Feedback on OICA's proposal for cyber security guideline (ITS/AD-08-05)

No.	Position	Original	OICA Proposal	Feedback on Proposal
1	(throughout the document)	(throughout the document)	OICA proposes to replace “shall” with “should” throughout the document since “shall” is too strict for a guideline. Considering the situation where ISO standard also treats the terms of "shall" as mandatory requirements (not only UN Regulation but also ISO standard), the usage of “shall” in the guideline should be avoided.	It is explained in the preamble in Part C that this “guideline is intended as interim guidance until the completion of ongoing research and collaboration activities and the development of more detailed globally harmonized requirements on cybersecurity and data protection.” From this it derives that there will be “shall” and should in future versions of the document. Which formulation is appropriate has to be decided for each single case.
2	Part A) I. Focus areas on automated and connected driving Paragraph 4	For cybersecurity and data protection required steps should be checked, e.g. system checks by external organisations or a certification of systems.	For cybersecurity and data protection required steps ~~shall~~should be checked, e.g. system checks by external organisations ~~or a certification of systems~~. For Justificaiton for delete “or a certification of systems” Checks by external organisations seems acceptable, however “certification of systems” seems too strict for the nature of a guideline.	1. see feedback No.1 2. Note that Part A) and B) are solely for explanation. The core of the document is Part C) with requirements. 3. The original wording should be kept. To clarify, this sentence addresses the use of systems or components of certified manufacturers without additional verification.

No.	Position	Original	OICA Proposal	Feedback on Proposal
3	Part B) Issues for discussion Item 1	1.The use of clear definitions should be provided for the outline of Work item 7	The ToR of the IWG ITS/AD mentions eSecurity (protection against unauthorized access from outside), however it does not mention the issues related to personal data. OICA believes that issues related to personal data and data privacy are out of the regulatory scope of WP.29.	Personal data and privacy are covered by the concept of eSecurity in the ToR. Moreover, Article 1 of the 1958 Agreement says that it is possible to make regulations for wheeled vehicles with characteristics which are relevant for road safety, and non-compliance with data protection may compromise road safety. This is the basis for the preparation of regulations.
4	2. Requirements/ Recommendations	Requirements / Recommendations	This document is laid down as guideline, therefore, OICA considers that the wording “requirements” is too strict and deviate from the original purpose of the document. Also, since content of the document is described abstractly as “requirements”, we are not able to verify whether it satisfies required conditions. OICA believes the proposed contents are intended as "guidelines". Hence, the usage of the term "requirements" in the guideline should be avoided.	Japan prefers: Requirements / [Recommendation] To be discussed

No.	Position	Original	OICA Proposal	Feedback on Proposal
5	2.1 General Item 2 and Item 3	·Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. ·The manufacturer, supplier [and service providers] shall respect the principles of data protection by design and data protection by default.	Remove two sentences OICA is of the opinion that issues related to personal data / privacy are different in the '58 Agreement countries and must be met/complied with regionally anyways. Regarding the regulatory scope of WP.29, OICA suggests that the guideline contains technical related items.	No agreement, see feedback No.3
6	2.1 General Item 5	·To prevent non-authorized access to vehicles, automotive manufacturers and component suppliers [and service providers] shall ensure the secure encryption of data and communications by the use of effective information and communication technologies.	·To prevent non-authorized access to vehicles, automotive manufacturers and component suppliers [and service providers] ~~shall~~should ensure the secure encryption of data and communications ~~by the use of effective information and communication technologies~~.	1. No change "Shall" see feedback No.1. 2. Reason for deleting the last part of the sentence is unclear.
7	2.1 General Item 6	·For cybersecurity and data protection required steps shall be verifiable independently by external organisations or a certification of systems.	·For cybersecurity ~~and data protection~~ required steps shall be verifiable independently by external organisations ~~or a certification of systems~~.	No change, see feedback No.3.

No.	Position	Original	OICA Proposal	Feedback on Proposal
8	2.3 Safety Item 1	Connected vehicles and vehicles with ADT shall be equipped with verifiable measures for cybersecurity taking into account the latest existing national and international standards.	·Connected vehicles and vehicles with ADT ~~shall~~should be equipped with verifiable measures for cybersecurity taking into account the ~~latest~~ existing national and international standards.	Wording "existing" is reasonable but no change "Shall"
9	2.4 Security Item 4	·The integrity of internal communications between controllers within connected vehicles should be protected by authentication.	The integrity of internal communications between controllers within connected vehicles should be protected e.g. by authentication. Justification for "appropriate measures" OICA is of the opinion that methods for protecting communications shall not be limited and that they should be prescribed in general terms. Hackers should not be given any hints. Furthermore, OICA understand that "authentication" means "message authentication" in this context, however even if that's the case, it should be considered as an example.	Insert "e.g." is reasonable