LIN LLC

Mobility Legal Updates

September 3rd, 2025

LIN's Mobility Team monitors legal and regulatory trends in the automotive industry and periodically sends newsletters to our clients.

The amended Motor Vehicle Management Act came into effect on August 14, 2025. A key aspect of this amendment is the requirement for vehicle manufacturers and others, when seeking self-certification for specific vehicles, to first establish a Cyber Security Management System (CSMS). This system must be certified by the Minister of Land, Infrastructure and Transport and must include procedures, *inter alia*, for detecting and responding to cybersecurity threats and attacks, as well as for ensuring secure software updates.

This newsletter will introduce the newly enacted Enforcement Decree and Enforcement Rule that accompany the amended Act and discuss their key implications.[1]

1. Partial Amendment to the Enforcement Decree of the Motor Vehicle Management Act (Presidential Decree No. 35703, effective August 14, 2025)

A. Key Provisions

- Any person that performs a software update without adhering to the compliance requirements stipulated in Articles 34-5(1)(1) through 34-5(1)(3) of the Act[2] may be

[1] The department in charge is the Autonomous Driving Policy Division of the Ministry of Land, Infrastructure and Transport.

[2] **Article 34-5 (Software Updates by Vehicle Manufacturers, etc.)**

subject to an administrative fine of up to 2% of the revenue from the sales of the relevant motor vehicle or part, capped at KRW 1 billion (Article 74(3)(6) of the Act, Article 15(5) of the Enforcement Decree and 2. Sub-item (Ra)-2 of [Attached Table 1-3]).

- A fine of KRW 5 million may be imposed on any person that conducts an update in violation of the compliance requirements under Articles 34-5(1)(4) through 34-5(1)(6) of the Act[3] (Article 84(2)(3-2) of the Act and Article 20 of the Enforcement Decree and 2. Sub-item (Do)-2 of [Attached Table 2]).
- Additionally, the Minister of Land, Infrastructure and Transport is authorized to order a restriction on a vehicle's operation if a cyberattack or threat occurs that could pose a serious risk to the vehicle's safe operation or to public safety (Article 25(1)(3) of the Act and Article 5 of the Enforcement Decree).

B. Implications

The failure to maintain compliance with safety standards after a vehicle software update has now been included as grounds for the imposition of administrative fines under the Motor Vehicle Management Act, which has the effect of compelling the obligations of vehicle manufacturers, etc. and parts manufacturers. Furthermore, since an inadequate response to cyberattacks and threats can lead to an order to restrict vehicle operation, it is imperative for

---

(1) When a vehicle manufacturer, etc. conducts a software update (hereinafter referred to as an "update"), which includes providing software that performs the update to vehicle users or vehicle maintenance businesses, etc. (the same shall apply hereinafter), they shall comply with the following:

1. To ensure that all devices and functions of the vehicle operate normally even after the update;
2. To ensure that the structure and devices of the vehicle related to the said update conform to the Vehicle Safety Standards even after the update;
3. To ensure that the update is conducted safely in a state protected from cyberattacks and threats targeting vehicles;

[3] Article 34-5 (Software Updates by Vehicle Manufacturers, etc.)
(1) When a vehicle manufacturer, etc. conducts a software update (hereinafter referred to as an "update"), which includes providing software that performs the update to vehicle users or vehicle maintenance businesses, etc. (the same shall apply hereinafter), they shall comply with the following:

4. To provide information regarding the said update to the vehicle user before and after conducting the update;
5. To record and retain the details and history of the update, and to prevent the damage, loss, forgery, or alteration thereof;
6. Other matters prescribed by the Ordinance of the Ministry of Land, Infrastructure and Transport as necessary for a safe and smooth update.

related companies to establish robust internal security systems in advance.

2. Partial Amendment to the Enforcement Rule of the Motor Vehicle Management Act (Ministry Ordinance No. 1519, effective August 14, 2025)

A. Key Provisions

The amendment introduces key provisions that stipulate the Cyber Security Management System (CSMS) certification and detailed procedures for the Software Update Management System (SUMS). The main points include: (i) the introduction of a CSMS certification process (Article 40-27); (ii) regulations for modification and renewal (Article 40-28); and (iii) the establishment of new software update management procedures (Articles 56-12 to 56-14).

B. Implications

Vehicle manufacturers and importers are now required to establish and periodically renew their CSMS. Additionally, a process for prior notification and verification of impact on safety standards is now necessary for Over-the-Air (OTA) software updates. Meanwhile, the implementation of detailed SUMS procedures is significant as it formally codifies the legal duties, procedural steps, and subsequent liabilities for each stage of a software update to manage risks associated with software modifications, etc.

Consequently, companies must now design their cybersecurity and software update systems to meet certification standards from the initial development stage. It is also advisable to create internal checklists to track the certification validity period (3 years) and the grounds for modification certification.

3. Partial Amendment to the Rule on Standards and Procedures for Administrative Dispositions under Provisions such as Article 21(2) of the Motor Vehicle Management Act (Ministry Ordinance No. 1521, effective August 14, 2025)

A. Key Provisions

This rule has been amended to provide clear standards for administrative dispositions (e.g., suspension or revocation of certification) corresponding to specific violations, in line with newly established articles in the amended Motor Vehicle Management Act, such as Article 30-9 (CSMS Certification) and Article 30-11 (Cancellation or Suspension of Certification).

- Certification shall be revoked if it was obtained through false or improper means or if a certified vehicle is sold while its certification is suspended (in violation of Article 30-11(1) of the Act).
- For violations such as failure to obtain modification certification, failure to report modifications, or maintaining a state of non-compliance with certification standards, penalties will escalate with each subsequent offenses, from the first to the third violation. A third violation will result in the revocation of the certification (in violation of Article 30-9(2) and Article 30-11(1)(3) through (5) of the Act).

B. Implications

Vehicle manufacturers and importers face immediate administrative actions (suspension or revocation) not only for failing to obtain CSMS certification but also for violating obligations related to its maintenance, modification, and data submission. Since a certification revocation directly impacts a model's sales, a robust internal compliance monitoring process is essential.

Furthermore, companies must establish procedures for proactively reporting and renewing certification when changes occur (e.g., in organization, security systems, or scope of certification). It will also be critical to monitor how the Ministry of Land, Infrastructure and Transport applies its standards for aggravating or mitigating circumstances in actual enforcement cases to inform practical responses.

4. Partial Amendment to the Rule on Performance and Standards of Motor Vehicles and Parts (Ministry Ordinance No. 1520, effective August 14, 2025)

A. Key Provisions

- **Cybersecurity Safety Standards (Article 18-4):** New safety standards for cybersecurity have been established. In line with the introduction of CSMS, these standards define the fundamental cybersecurity requirements for vehicles, including technical standards for communication security, data integrity, and access control to defend against external attacks like hacking and remote intrusion.
- **Software Update (SUMS) Safety Standards (Article 18-5):** Safety standards for software updates have been introduced. For vehicles equipped with OTA update capabilities, the rule specifies safety standards for the update mechanism and incorporates procedures for verification, rollback, and safety confirmation to ensure that compliance with safety standards is maintained during updates.

B. Implications

Companies must build internal processes to verify the safety of their OTA update devices and procedures, as well as to handle prior reporting and compliance checks. Failure to establish such a software update operation system significantly impact vehicle sales. Significantly, these regulations extend beyond vehicle manufacturers to encompass the entire automotive parts and software supply chain. As a result, this topic is expected to become a central agenda item for all related businesses, including those involved in vehicle exterior, interior device, and software management.

LIN has extensive experience in providing advisory and litigation services in the mobility industry, particularly in areas such as administrative regulations and patent and trade secret disputes related to motor vehicles. Our Mobility Team consists of attorneys and experts with a distinctive interest and passion for automobiles.

Should you wish to learn more about this newsletter or have any other inquiries, please do not hesitate to contact our firm's **Mobility Team**.
