Questions and Answers/Comments derived from the Workshop on the implementation of UN Regulation No. 155 (Updated, 24 September 2022)

I. Context

1. UN Regulation No. 155 was established to support vehicle cyber security. This regulation is rather unique in the framework of the 1958 Agreement and also in the field of cyber security. The regulation makes the vehicle manufacturer responsible for ensuring cybersecurity throughout the supply chain and the lifecycle of the vehicle. It requires addressing two types of requirements, those related to the cyber security management and those related to the type approval.

II. Specificities

2. The regulation does not provide a high level of details on the way to evidence the compliance with the requirements. The regulator chose to provide guidance in a guidance document instead of inserting them in the regulation. This choice has an importance in the context of the mutual recognition obligation of type approvals according to the provisions of the 1958 Agreement. The regulator therefore inserted in the regulation the obligation for the Approval Authorities to exchange information, via the Database for the Exchange of Type Approval (DETA) on the assessment method used in the context of this regulation.

III. Workshop on the implementation of UN Regulation No. 155

3. The Working Party on Automated/Autonomous and Connected Vehicles (GRVA) agreed to organize a workshop on the implementation of UN Regulation No. 155 and the first meeting was organized in 2021, see ECE/TRANS/WP.29/GRVA/10, para. 43. GRVA approved further workshops. To date the expert from NTSEL (Japan) and the secretariat organized 11 workshops.

4. The purpose of these workshops was to gather the Approval Authorities and technical services that are applying the Regulation. Approval Authorities of CPs exchanged views on the implementation for fulfilment of the requirements of the Regulation.

5. This document captures and summaries discussions in the workshops in the form of a Q&A. Answers or comments which have been agreed by the workshop so far are summarised as the table below.

IV. Questions gathered and discussed

Categories	Questions	Answers (Comments) – under development
CSMS scope/assessment	How much detail manufacturers' documents should be assessed?	The assessment should entail enough detail to be confident to state that the CSMS is compliant with all relevant requirements of R155 and implemented. Harmonization of auditing/assessing manufacturer could be part of future work.
	How the steps to Audit is configurated?	Other standards on management systems, such as the ISO/IEC 27000-series or ISO/PAS 5112 etc. could be used as reference.

	How to assess Stage-2-OEM?	Depending on the impact of the changes made by the Stage-2-OEM. The Stage-2-OEM must explain the changes made and why they are not CSMS relevant. Three categories have been defined: Cat. A - UN-R155 CSMS for the Stage-2-OEM not required: Changes which are not cyber relevant and do not relate to the E/E Architecture of the Stage-1-OEM (e.g. by adding pure hardware or devices which are not connected to the E/E Architecture of the Stage-1-OEM). Cat B - UN-R155 CSMS might (not) be required: Changes are cyber relevant or related to the E/E Architecture but only with "read-access". Stage-2-OEM has to explain based on a risk assessment why the changes are not relevant. Cat. C - UN-R155 CSMS required: Changes are cyber relevant or related to the E/E Architecture with "read/write" access to the E/E Architecture. For cyber relevant modifications, elements given to the TAA/TS should include information regarding interface between manufactures at each stage. Note: Type approval for multi stage vehicles regarding R155 needs to be further explored.
	How to assess outsourcing/suppliers?	The manufacturer must demonstrate that the cyber security interface agreement with its suppliers is in place, and how all the relevant items, such as testing, are put under control (documentation / audits).
	One or more certificates for one applicant (legal person)?	Manufacturer can have one or more CSMSs. The scope of each CSMS and its CoC has to be defined.
	For how long the OEM shall maintain cyber-security?	The manufacturer must manage the cybersecurity risk until the vehicle is end of life. The strategy must define the conditions for end of life and how cybersecurity risks will be mitigated in the event that software update is no longer provided.
	Is it required to have agreements/arrangements for cybersecurity with service providers across all geographies implementing R155?	Agreements with service providers do not need to extend to all R155 geographies as long as the same level of security is guaranteed (e.g. by disabling the relevant interface)
	What should be the depth of review of Information	The OEM must convince the TS (in audit and test). This might be also by explaining the

	security items for CSMS Annex 5 threats/mitigations especially, threats 1.1, 1.2, 1.3, 2.1, 3.1, 3.2, 3.3, 3.4, 3.5, 15.1, 15.2, 16.2, 19.3, 20.2. ?	own strategy, in giving evidence of competence of own staffs who are responsible for theses (and other) items, of doublechecking (supplier by the OEM or OEM-developing department or other neutral department etc.).
	How to handle different production sides within the scope of CSMS?	All production sites/plants relevant for R155 should be within the scope of CSMS.
	What is minimum criteria on reasonable timeframe?	As a future work, the workshop agreed to develop consensus reasonable timeframe accumulating experiences.
Testing	What is the purpose of test by Technical Service?	(TBD)
	How many tests? Chosen on what basis?	(TBD)
	How will the sensitive information related vehicle type be treated?	(TBD)
	Destructible test methods allowed?	(TBD)
	How much effort (time) shall be spent (in particular on pen-testing)?	(TBD)
Homologation process	What communication between the TS and the TAA?	Breadth and depth of communication with the Technical Service shall be defined ad hoc and may not need to be constrained by precise guidelines. However, a type-approval authority wishing to give specific guidance on information exchange may do so within their Method & Criteria document.
	Certificates / Approval for suppliers	Certificates to suppliers is not in the scope of this regulation. It is the responsibility of each OEM to specify what methods, standards and associations are applicable to their suppliers.
	Acceptance of foreign Certificates (for CSMS/SUMS) for the type approval	Contracting Parties may, for example by bilateral or by reciprocal agreement, recognize another contracting party's Certificate of Compliance for some or all elements of the Cyber Security Management System. <Introduction of guidance in § K. of the interpretation document regarding § 6.1. of the Regulation> This amendment was proposed in the light of discussing specific scenarios, such as joint ventures, which involve several OEMs and authorities.
	Approval with withdrawn or expired certificate	The CSMS CoC must be valid at the time of signing the R155 communication file.
	Extensions for vehicles with approvals under transitional provisions of UN-R 155	See amendment of the interpretation document. ECE-TRANS-WP29-2022-061e

Risk Assessment	(How to handle non critical elements?)	(TBD)

V. Follow up

6. The participants of the workshop propose the following activities in coming meetings:

   i. To complete the table of Q&A(C)

   ii. To draft a proposal to amend the current official documents ([UN R155 and] its interpretation document) to address the identified issues regarding certification of CSMS and approval of types for UN R 155