Amendment No. 1 to National Standard GB 44495-2024 *Technical Requirements for Vehicle Cybersecurity*

(Draft for Approval)

I. Throughout the text, "cybersecurity management system" and "requirements for cybersecurity management system" were changed to "cybersecurity assurance requirements". The specific provisions involved are as follows:

1. "1 Scope" was changed to: This document specifies the vehicle cybersecurity assurance requirements, basic requirements for cybersecurity, technical requirements for cybersecurity and determination of the same type, and describes the corresponding inspection and test methods. This document is applicable to vehicles of categories M and N, and does not apply to special vehicles modified based on Type II chassis or complete vehicles that have obtained type approval.

2. The term and definition of 3.2 were deleted.

3. The title of Chapter 5 (also in the Table of Contents) was changed to: Vehicle Cybersecurity Assurance Requirements.

4. The first sentence of 5.1 was changed to: The vehicle manufacturer shall meet the vehicle cybersecurity assurance requirements for the full life cycle of the vehicle.

5. The first sentence of 5.2 was changed to: Vehicle cybersecurity assurance requirements shall include the following.

6. 6.1 was changed to: The vehicle product development process shall follow the vehicle cybersecurity assurance requirements.

7. The first sentence of 8.1 was changed to: The inspection and test methods include vehicle cybersecurity assurance requirements inspection, basic requirements inspection and technical requirements test.

II. Throughout the text, "check" was changed to "inspect". The specific provisions involved are as follows:

1. The title of Chapter 8 (also in the Table of Contents) was changed to: Inspection and Test Methods.

2. The content of 8.1 was changed to: The inspection and test methods include vehicle cybersecurity assurance requirements inspection, basic requirements inspection and technical requirements test:

- Documentation related to the vehicle manufacturer's cybersecurity assurance requirements shall be inspected to confirm that the vehicle manufacturer meets the requirements specified in Chapter 5;

- Documentation related to cybersecurity in the process of vehicle development and production shall be inspected to confirm that the vehicle under test (VUT) complies with the requirements specified in Chapter 6;

- The test scope of technical requirements for vehicle cybersecurity shall be confirmed according to 8.3 based on the identified risks of the vehicle and the relevance of handling measures in Chapter 7, and tests shall be carried out according to the test scope to confirm that the vehicle meets the requirements specified in Chapter 7.

Note: The test scope includes the clauses of Chapter 7 applicable to the VUT and the test objects corresponding to each applicable clause.

3. Modify 8.2 as follows:

8.2 Inspection of basic requirements for cybersecurity

8.2.1 Inspection requirements

8.2.1.1 The vehicle manufacturer shall keep documentation describing the cybersecurity of vehicles during development and production, including documentation submitted and retained.

8.2.1.2 The documentation submitted shall be in Chinese and include at least:

- a summary document demonstrating that the vehicle meets the requirements specified in Chapter 6;
- a list of documentation retained, with the version information.

8.2.1.3 The vehicle manufacturer shall retain the process documentation related to vehicle cybersecurity locally in a secure manner, and take tamper-proofing measures for documentation retained after inspection.

8.2.1.4 The vehicle manufacturer shall make a self-declaration on the consistency and traceability of the documentation submitted and retained with the vehicle.

8.2.2 Inspection method

8.2.2.1 Inspect the documentation submitted by the vehicle manufacturer and confirm the inspection scheme, including the inspection scope, method and schedule and a list of necessary supporting documentation for on-site inspection.

8.2.2.2 Inspect the cybersecurity-related process documentation retained at the vehicle manufacturer's site according to the inspection scheme confirmed in 8.2.2.1, to confirm whether the vehicle meets the requirements of Chapter 6.

4. 8.3.2.2.1 b) was changed to: Forge, tamper with and send remote vehicle control instructions to inspect whether the instructions can be forged or tampered with and whether the vehicle executes the instructions.

5. 8.3.2.2.3 a) was changed to: Trigger the remote vehicle control function, and inspect whether there is a security log and whether the contents recorded in the security log include information such as the time, sender, remote control object and operation results of the remote control instructions.

6. 8.3.2.2.3 b) was changed to: Inspect whether the time span of security logging is not less than 6 months or whether security incident logs can be kept for at least 6 months.

7. 8.3.3.1 b) was changed to: If the vehicle communicates with the vehicle manufacturer's cloud platform in a public network environment using a public communication protocol, the tester shall use a network data packet capture tool to capture data packets and parse the communication message data, to inspect whether the vehicle verifies the identity authenticity of the vehicle manufacturer's cloud platform. If data packets cannot be captured with the network data packet capture tool, the tester shall confirm whether the vehicle meets the requirements of 7.2.1 according to the supporting documents on communication identity authenticity of the vehicle cloud platform provided by the manufacturer.

8. 8.3.3.3 was changed to: The tester shall trigger the transmission of external wireless communication data of the vehicle in turn according to the list of external communication channels such as vehicle mobile cellular communication, WLAN and Bluetooth provided by the vehicle

manufacturer, and capture the packets of external wireless communication channel data of the vehicle with test equipment, to check whether an integrity protection mechanism is adopted for the channels and determine whether the vehicle meets the requirements of 7.2.3. If packets of vehicle mobile cellular communication data cannot be captured with the test equipment, the tester shall determine whether the vehicle meets the requirements of 7.2.3 according to the supporting documentation on integrity protection of vehicle mobile cellular communication channel provided by the manufacturer.

9. 8.3.3.4 was changed to: The tester shall use an unauthorized identity to operate, clear and write the vehicle data beyond the access control mechanism in turn through the external communication channel of the vehicle to inspect whether the data may be operated, cleared and written and determine whether the VUT meets the requirements of 7.2.4.

10. 8.3.3.5 was changed to: The tester shall use the test equipment to record the critical instruction data according to the list of critical instruction data provided by the vehicle manufacturer and resend the recorded instruction data, to inspect whether the vehicle responds and determine whether the vehicle meets the requirements of 7.2.5.

11. 8.3.3.6 was changed to: The tester shall trigger the function of transmitting sensitive personal information from the vehicle to the outside according to the list of functions provided by the vehicle manufacturer and capture the transmitted data packets using the port and access permission provided by the vehicle manufacturer, to inspect whether the sensitive personal information transmitted by the vehicle is encrypted and determine whether the vehicle meets the requirements of 7.2.6.

12. 8.3.3.7 was changed to: The tester shall replace the components used for direct wireless communication between the VUT and the outside with those unauthorized of the same model and install them at the same locations of the VUT according to the list of components used for direct wireless communication between the VUT and the outside provided by the vehicle manufacturer, and then start the vehicle, to inspect whether such components function abnormally or whether the vehicle gives an alarm for abnormal component connection and determine whether the vehicle meets the requirements of 7.2.7.

13. 8.3.3.12 a) was changed to: Construct and trigger a critical vehicle communication cybersecurity incident to inspect whether the incident is recorded according to the logging mechanism of critical communication cybersecurity incidents;

14. 8.3.3.12 b) was changed to: Inspect whether the time span of logging is not less than 6 months or whether incident logs can be kept for at least 6 months.

15. 8.3.4.2.1 b) was changed to: If the vehicle communicates with the over-the-air update server in a public network environment using a public communication protocol, the tester shall use the test equipment to capture data packets and parse the communication message data to inspect whether the vehicle verifies the identity authenticity of the over-the-air update server; interrupt and then resume the download, use the test equipment to capture data packets and parse the communication message data to inspect whether the identity authenticity is verified again. If data packets cannot be captured with the test equipment, the tester shall confirm whether the vehicle meets the requirements of 7.3.2.1 according to the supporting documents for the identity authentication security function of the over-the-air update server provided by the manufacturer;

16. 8.3.4.2.2 b) was changed to: After confirming that the over-the-air update function is normal, construct an update package with damaged authenticity and integrity, download or transmit this update package to the vehicle according to the method and permission provided by the vehicle manufacturer, and perform software update to test whether the update is successful. If the vehicle cybersecurity protection mechanism does not support downloading or transmitting this update

package to the vehicle, inspect whether the vehicle meets the requirements of 7.3.2.2 according to the supporting documentation of over-the-air update cybersecurity protection mechanism provided by the vehicle manufacturer.

17. 8.3.4.2.3 a) was changed to: Construct an update security event and inspect whether there is an online update cybersecurity event log;

18. 8.3.4.2.3 b) was changed to: Inspect whether the time span of logging is not less than 6 months or whether incident logs can be kept for at least 6 months.

19. 8.3.5.1 b) was changed to: If the key is stored in a hardware security module such as HSM, inspect whether the vehicle is equipped with a hardware security module to protect the key at the location indicated in the document describing the installation location of the hardware security module;

20. 8.3.5.1 c) was changed to: If the key is stored in a secure software storage form, inspect whether the key is stored in a secure manner according to the supporting documentation provided by the vehicle manufacturer to ensure the secure storage of the vehicle key.

21. 8.3.5.6 was changed to: The tester shall use the personal information clearing function of the VUT, confirm the test components, trigger the personal information recording functions of the vehicle in turn and clear the personal information stored in the vehicle, to inspect whether such personal information is completely deleted through the component debugging interface according to the list of personal information stored in the vehicle and the storage address provided by the vehicle manufacturer, and determine whether the vehicle meets the requirements of 7.4.6.

22. 8.3.5.7 was changed to: The tester shall enable all mobile cellular communication channels and WLAN communication channels of the vehicle, successively simulate that the VUT is not powered on, just powered on, and powered on with various pre-installed data transmission functions normally enabled, then use a network data packet capture tool to capture data packets from the external communication network channels simultaneously for not less than 3600 s in total and parse the communication message data, to inspect whether the destination IP address contains an overseas IP address and determine whether the vehicle meets the requirements of 7.4.7.

III. The first item "The cybersecurity management system is effective" in 9.1 and 9.2 was changed to: The relevant contents of vehicle cybersecurity assurance requirements in the inspection and test report on technical requirements for vehicle cybersecurity are valid and the date of issuance does not exceed three years.

IV. The text in Chapter 10 was changed from "For new vehicles under type approval, the standard shall be executed from the implemented date of this document." to: For new vehicles under type approval, the standard shall be executed from the 7th month since the implemented date of this document.