

ICS 35.240.50

CCS L 67



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 46885-2025

Digital supply chain - General safety requirements

数字化供应链 通用安全要求

Issued on: December 31, 2025

Implemented on: April 1, 2026

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

1.Scope	1
2 Normative References	1
3.Terms and Definitions	1
4.Abbreviations	2
5 Basic Principles	2
5.1 Improved resilience	2
5.2 Full-chain visibility	2
5.3 Dynamic Flexibility	2
5.4 Internal and External Collaboration	2
6.Safety Management Requirements	2
6.1 System adaptability requirements	2
6.2 Business Continuity Requirements	3
6.3 Technical Reliability Requirements	4
6.4 Data security requirements	5
6.5 Funding Stability Requirements	6
7 Safety assessment requirements	6
7.1 Indicator System	6
7.2 Evaluation Methods	7
7.3 Evaluation Process	8
10 Reference	18

Foreword

This document complies with the provisions of GB/T 1.1-2020 "Standardization Work Guidelines Part

1.Structure and Drafting Rules of Standardization Documents". Drafting. Please note that some content in this document may involve patents. The issuing organization of this document assumes no responsibility for identifying patents. This document was proposed by the Ministry of Industry and Information Technology of the People's Republic of China. This document is under the jurisdiction of the National Technical Committee on Standardization of the Integration of Informatization and Industrialization (SAC/TC573). This document was drafted by: National Industrial Information Security Development Research Center, Chengdu Aircraft Industry (Group) Co., Ltd., and National Energy Administration.

Group Materials Co., Ltd., Inspur Smart Supply Chain Technology (Shandong) Co., Ltd., Inspur General Software Co., Ltd., and AVIC International Gold Network (Beijing) Technology Co., Ltd., Kunlun Digital Technology Co., Ltd., Shanghai Electrical Apparatus Research Institute (Group) Co., Ltd., COSMOPlat Digital Technology (Shanghai) Co., Ltd. Hai) Co., Ltd., Inspur Cloud Industrial Internet Co., Ltd., Jiangsu Zhixin Traceability Information Technology Research Institute Co., Ltd., Tianjin University, Architecture Materials Industry Information Center, State Grid Corporation of China, State Grid Zhejiang Electric Power Co., Ltd., Shanghai Standards Association, Haidebang International Logistics Control Guangdong Power Grid Co., Ltd. Guangzhou Power Supply Bureau, Industrial Cloud Manufacturing (Sichuan) Innovation Center Co., Ltd., China Communications Construction Second Engineering Bureau Co., Ltd. Public Works Bureau Third Engineering Co., Ltd., Shanghai Computer Software Technology Development Center, Youlai (Beijing) Technology Co., Ltd., National Pipeline Group North Beijing Pipeline Co., Ltd., Huaqin Technology Co., Ltd., Dongfang Electric Group Dongfang Turbine Co., Ltd., Zhengzhou Yunzhixin'an Security Technology Co., Ltd. Limited Liability Company, Yidao Xin'an (Beijing) Technology Co., Ltd., Zhejiang Lanbes Information Technology Co., Ltd., and Sichuan Xianglilai Technology Co., Ltd. The main drafters of this document are. Xu Shunyi, Dou Keqin, Li Jun, Song Yuguang, Sun Shiguo, Zheng Yi, Liang Weicong, Zhang Di, Zheng Weibao, and Zhang Chaoyang. Zhou Haipeng, Chen Wei, Liu Weihua, Li Yanlei, Zhang Liang, Si Qile, Jiang Yuan, Wang Jinde, Shi Qingchao, Bao Yude, Pang Songtao, Luo Tao, Yu Huaide, Li Menglong Liu Xin, Luo Chao, Liu Botao, Man Yongping, Zhou Jia, Zhang Meng, Yuwen Daojing, Wang Yanjun, Qian Xuetao, Xiong Jiankun, Zhang Qiankun, Huang Caixia, Li Haibing Yu Feng and Luo Yi.

Ensuring supply chain security is not only a practical necessity for the normal operation of enterprises, but also essential for maintaining industrial chain security, stabilizing national economic development, and building a community with a shared future for mankind. A crucial support for the new development paradigm. With the integration of next-generation information technologies such as cloud computing, big data, the Internet of Things, and mobile internet with traditional manufacturing... Rapid integration and the construction of a secure and reliable digital supply chain are crucial for enhancing the overall competitiveness of enterprises and improving the stability and security of my country's industrial and supply chains. Level is crucial. In a digital environment, the internal and external environments faced by supply chains are more complex and comprehensive, posing greater challenges for enterprises in conducting supply chain security management. The supply chain network suffers from uneven capabilities among nodes, weak business resilience, high complexity in full-chain traceability, vulnerability to core data leakage, and risks associated with capital operations. Addressing issues such as amplification necessitates the urgent research and development of a set of principles and methods for digital supply chain security management to safeguard corporate interests and maintain supply chain stability. Establish operations and improve supply chain security. This

document clarifies relevant requirements regarding digital supply chain security management, assessment management, and risk handling, effectively guiding enterprises to conduct digital supply chain management. Digital supply chain security management comprehensively enhances supply chain security from aspects such as supply chain system, business, technology, data, and finance, helping enterprises... This will help to build a secure and controllable digital supply chain system, and also provide a platform for relevant research institutions to conduct research on the security management of digital supply chains. For reference only. General security requirements for digital supply chains

1 Scope

GB/T 46885-2025 is the Chinese national standard covering the security of a supply chain that runs on shared data - the identity and access between companies, the integrity of the data exchanged, the resilience when a partner's system is compromised and the obligations each party carries for the others. First edition, with the traceability and procurement standards GB/T 46881-2025 and GB/T 46888-2025. It was issued on 31 December 2025 and has been in force since 1 April 2026, as a first edition. The document is under the responsibility of the Ministry of Industry and Information Technology. This page is published from the official record of the 2025 edition; the clause text of a standard this recent is not yet in circulation, and the figures, limits and tables it contains are those of the document itself, delivered in full with the English translation.

This document establishes the basic principles of digital supply chain security management and stipulates the requirements for digital supply chain security management, digital supply... Chain security assessment requirements and security risk handling requirements. This document is applicable to enterprises conducting security management, security assessment, and risk mitigation in their digital supply chains, and provides a framework for implementing digital supply chain management. This provides a reference for research institutes, third-party service providers, and others engaged in research, consulting services, and solution development.

2 Normative references

The contents of the following documents, through normative references within the text, constitute essential provisions of this document. Dated citations are not included. For references to documents, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies. This document.

GB/T 37939 Information Security Technology - Network Storage Security Technical Requirements

GB/T 41479 Information Security Technology - Security Requirements for Network Data

Processing

GB/T 45403-2025 Digital Supply Chain Maturity Model

GB/T 46881-2025 General Requirements for Digital Supply Chain Traceability Systems

GB/T 46887-2025 Digital Supply Chain Architecture

3 Terms and Definitions

The terms and definitions defined in GB/T 46887-2025, GB/T 45403-2025, and GB/T 46881-2025, as well as the following terms and definitions, apply. This document.

3.1 Digital Supply Chain In a digital environment, a customer-centric, value-creation-oriented, data-driven, and platform-based approach is needed to achieve supply chain efficiency. The supply chain partners, including suppliers, manufacturers, service providers, distributors, and customers (consumers), are connected across multiple lines, enabling efficient collaboration of data, materials, and funds. A new form of supply chain with flexible configuration. [Source: GB/T 45403-2025, 3.1]

3.2 Supply chain safety Throughout the entire supply chain operation, a series of strategies and measures are adopted to ensure the security of the flow of products, services, information, and funds. Ensuring the safety, reliability, and integrity of the supply chain to prevent disruptions, damage, or failures due to various risks, and maintaining the normal operation and internal and external stability of the supply chain. The ability to stabilize and sustain development.

3.3 critical materials The term refers to materials, raw materials, semi-finished products, outsourced parts, purchased parts, and packaging materials that have a significant impact on the entire product lifecycle. [Source: GB/T 39259-2020, 3.1, with modifications]