**Draft proposal to introduce a Regulation on Cyber Security**

 **Draft Regulation on Cyber Security**

|  |  |  |
| --- | --- | --- |
|  | United Nations | ECE/TRANS/WP.29/201x/xx |
| _unlogo | **Economic and Social Council**TFCS-16-31 – cyber security regulatory text – updated to Include suggested amendments up to TFCS 16-30 | Distr.: GeneralDD MM YYYYOriginal: English |

**Economic Commission for Europe**

Inland Transport Committee

**World Forum for Harmonization of Vehicle Regulations**

**xxx session**

Geneva, DD–DD MM YYYY

Item XXX of the provisional agenda

**Draft new UN Regulation on software updates**

 **A**mendment

 **Draft new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security**

 **Submitted by the expert from xxx**

The text reproduced below was prepared by the experts from xxx

 **I. Proposal**

 **A**mendment

 **Draft new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security**

Contents

 *Page*

 1. Scope 3

 2. Definitions 3

 3. Application for approval 3

 4. Markings 3

 5. Approval 4

 Amendment

 6. **Certificate of Compliance for** Cyber Security Management System (CSMS) ~~Certificate of compliance~~ 4

 7. Specifications 5

 8. Modification and extension of the vehicle type 7

 9. Conformity of production 7

 10. Penalties for non-conformity of production 7

 11. Names and addresses of technical services responsible for conducting approval tests and of

 Administrative departments 7

Annexes

 1. Information document 8

 2. Communication form 9

 3. Arrangement of approval mark 10

 Amendment

 4. Model of ~~CSMS~~ Certificate of Compliance **for CSMS** 11

 1. Scope

Amendment with IMMA proposal from GRVA (GRVA-040-25)

1.1. This Regulation applies to vehicles**, with regard to cyber security,** of the categories **~~[L ] [L6, L7]~~,** M, N, O [**and**, R, S and T].

**1.2. This regulation also applies to vehicles of the categories L6 and L7 if equipped with automated driving functionalities from SAE Level 3 onwards.\***

**\* As defined in the Reference document with definitions of Automated Driving under WP.29 and the General Principles for developing a UN Regulation on automated vehicles (****ECE/TRANS/WP.29/1140)**

Amendment agreed by GRVA.

1.3. **This Regulation is without prejudice to other UN Regulations, regional or national legislations governing the access by authorized parties to the vehicle, its data, functions and resources, and conditions of such access. It is also without prejudice to the application of national and regional legislation on privacy and the protection of natural persons with regard to the processing of their personal data.**

 2. Definitions

 For the purpose of this Regulation the following definitions shall apply:

Amendment with comment

2.1. "*Vehicle type*" means vehicles ~~of a particular category~~ which do not differ in at least the following essential respects:

 (a) ~~The manufacturer~~;

 (b) The manufacturer’s ~~type~~ designation **of the vehicle type**;

 ~~(c)~~ Essential aspects of ~~vehicle design~~ **the electric/electronic architecture and external interfaces** with respect to cyber security

Amendment with NL comment **with proposed amendment (FIGIEFA et al from 16-27)**

2.2. "*Cyber security*" means the condition in which road vehicles and their functions are protected ~~against threats~~ **from cyber threats to** ~~electrical or~~ electronic components **and system functions**.

Alternative proposal amendment (NL)

 **“*Cyber security*” means the condition in which assets are sufficiently protected against threat scenarios to electrical or electronic components of road vehicles and their functions**

Amendment with proposed amendment (NL comment)

2.3. "*Cyber Security Management System (CSMS)*" means a systematic risk-based approach defining organisational processes, responsibilities and governance to **~~treat~~** ~~cyber threats~~ **~~to vehicles~~** ~~and protect~~ *~~vehicles~~* ~~them from cyber- attacks~~ **treat risk associated with cyber threats to vehicles and protect them from cyber-attacks**”.

Proposed Amendment (GER) from GRVA-04-22

**2.x “*Cyber threat*" means threats to electronic components and network based information technology**

Amendment

**2.4 “*System*” means a set of components and/or sub-systems that implements a function or functions.**

**2.5 “*Development phase*” means the period before a vehicle type is type approved.**

**2.6 “*Production phase*” refers to the duration of production of a vehicle type.**

**2.7 “*Post-production phase*” refers to the time frame after the End of Production of a vehicle type. Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced.**

Proposed Amendment (GER) from GRVA-04-22

**2.8. "*Mitigation*" means a measure that is modifying risk.**

**Proposed amendment (NL) based on proposed EC amendment**

**2.9. "*Risk*" means ~~the effect of uncertainty on security objectives~~**  **potential that a given threat will exploit vulnerabilities of a vehicle and thereby cause harm to the organization or to an individual.**

**2.10. "*Risk Assessment*" means the overall process of finding, recognizing and describing risks (risk identification) , to comprehend the nature of risk and to determine the level of risk (risk analysis), and of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable (risk evaluation).**

**2.11. "*Risk Management*" means coordinated activities to direct and control an organization with regard to risk.**

**Proposed amendment based on proposed EC amendment**

**2.12. "*Threat*" means a potential cause of an unwanted incident, which may result in harm to a system, ~~or~~ organization or individual**

**2.13. "*Vulnerability*" means a weakness of an asset or mitigation that can be exploited by one or more threats.**

**Proposed amendment (FIGIEFA et al) from 16-27**

**2.14. "Decommissioning a vehicle” means a vehicle which the holder discards or intends or is required to discard in accordance with UN Regulation No 133**

 3. Application for approval

3.1. The application for approval of a vehicle type with regard to cyber security shall be submitted by the vehicle manufacturer or by their duly accredited representative.

3.2. It shall be accompanied by the undermentioned documents in triplicate, and by the following particulars:

3.2.1. A description of the vehicle type with regard to the items specified in Annex 1 to this Regulation.

3.2.2. In cases where information is shown to be covered by intellectual property rights or to constitute specific know-how of the manufacturer or of their suppliers, the manufacturer or their suppliers shall make available sufficient information to enable the checks referred to in this Regulation to be made properly. Such information shall be treated on a confidential basis.

Amendment

3.2.3. The ~~CSMS~~ Certificate of Compliance **for CSMS** according to paragraph 6 of this Regulation.

New suggested amendment (chair) with suggested amendment (US)

**3.3. Documentation shall be made available in two parts:**

**(a) The formal documentation package for the approval, containing the material specified in Annex 1 which shall be supplied to the Technical Service or Approval Authority at the time of submission of the type approval application. This documentation package shall be used by the Technical Service or Approval Authority as the basic reference for the approval process. The Technical Service shall ensure that this documentation package remains available for at least 10 years counted from the time when production of the vehicle type is definitely discontinued.**

**(b) Additional material relevant to the requirements of this regulation may be retained by the manufacturer, but made open for inspection at the time of type approval. The manufacturer shall ensure that ~~this~~ any material made open for inspection at the time of type approval remains available for at least a period of 10 years counted from the time when production of the vehicle type is definitely discontinued.**

 4. Marking

4.1. There shall be affixed, conspicuously and in a readily accessible place specified on the approval form, to every vehicle conforming to a vehicle type approved under this Regulation an international approval mark consisting of:

4.1.1. A circle surrounding the Letter "E" followed by the distinguishing number of the country which has granted approval.

4.1.2. The number of this Regulation, followed by the letter "R", a dash and the approval number to the right of the circle described in paragraph 4.1.1. above.

4.2. If the vehicle conforms to a vehicle type approved under one or more other Regulations annexed to the Agreement in the country which has granted approval under this Regulation, the symbol prescribed in paragraph 4.1.1. above need not be repeated; in this case the Regulation and approval numbers and the additional symbols of all the Regulations under which approval has been granted in the country which has granted approval under this Regulation shall be placed in vertical columns to the right of the symbol prescribed in paragraph 4.1.1. above.

4.3. The approval mark shall be clearly legible and shall be indelible.

4.4. The approval mark shall be placed on or close to the vehicle data plate affixed by the Manufacturer.

4.5. Annex 3 to this Regulation gives examples of the arrangements of the approval mark.

 5. Approval

5.1. Approval Authorities shall grant, as appropriate, type approval with regard to cyber security, only to such vehicle types that satisfy the requirements of this Regulation.

5.2. Notice of approval or of extension or refusal of approval of a vehicle type pursuant to this Regulation shall be communicated to the Parties to the 1958 Agreement which apply this Regulation, by means of a form conforming to the model in Annex 2 to this Regulation.

Amendment

5.3. Approval Authorities shall not grant any type approval without ~~ensuring~~ **verifying** that the manufacturer has put in place satisfactory arrangements and procedures to manage properly the cyber security aspects as covered by this Regulation.

Proposed Amendment (GER) from GRVA-04-22

5.4. For the purpose of paragraph 7.2. of this Regulation, the manufacturer shall ensure, **that** the cyber security aspects covered by this regulation are implemented.

Amendment

6. Certificate of Compliance for Cyber Security Management System ~~Certificate of Compliance~~

 Suggested amendment (UNISS)

**6.x.x               A Cyber Security Management System shall be implemented by the vehicle manufacturer.**

**6.x.x.              Suppliers and service providers shall implement a Cyber Security Management System.**

Amendment

6.1. Contracting Parties shall appoint an Approval Authority or Technical Service to carry out the ~~preliminary~~ **initial** assessment of the manufacturer and to issue a ~~CSMS~~ Certificate of Compliance **for CSMS**.

Amendment with amendment (Chair)

6.2. In the context of the ~~preliminary~~ **initial** assessment**,** ~~of~~ the manufacturer~~,~~ **shall declare ~~[~~using the model as defined in Appendix 1 to Annex 1 ~~XYZ]~~ and demonstrate to the satisfaction of** the Approval Authority or Technical Service ~~shall ensure~~ that ~~the manufacturer has~~ **they have** ~~installed~~ the necessary processes to comply with all ~~legal~~ **the** requirements ~~from this which are relevant~~ for cyber security according to this Regulation.

New suggested amendment (UK)

**6.2.1.             The application for Certificate of Compliance for Cyber Security Management System shall be submitted by the vehicle manufacturer or by their duly accredited representative.**

**6.2.2.             It shall be accompanied by documents describing the Cyber Security Management System in triplicate.**

Amendment with proposed amendment (Chair)

6.3. When this ~~preliminary~~ **initial** assessment has been ~~carried out~~ **satisfactorily completed ~~demonstrated~~ and in receipt of a signed declaration from the manufacturer ~~[~~according to the model as defined in Appendix 1 to Annex 1 ~~XYZ]~~**, a certificate named ~~CSMS~~ Certificate of Compliance **for CSMS** as described in Annex 4 to this Regulation (hereinafter the ~~CSMS~~ Certificate of Compliance **for CSMS**) shall be granted to the manufacturer.

Amendment

6.4. The Approval Authority or Technical Service shall use the model set out in Annex 4 to this Regulation for the ~~CSMS~~ Certificate of Compliance **for CSMS**.

Amendment with Proposed Amendment (GER) from GRVA-04-22

6.5. The ~~CSMS~~ Certificate of Compliance **for CSMS** shall remain valid for **a maximum of** three years from the date of deliverance of the certificate **unless it is withdrawn.**

Amendment

6.6. The Approval Authority which has granted the ~~CSMS~~ Certificate of Compliance **for CSMS** may at any time verify its continued validity. The ~~CSMS~~ Certificate of Compliance **for CSMS** may be withdrawn if the requirements laid down in this Regulation are no longer met.

Amendment

6.7. The manufacturer shall inform the Approval Authority or Technical Service of any ~~significant~~ change that **will** ~~could~~ affect the relevance of the ~~CSMS~~ Certificate of Compliance **for CSMS**. After consultation with the manufacturer, the Approval Authority or Technical Service shall decide whether new checks are necessary.

Amendment with Proposed Amendment (GER) from GRVA-04-22

6.8. At the end of the period of validity of the ~~CSMS~~ Certificate of Compliance **for CSMS**, the Approval Authority shall, **~~as appropriate~~** **after a renewed positive assessment**, issue a new ~~CSMS~~ Certificate of Compliance **for CSMS** or extends its validity for a further period of three years. The Approval Authority shall issue a new certificate in cases where ~~significant~~ changes have been brought to the attention of the Approval Authority or Technical Service **and the changes have been positively re-assessed**.

Amendment with Proposed Amendment (GER) from GRVA-04-22

6.9. Existing vehicle type approvals **~~shall~~** **may** not lose their validity due to the expiration of the manufacturer’s ~~CSMS~~ Certificate of Compliance **for CSMS**. **Vehicles without a valid Certificate of Compliance for CSMS may be classified as unsafe or dangerous due to national or regional legislation. The responsibility for services relevant to the cyber security of a vehicle type may be handed over to a third party other than the manufacturer, if this third party has a valid CSMS certificate for this vehicle type. In this case the original holder of the Certificate of Compliance for CSMS shall provide all information about the vehicle type necessary to acquire such certificate to this third party.**

Proposed amendment (UK)

**6.10.              At the discretion of Approval Authorities an application for Certificate of Compliance for Cyber Security Management System for a vehicle system may be made by system suppliers.**

Proposed amendment (UK)

**6.11.              If the vehicle manufacturer is not able to demonstrate that the processes described in their CSMS are implemented at the time of the initial assessment, the Technical Service or Approval Authority shall perform follow-up audits on an annual basis until the vehicle manufacturer is able to demonstrate their application or the relevant Certificate of Compliance for CSMS is no longer valid or is withdrawn.**

7. Specifications

7.1. General specifications

7.1.1. The requirements of this Regulation shall not restrict provisions or requirements of other UN Regulations.

Amendment with Proposed Amendment (GER) from GRVA-04-22

7.1.2. The vehicle manufacturer **~~may~~ shall** refer to [the Recommendation / Resolution on Cyber Security **and Interpretation Document]** in their assessment of cyber security risks and the mitigations, as well as when describing the processes employed.

 7.2. Requirements for the Cyber Security Management System

Amendment

7.2.1. For the ~~preliminary~~ **initial** assessment the Approval Authority or Technical Service shall verify that the vehicle manufacturer has a Cyber Security Management System in place and shall verify its compliance with this Regulation.

7.2.2. The Cyber Security Management System shall cover the following aspects:

Proposed Amendments (GER) from GRVA-04-22 and 16-27 (FIGIEFA et al)

7.2.2.1. The vehicle manufacturer shall demonstrate to ~~an~~ **the** Approval Authority ~~or~~ **and** Technical Service that their Cyber Security Management System considers the following phases **of the vehicle** that **they have designed, manufactured, have made commercially available and which remains in service until decommissioned** **for their commercially available and serviced fleet**:

- Development phase;

- Production phase;

- Post-production phase.

Amendment with Proposed Amendment (GER) from GRVA-04-22 and UNISS

7.2.2.2. The vehicle manufacturer and its suppliers shall demonstrate that the processes used within their Cyber Security Management System ensure security is adequately considered. This shall include:

(a)  The processes used within the manufacturer’s organization to manage cyber security **for vehicles, their systems and/or parts**;

 (b)  The processes used for the identification of risks to vehicle types; **and the respective IT infrastructure necessary for post-production services**;

 (c) The processes used for the assessment, categorization and treatment of the risks identified;

(d)  The processes in place to verify that the risks identified are appropriately managed;

(e)  The processes used for testing **~~verifying~~** the security of the ~~system~~ **vehicle type** ~~throughout its development and production phases~~;

(f)  The processes used for ensuring that the risk assessment is kept current;

(g)  The processes used to monitor for, detect and respond to cyber-attacks**, cyber threats and vulnerabilities** on vehicle types **and the processes used to assess whether the security measures implemented are still effective in the light of new threats and vulnerabilities that have been identified;**

**The processes shall be based on relevant established international standards where applicable.**

**Within the processes for identification of risks the threats in section IV and Annex B of the [the Recommendation / Resolution on Cyber Security] shall be considered.**

~~(h)  The processes used to identify new and evolving cyber threats and vulnerabilities to vehicle types;~~

~~(i)  The processes used to appropriately react to new and evolving cyber threats and vulnerabilities.~~

Amendment

7.2.2.3. ~~The vehicle manufacturer may refer to [the Recommendation / Resolution on cyber security] when describing the processes they have employed.~~

Amendment with comment

~~7.2.2.4~~ **7.2.2.3**. The vehicle manufacturer shall be required to demonstrate how their Cyber Security Management System will manage dependencies that may exist with contracted suppliers ~~and~~**,** service providers **or manufacturer’s other sub- organizations** in regards of the requirements of paragraph 7.2.2.2.

Proposed Amendment (GER) from GRVA-04-22

**7.2.3 For the initial assessment the Approval Authority or Technical Service shall further verify that the vehicle manufacturer has an Information Security Operations Centre (ISOC) in place and shall verify its compliance with this regulation**

**7.2.3.1 The ISOC shall be capable of and charged with the handling of the following tasks with respect to the IT infrastructure necessary for the provision of services to the manufacturers commercially available and serviced fleet**

 **- Proactive information collection and analysis focusing on the threat landscape for the manufacturers vehicle fleet;**

 **- Intrusion Detection and Prevention**

 **- Fast Incident Response**

 **- Running a Security Information and Event Management (SIEM) System**

 7.3. Requirements for vehicle types

 Amendment

7.3.1. Before the assessment of a vehicle type for the purpose of type approval is carried out the vehicle manufacturer shall demonstrate to the Approval Authority or Technical Service that their Cyber Security Management System has a valid ~~CSMS~~ Certificate of Compliance **for CSMS** relevant to the vehicle type being approved.

Amendment with Proposed Amendment (GER) from GRVA-04-22

7.3.2. The Approval Authority or Technical Service shall verify **by means of document checks and testing of sample vehicles** that the manufacturer has taken the necessary measures relevant for the vehicle type to:

(a) Collect and verify ~~as appropriate~~ information required under this **~~r~~R**egulation, through the ~~full~~ supply chain;

(b) **Document** ~~Maintain appropriate design and test information~~ **risk assessment, test results and mitigations applied to the vehicle type, including design information supporting the risk assessment**;

(c) Implement appropriate security measures in the design of the vehicle and its systems;

Amendment with Proposed Amendment (GER) from GRVA-04-22

7.3.3. The vehicle manufacturer shall demonstrate **to the satisfaction of the Approval Authority or Technical Service** the risk assessment for the vehicle type**~~,~~ and that it considers its ~~sub~~systems and their interactions** **and any external system relevant for the safe and secure operation of the vehicle** ~~in terms of the vehicle systems, the interactions of the different vehicle systems and the entire vehicle~~.

Amendment with Proposed Amendment (GER) from GRVA-04-22

7.3.4. The vehicle manufacturer shall demonstrate **to the satisfaction of the Approval Authority or Technical Service** ~~how the design of~~ **that** critical elements of the vehicle type are protected against risks identified in the vehicle manufacturer’s risk assessment. Proportionate mitigations shall be implemented to protect such elements.

Amendment with Proposed Amendment (GER) from GRVA-04-22

7.3.5. The vehicle manufacturer shall demonstrate **to the satisfaction of the Approval Authority or Technical Service** ~~how they have implemented~~ **that** appropriate and proportionate measures ~~to~~ ~~protect~~ **have been put in place to** **secure** dedicated environments on the vehicle type (if provided) for the storage and execution of aftermarket software, services, applications or data.

Proposed Amendment (GER) from GRVA-04-22

7.3.6. The vehicle manufacturer shall **~~describe~~ demonstrate** what testing has been performed to verify the effectiveness of the security measures implemented and the outcome of those tests.

**7.3.7. The vehicle manufacturers ISOC shall describe and demonstrate its capabilities to fulfill its tasks as described above with respect to the vehicle type in question for approval.**

 8. Modification and extension of the vehicle type

Amendment with proposed amendment (NL)

8.1. ~~Every modification of the vehicle type shall be notified to the approval authority which granted the approval.~~ **Every modification of the vehicle type which affects its technical performance with respect to cybersecurity and/or documentation required in this Regulation shall be notified to the approval authority which approved the vehicle type**. The Approval Authority may then either:

Amendment with proposed amendment (NL)

8.1.1. Consider that the modifications made ~~are unlikely to have an appreciable adverse effect and that in any case the vehicle still complies with the requirements~~ **still comply with the requirements and documentation of ~~prior~~ existing type approval**; or

8.1.2. Require a further test report from the technical service responsible for conducting the tests.

8.1.3. Confirmation or extension or refusal of approval, specifying the alterations, shall be communicated by means of a communication form conforming to the model in Annex 2 to this Regulation. The Approval Authority issuing the extension of approval shall assign a series number for such an extension and inform there of the other Parties to the 1958 Agreement applying this Regulation by means of a communication form conforming to the model in Annex 2 to this Regulation.

 9. Conformity of production

9.1. The Conformity of Production Procedures shall comply with those set out in the 1958 Agreement, Schedule 1 (E/ECE/TRANS/505/Rev.3) with the following requirements:

9.1.1. The holder of the approval shall ensure that results of the conformity of production tests are recorded and that the annexed documents remain available for a period determined in agreement with the Approval Authority or Technical Service. This period shall not exceed 10 years counted from the time when production is definitively discontinued;

9.1.2. The Approval Authority which has granted type approval may at any time verify the conformity control methods applied in each production facility. The normal frequency of these verifications shall be once every three years.

 10. Penalties for non-conformity of production

10.1. The approval granted in respect of a vehicle type pursuant to this Regulation may be withdrawn if the requirements laid down in this Regulation are not complied with or if sample vehicles fail to comply with the requirements of this Regulation.

10.2. If an Approval Authority withdraws an approval it has previously granted, it shall forthwith so notify the Contracting Parties applying this Regulation, by means of a communication form conforming to the model in Annex 2 to this Regulation.

Amendment

#  11. Production definitively discontinued

## 11.1 If the holder of the approval completely ceases to manufacture a type of vehicle approved in accordance with this Regulation, he shall so inform the authority which granted the approval. Upon receiving the relevant communication that authority shall inform thereof the other Contracting Parties to the Agreement applying this Regulation by means of a copy of the approval form bearing at the end, in large letters, the signed and dated annotation "PRODUCTION DISCONTINUED".

 Amendment

12 Names and addresses of Technical Services responsible for conducting approval test, and of type approval authorities

Amendment

**12.1** The Contracting Parties to the Agreement which apply this Regulation shall communicate to the United Nations Secretariat the names and addresses of the Technical Services responsible for conducting approval tests and of the Type Approval Authorities which grant approval and to which forms certifying approval or extension or refusal or withdrawal of approval, issued in other countries, are to be sent.

Annex 1

 Information document

The following information, if applicable, shall be supplied in triplicate and include a list of contents. Any drawings shall be supplied in appropriate scale and in sufficient detail on size A4 or on a folder of A4 format. Photographs, if any, shall show sufficient detail.

~~0. General~~

~~0.1 Make (trade name of manufacturer):~~

~~0.2. Type:~~

~~0.2.0.1 Chassis:~~

~~0.2.1. Commercial name(s) (if available):~~

~~0.3. Means of identification of type, if marked on the vehicle (b):~~

~~0.3.1. Location of that marking:~~

~~0.4. Category of vehicle (c):~~

~~0.8. Name(s) and address(es) of assembly plant(s):~~

~~0.9. Name and address of the manufacturer's representative (if any):~~

~~12. MISCELLANEOUS~~

~~12.8. Cyber Security~~

~~12.8.1. General construction characteristics of the vehicle type~~

~~12.8.1.1. Schematic representation of the vehicle type:~~

~~12.8.1.2. Documents for the vehicle type to be approved describing:~~

~~(a) The outcome of the risk assessment for the vehicle type;~~

~~(b) The vehicle systems (both type approved and non-type approved) which are relevant to the cyber security of the vehicle type;~~

~~(c) The components of those systems that are relevant to cyber security;~~

~~(d) The interactions of those systems with other systems within the vehicle type and external interfaces;~~

~~(e) The risks posed to those systems that have been identified in the vehicle type’s risk assessment;~~

~~(f) The mitigations that have been implemented on the systems listed, or to the vehicle type, and how they address the stated risks;~~

~~(g) What tests have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests.~~

~~12.8.2. The number of the CSMS Certificate of Compliance~~

**1. Make (trade name of manufacturer):**

**2. Type and general commercial description(s):**

**3. Means of identification of type, if marked on the vehicle:**

**4. Location of that marking:**

**5. Category(ies) of vehicle:**

**6. Name and address of manufacturer/ manufacturer's representative:**

**7. Name(s) and Address(es) of assembly plant(s):**

**8. Photograph(s) and/or drawing(s) of a representative vehicle:**

**9. Cyber Security**

**Amendment in ad-hoc meeting**

**9.1. General construction characteristics of the vehicle type, including:**

1. **The vehicle systems which are relevant to the cyber security of the vehicle type;**
2. **The components of those systems that are relevant to cyber security;**
3. **The interactions of those systems with other systems within the vehicle type and external interfaces;**

**9.2. Schematic representation of the vehicle type**

**9.3. The number of the Certificate of Compliance for CSMS**

**Amendment in ad-hoc meeting, in yellow for further consideration**

~~9.4. [Documents for the vehicle type to be approved describing:~~

1. ~~The outcome of the risk assessment for the vehicle type;~~
2. ~~The vehicle systems (both type approved and non-type approved) which are relevant to the cyber security of the vehicle type;~~
3. ~~The components of those systems that are relevant to cyber security;~~
4. ~~The interactions of those systems with other systems within the vehicle type and external interfaces;~~
5. ~~The risks posed to those systems that have been identified in the vehicle type’s risk assessment;]~~

**9.4. Documents for the vehicle type to be approved describing the outcome of its risk assessment,** [**including risks posed to those systems that have been identified in the vehicle type’s risk assessment**~~]~~

**9.5 Documents for the vehicle type to be approved describing the mitigations that have been implemented on the systems listed, or to the vehicle type, and how they address the stated risks;**

**9.6. Documents for the vehicle type to be approved describing protection of dedicated environments for aftermarket software, services, applications or data**

**9.7. Documents for the vehicle type to be approved describing what tests have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests.**

**9.8. Description of the consideration of the supply chain with respect to cyber security.**

Proposed amendment (UK and OICA)

**Appendix 1 to Annex 1 Information document**

**Manufacturer’s declaration of compliance with the requirements for the Cyber Security Management System**

**Manufacturer Name: …………………………………………………………………………**

**Manufacturer Address: ………………………………………………………………………**

**We have installed the necessary processes to comply with the requirements for the Cyber Security Management System laid down in paragraph 7.2 of UN Regulation [15x].**

**Done at: …………………… (place)**

**Date: ………………**

**Name of the signatory: ………………**

**Function of the signatory: ………………**

**……………………………………………**

**(Stamp and signature of the manufacturer’s representative)**

Annex 2

 Communication form

COMMUNICATION

(Maximum format: A4 (210 x 297 mm))

issued by : Name of administration:

......................................

......................................

......................................



concerning: 2/ APPROVAL GRANTED

 APPROVAL EXTENDED

 APPROVAL REFUSED

 APPROVAL WITHDRAWN

 PRODUCTION DEFINITELY DISCONTINUED

of a vehicle type with regard to xxx equipment pursuant to Regulation No. **X**

Approval No. ………..

…

x.y ……

Amendment

**Extension No.:**

**1. Make (trade name of manufacturer):**

**2. Type and general commercial description(s)**

**3. Means of identification of type, if marked on the vehicle:**

**3.1. Location of that marking:**

**4. Category(ies) of vehicle:**

**5. Name and address of manufacturer / manufacturer’s representative:**

**6. Name(s) and Address(es) of the production plant(s)**

**7. Number of the certificate of compliance for cyber security management system:**

**8. Technical Service responsible for carrying out the tests:**

**9. Date of test report:**

**10. Number of test report:**

**11. Remarks: (if any).**

**12. Place:**

**13. Date:**

**14. Signature:**

**15. The index to the information package lodged with the Approval Authority, which may be obtained on request is attached.**

Annex 3

 Arrangement of approval mark

Model A

(See paragraph 4.2 of this Regulation)



xxx

 a = 8 mm min.

Amendment

 The above approval mark affixed to a vehicle shows that the road vehicle type concerned has been approved in the Netherlands (E 4), pursuant to Regulation No. xxx, and under the approval number 002492. The first two digits of the approval number indicate that the approval was granted in accordance with the requirements of **this** Regulation ~~No. xx~~**~~.~~ in its original form (00)**.

Annex 4

Amendment

 Model of ~~CSMS~~ Certificate of Compliance for CSMS

~~CYBER SECURITY MANAGEMENT SYSTEM CERTIFICATE OF COMPLIANCE~~

**CERTIFICATE OF COMPLIANCE FOR CYBER SECURITY MANAGEMENT SYSTEM**

WITH REGULATION No. [Cyber Security Regulation] xxx

No. [Reference number]

[……. Approval Authority]

Certifies that

Manufacturer: ...........................................................................................................................

Address of the manufacturer: ...................................................................................................

complies with the provisions of paragraph 7**.2** of Regulation No. xxx

Checks have been performed on:

by (name and address of the Type Approval Authority or Technical Service):

Number of report:

The certificate is valid until […..date]

Done at [……Place]

On […….Date]

[………….Signature]

**Attachments: description of the Cyber Security Management System by the manufacturer.**