agree common terms and definitions, including defining “Over The Air updates” in the context of the automotive industry~~
  - ~~○ Develop recommendations on security aspects of software updates, including over the air updates~~
  - ~~○ Consider and identify key risks and threats concerned with software updates~~
  - ~~○ Consider existing and developing standards, practice, directives and regulations concerning software and its updates~~
  - ~~○ 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~~
  - ~~○ Outputs to be presented to the IWG on ITS/AD of WP.29 for their consideration. This shall include recommendations on the outputs use as a regulation or a resolution and, if applicable timelines, for delivery~~
- 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 ~~the IWG on ITS/AD~~ 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. ~~4.~~ The ~~Task Force 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. ~~5.~~ The ~~Task Force Informal Working Group~~ will be chaired by [the United Kingdom Department for Transport and Japan]. The [Technical] Secretariat will be provided by [OICA].
3. ~~6.~~ The working language of the ~~Task Force Informal Working Group~~ will be English.
4. ~~7.~~ 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. ~~8.~~ An agenda and related documents will be circulated to all ~~Task Force Informal Working Group~~ members in advance of all scheduled meetings.

6. ~~9.~~ All ~~Task Force 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. ~~10.~~ The ~~Task Force Informal Working Group~~ decisions will be reached by consensus. When consensus cannot be reached, the ~~Task Force Informal Working Group~~ Chairmen shall present the different points of view to ~~the IWG on ITS/AD~~ GRVA and seek guidance as appropriate.

8. ~~11.~~ The IWG progress will be routinely reported at sessions of ~~the IWG on ITS/AD~~ GRVA by the Chair(s) or representative(s).

### ~~C.~~ **Timeline**

~~12. — The Task Force is expected to outline its plan (including any steps, deliverables and expected timelines) for presentation to the March 2017 meeting of IWG on ITS/AD.~~

~~13. — The Task Force is expected to deliver documentation to the IWG on ITS/AD, detailing its recommendations or provisions on cyber security, Over The Air updates and data protection within a year from its first meeting. This shall be in time for the IWG on ITS/AD on the (date to be confirmed — probably Jan 2018).~~

~~14. — The Task Force shall make a recommendation on whether it should continue after its first full year and present this to the IWG on ITS/AD on the (date to be confirmed — probably Jan 2018).~~