TABLE OF CONTENTS

A. STATEMENT OF TECHNICAL RATIONALE AND JUSTIFICATION

B. TEXT OF REGULATION

1. SCOPE AND PURPOSE

2. DEFINITIONS

3. REQUIREMENTS

**A. STATEMENT OF TECHNICAL RATIONALE AND JUSTIFICATION**

**B. GLOBAL TECHNICAL REGULATION ON CYBER SECURITY**

1. SCOPE AND PURPOSE

 This regulation applies to vehicles of Category 1, Category 2, [Category 3} and trailers. The purpose of this regulation is to ensure the safe execution of vehicle software updates.

2. DEFINITIONS

2.1. Cyber security means the use of technologies, processes and practices designed to protect vehicles, vehicle systems, networks, devices and services – and their information, data and functionality – from theft, damage, attack or unauthorized access.

 (new language below)

 means the condition in which stakeholders' assets are protected against threats to electrical or electronic components of road vehicles and their functions.

2.2. Cyber security management system (CSMS) means a systematic risk-based approach defining organizational processes, responsibilities and governance to protect vehicles from cyber threats and cyber-attacks.

2.x Download means the process of copying data from the manufacturer’s computer system to a vehicle.

2.x. Electronic Control System means a combination of units, designed to co-operate in the production of the stated vehicle control function by electronic data processing. Such systems, controlled by software, are built from discrete functional components such as sensors, electronic control units and actuators and are connected by transmission links. It may include mechanical, electro-pneumatic or electro-hydraulic elements.

2.x. Execution means the process of installing and activating a software update that has been downloaded.

2.x. Risk means the combination of the consequences of an event and the associated likelihood of occurrence of that event.

2.x. [RX Software Identification Number (RXSWIN) means a dedicated identifier, defined by the vehicle manufacturer, representing information about the software of the Electronic Control System.]

2.x. Software means the part of an Electronic Control System that consists of digital data and instructions.

2.x. Software update means a package used to install a new version of software. The update may contain a fix for a specific problem or introduce new product functionality. Note: The terms "update" and "upgrade" are synonymous when referring to installing new versions of software.

2.x. Threat means the potential cause of an unwanted incident, which may result in harm to a system or organization.

2.x. Update process means the steps involved in the downloading and execution of new versions of software.

2.x. Vehicle user means a person operating or driving the vehicle, a vehicle owner, an authorized representative or employee of a fleet manager, an authorized representative or employee of the vehicle manufacturer, or an authorized technician.

2.3. ~~Vehicle type means vehicles of a particular category that do not differ in at least the following essential respects:~~

~~2.3.1 The manufacturer;~~

~~2.3.2 The manufacturer’s type designation;~~

~~2.3.3 The manufacturer’s cyber security management system; and,~~

~~2.3.4 Essential aspects of vehicle design with respect to cyber security.~~

3. REQUIREMENTS

3.1. Requirements for cyber security management systems

3.1.1. The cyber security management system shall be operational over the following phases:

* Development phase;
* Production phase;
* Post-production phase.

3.1.2. The following processes are part of the cyber security management system:

* The processes used within the manufacturer’s organization to manage cyber security;
* The processes used for the identification of risks to the vehicle;
* The processes used for the assessment, categorization and treatment of the risks identified;
* The processes in place to verify that the risks identified are appropriately managed;
* The processes used for testing the security of the system throughout its development and production phases;
* The processes used for ensuring that the risk assessment is kept current;
* The processes used to monitor for, detect and respond to cyber-attacks on vehicles;
* The processes used to identify new and evolving cyber threats and vulnerabilities to the systems and vehicles during post production phase;
* The processes used to maintain the safety, integrity and availability of the vehicles during postproduction phase in the face of new and evolving cyber threats and vulnerabilities.

3.2. Requirements for Software Updates

3.2.1. The vehicle manufacturer shall have the following processes in place:

* A process whereby the software and hardware components of the cyber security management system can be uniquely identified documented and recorded as well as any interdependencies of that system on other systems.
* A process whereby the vehicle manufacturer can assess, identify and record if a software update will affect the safe and continued operation of a vehicle or if the update will add or alter functionality of the vehicle.
* A process whereby a vehicle manufacturer can identify target vehicles for a software update.
* A process to verify the compatibility of possible software/ hardware configurations in target vehicles.
* A process to record the status of software updates in the target vehicles that can be checked.
* A process to trace the software versions and verify that they are correct (and is able to provide this information to an authority should it be required).
* A process to inform national authorities about successful software updates if required.

3.2.2. The vehicle manufacturer shall inform the vehicle user about the update before the update is executed. The notification shall contain:

* The purpose of the update. This should include an evaluation of the criticality of the update, and if the update is for recall, safety and/or security purposes;
* Any changes to vehicle functions that would be implemented by the updates;
* The expected time to complete execution of the update;
* If applicable, any vehicle functionalities which will not be available during the execution of the update;
* Any necessary instructions in order for the vehicle user to safely execute the update;
* In case of groups of updates with a similar content one information may cover a group.

3.2.3. Execution of a software update.

3.2.3.1. Except as provided in section 3.3.2.3., the location and movement of the vehicle shall not be restricted during the download stage of a software update.

3.2.3.2. The software update shall only be executed when the vehicle has enough power to complete the update process (including that needed for a possible recovery to the previous version or for the vehicle to be placed into a safe state).

3.2.3.3. If the execution of an update whilst driving might pose a safety hazard, or would restrict any vehicle functions, the vehicle manufacturer shall:

* Notify the vehicle user as required by section 3.3.1; and,
* Ensure the vehicle cannot be driven during the execution of the update; or
* Ensure that the driver is not able to use any functionality of the vehicle that would affect the safety of the vehicle or the successful execution of the update.

3.2.4. The vehicle manufacturer shall ensure that the system being updated can be restored to the previous version after a failed or interrupted update or the vehicle can be placed into a safe state.

- - - - -