**From:** Ross Hughes <Ross.Hughes@vca.gov.uk>
**Sent:** Monday, December 6, 2021 3:14 PM
**To:** GALASSI Maria Cristina (JRC-ISPRA) <Maria-Cristina.GALASSI@ec.europa.eu>
**Subject:** VMAD & R155

Hello Christina,

R155 Also has [an interpretation document](https://urldefense.com/v3/__https%3A/unece.org/fileadmin/DAM/trans/doc/2020/wp29/WP29-182-05e.pdf__;!!DOxrgLBm!UA2A_kFa5ZiNwIZ22UVXKXTi0cjdt8j1P65r_Us6Vt2uVOmFXysOCa8gsKKgQTbyPnT7oaIrB_IgOQ$):

Paragraph 7.4.

7.4. Reporting provisions

7.4.1. “**The vehicle manufacturer shall report at least once a year, or more**

**frequently if relevant, to the Approval Authority or the Technical Service**

**the outcome of their monitoring activities, as defined in paragraph**

**7.2.2.2.(g)), this shall include relevant information on new cyber-attacks.**

**The vehicle manufacturer shall also report and confirm to the Approval**

**Authority or the Technical Service that the cyber security mitigations**

**implemented for their vehicle types are still effective and any additional**

**actions taken.”**

Explanation of the requirement

The main purpose of this requirement is to confirm that the aspects of the CSMS related

to the cyber security monitoring activities, as defined in paragraph 7.2.2.2.(g), continue

to be applied properly after Development Phase and that the relevant cyber security

mitigations implemented continue to be effective.

The manufacturer shall at least annually report to the Type Approval Authority who

granted the type approval or the Technical Service who verified the compliance of its

CSMS with this Regulation. The reporting should be more frequent if events such as new

cyber-attacks are observed, especially to report on any actions taken.

Examples of documents/evidence that could be provided

The following standards may be applicable:

(a) ISO/SAE 21434 defines [WP-07-02] Results from the triage of cybersecurity

information and [WP-07-04] Vulnerability Analysis. Both can be used as the

baseline for the required reporting.

Regards
Ross