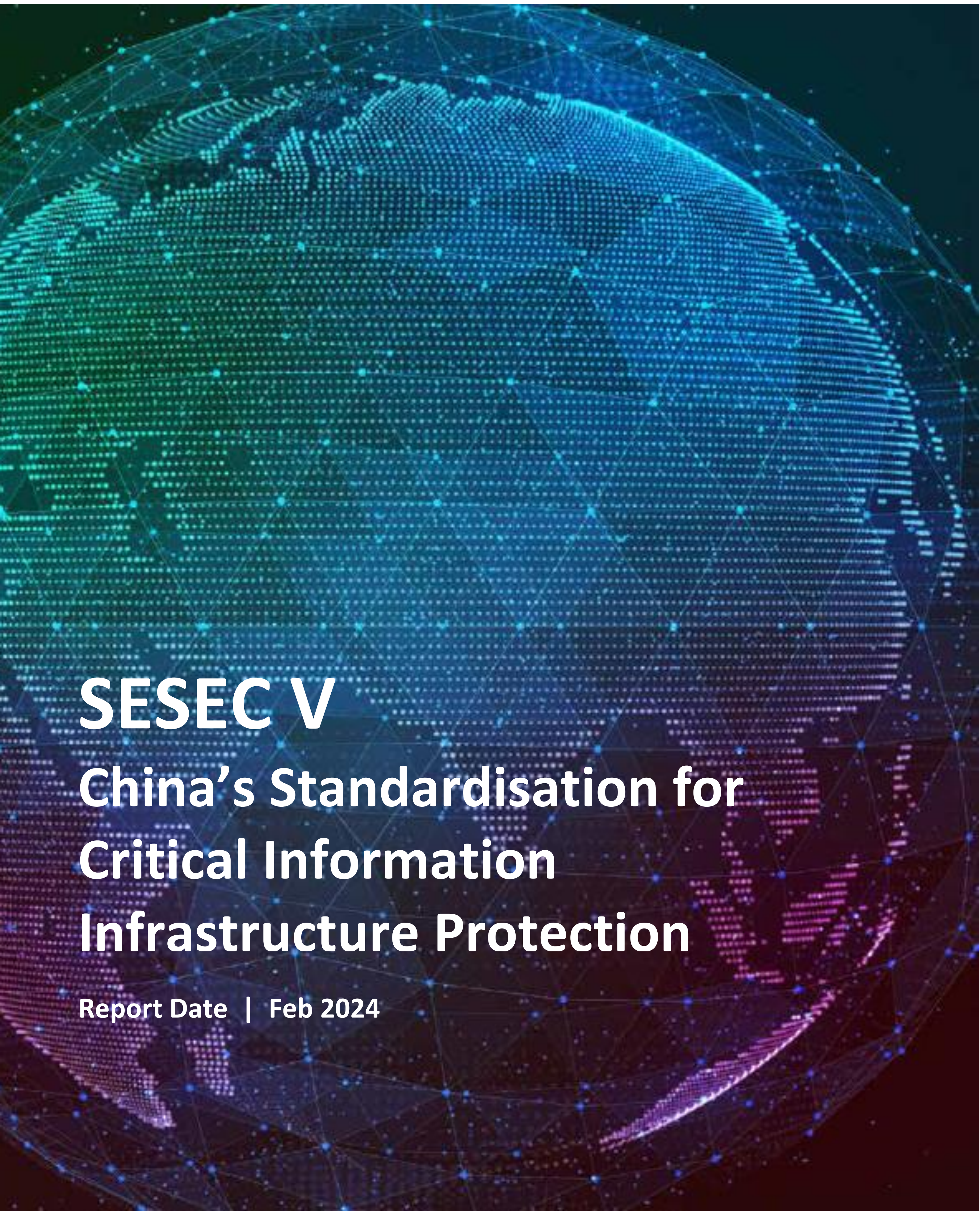


SESEC V

China's Standardisation for Critical Information Infrastructure Protection

Report Date | Feb 2024

Seconded European Standardisation Expert in China
(SESEC)

China's Standardisation Development for Critical Information Infrastructure Protection

1. Background

1.1 China has established a protection system for critical information infrastructure.

The *National Cyberspace Strategy*, which was released in 2016, proposed to "establish and implement a protection system for critical information infrastructure (CII)."

The *Cybersecurity Law*, introduced in the same year, requires that "key protection measures shall be implemented based on the network security graded protection system, for important industries and sectors such as public communication and information services, energy, transportation, water conservancy, finance, public services, electronic government affairs, and other critical information infrastructure that, once damaged, experiences loss of functionality or data leakage, may seriously endanger national security, national economy, people's livelihood, and public interests." It also specifies that "key network equipment and special products for network security must undergo security certification or pass security testing by qualified institutions, following the mandatory requirements of relevant national standards, before they can be sold or provided."

In September 2021, China reiterated and supplemented the scope of critical information infrastructure in the *Regulations on Security Protection of Critical Information Infrastructure*. According to the document, CII includes "important industries and sectors such as public communication and information services, energy, transportation, water conservancy, finance, public services, electronic government affairs, national defence technology industry, and other significant network facilities and information systems that, once damaged, experience loss of functionality or data leakage, may seriously endanger national security, national economy, people's livelihood, and public interests." CII operators are those who operate or manage the Critical Information Infrastructure in China. The document also specifies the responsibilities and obligations of competent authorities and CII operators, as well as the technical and administrative requirements to ensure the security of CII. The document indicates that "the state should formulate and improve security standards for CIIs to guide and regulate the work of protecting the security of such infrastructure."

Since the publication of the above laws and regulations, China has established a protection system for critical information infrastructure until 2023.

1.2 Regulatory requirements of other cybersecurity regulations for CII

In context of national security, the *Cryptography Law of the People's Republic of China*, which was enforced in 2019, stipulates that CII operators must undergo a national security review organized by the Cyberspace Administration of China in conjunction with the State Cryptography Administration and other competent departments, when purchasing network products and services involving commercial cryptography that may affect national security. The *Cybersecurity Review Measures* released in 2021 require that CII operators, when procuring network products and services, and network platform operators engaged in data processing activities that may affect or potentially affect national security, must undergo a cybersecurity review according to the specified measures. Those requirements above impacted the business of the overseas' manufacturers or providers for network products and services, or those involving commercial cryptography, as they are not sure if their products or services can be accepted by such national security review.

In context of data exports, the *Personal Information Protection Law* released in 2021 states that CII operators as well as data processors handling personal information to certain quantities specified by the Cyberspace Administration of China, should store personal information collected and generated within the territory of the People's Republic of China. If it is needed to provide information overseas, a prior security assessment organized by the Cyberspace Administration of China should be conducted. In cases where laws, administrative regulations, or provisions of the Cyberspace Administration of China stipulate that a security assessment is not required, other respective provisions should be fulfilled. Furthermore, the *Data Security Law* released in 2021 requires that the security management of important outbound data collected and generated by CII operators within the People's Republic of China are subject to the provisions of the *Cybersecurity Law*. Finally, the *Measures for Security Assessment of Outbound Data Transfers* released in 2022 stipulate that CII operators as well as data processors handling personal information of over one million people, should apply for data export security assessments to the Cyberspace Administration of China when providing personal information overseas.

In this context, the National Information Security Standardisation Technical Committee (TC260)[1] conducted research on the standards system for CII security and initiated a series of standards projects to support the implementation of the laws and regulations mentioned above.

2. The development of Standardization

2.1 Identification of CII

The 2021 *Regulations on Security Protection of Critical Information Infrastructure* state that "the administrative authorities and supervisory departments in important industries and sectors (such as public communication and information services, energy, transportation, water conservancy, finance, public services, electronic government affairs, national defense technology industry, etc.) are responsible for the security protection of CIIs in their respective fields." Specifically, they are required to "formulate rules for the identification of CIIs based on the conditions of their respective industries and sectors."

In practice, after a CII is identified by the relevant administrative authority, the operating organization for this CII will be notified by the authority, and they will be called as CII operator. Then the CII operator further analyses its critical businesses, to identify the essential network facilities and information systems necessary for continuous and stable operations. This analysis forms the basis for conducting protection, review, emergency response, and other tasks. The ***Information Security Technology—Method of boundary identification for critical information infrastructure (Draft for Comments)*** provides a method for determining the boundaries of CIIs based on information flow. It serves as a reference for CII operators in the process.

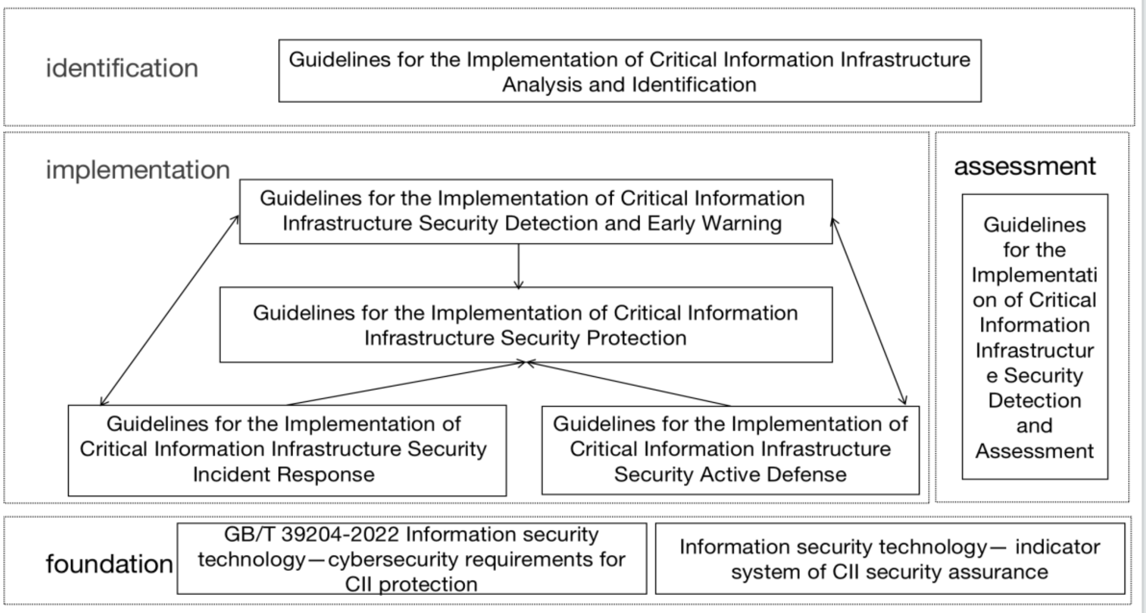
2.2 Core standards

The core of the CII standards system in China consists of eight national standards, specifically:

1. ***GB/T 39204-2022 Information security technology — Cybersecurity requirements for CII protection*.**
2. ***Information security technology — Indicator system of CII security assurance*.**
3. ***Guidelines for the Implementation of Critical Information Infrastructure Analysis and Identification*.**
4. ***Guidelines for the Implementation of Critical Information Infrastructure Security Protection*.**
5. ***Guidelines for the Implementation of Critical Information Infrastructure Security Detection and Early Warning*.**
6. ***Guidelines for the Implementation of Critical Information Infrastructure Security Incident Response*.**
7. ***Guidelines for the Implementation of Critical Information Infrastructure Security Active Defense*.**
8. ***Guidelines for the Implementation of Critical Information Infrastructure Security Detection and Assessment***.

The relationship of these eight standards is illustrated in the following diagram:

[1] According to the *Several Opinions on Strengthening National Standardisation of Cybersecurity*, issued in August 2016: "Under the leadership of the Standardisation Administration of China and the overall coordination of the Cyberspace Administration of China, and with the support of relevant cybersecurity regulatory authorities, the National Information Security Standardisation Technical Committee is responsible for the unified management of of cybersecurity national standards. They organize the application of new cybersecurity standard projects, the review in their development processes, and the submission for approval of cybersecurity standard drafts"


identification
Guidelines for the Implementation of Critical Information Infrastructure Analysis and Identification
implementation
Guidelines for the Implementation of Critical Information Infrastructure Security Detection and Early Warning
Guidelines for the Implementation of Critical Information Infrastructure Security Protection
Guidelines for the Implementation of Critical Information Infrastructure Security Incident Response
Guidelines for the Implementation of Critical Information Infrastructure Security Active Defense
assessment
Guidelines for the Implementation of Critical Information Infrastructure Security Detection and Assessment
foundation
GB/T 39204-2022 Information security technology—cybersecurity requirements for CII protection
Information security technology— indicator system of CII security assurance

Among the eight standards, China has completed and begun the implementation of the first standard, which is the foundational standard of the entire system: ***GB/T 39204-2022 Information security technology — Cybersecurity requirements for CII protection.*** The standard outlines three fundamental principles for CII security and provides a framework for CII security protection. Specifically:

- Three fundamental principles: i) Implement comprehensive prevention and control, with critical business as the core; ii) Adopt dynamic protection oriented by risk management; and iii) Establish collaborative defense based on information sharing.
- Protection framework: Centered on the critical business carried by a CII, its protection should be conducted in six aspects: analysis and identification, security protection, detection and evaluation, monitoring and early warning, active defense, and incident response. On one hand, this framework introduces the concept of active defense, which involves taking proactive measures – such as exposure reduction, discovery and blocking, attack-defense exercises, and threat intelligence – to enhance the capabilities for identifying, analyzing, and responding to network threats and attacks. On the other hand, the framework focuses on risk management and builds up a comprehensive system for risk identification, analysis, evaluation, and prevention.

Additionally, to achieve core targets such as stable and continuous operation of critical business, prevention of data leakage and tampering, and ensuring supply chain security, GB/T 39204-2022 describes the requirements for establishing a dedicated security management organization, appointing a chief information security officer, conducting supply chain security management, and implementing data security protection. It also addresses the flow of information among different network security protection systems, business systems, regional systems, and systems of different operators by outlining boundary protection requirements. The standard puts forward "one main, dual backup" protection, which involves multiple telecommunications operators and routes for communication lines. Furthermore, responding to the need for CIIs to respond to abnormal situations, the standard introduces the requirements promptly and efficiently for asset automation management, situation awareness, information sharing, and measures like attack detection and prevention.

Building on the fundamental principles and framework outlined by GB/T 39204-2022, the other standards will provide implementation methods from six aspects: analysis and identification, safety protection, detection and assessment, monitoring and early warning, active defence, and incident response. The capability indicator system standard will provide support for these methods.

2.2.1 Other standards

The entire business chain of CIIs should be protected, which may involve single or multiple information systems and even complex internet systems covering different organizations, regions, levels, and systems. Currently, TC260 is advancing the development and publication of relevant standards based on GB/T 39204-2022, covering aspects such as supply chain security, data security, information sharing and situation awareness.

- Supply chain security. The ***Information security technology—Security requirements for software supply chain (draft for approval)*** addresses security issues such as software vulnerabilities, backdoors, and supply chain hijacking in the software supply chain. It outlines requirements for both suppliers and consumers regarding the management of security risks in the software supply chain. Furthermore, the ***Information security technology—Evaluation method for open-source code security of software products (draft for comments)*** focuses on the open-source code in software products. It covers aspects such as intellectual property risks and sustainability risks, providing an evaluation framework and methodology for assessing the source, quality, intellectual property, and management capabilities of open-source code.

- Data security. Currently, a number of standards are being developed, such as ***Information security technology—Requirements for classification and grading of network data (draft for approval***), ***Information security technology—Risk assessment method for data security (draft for comments), Information security technology—Important data processing security requirements (draft for comments)*** and ***Information security technology—Certification requirements for cross-border transmission of personal information (draft for comments)***. These standards can be applied to address typical data security issues in CIIs, including data classification and grading, data security risk assessment, protection of important data, and cross-border transmission of data; they can also be applied to regulate the implementation of related data protection tasks.

- Information sharing, situational awareness, monitoring, and warning. Several standards provide guidance for operators in assessing the security protection situation of CIIs. Some examples are ***GB/Z 42885-2023 Information security technology—Guidance for cyber security information sharing***, ***Information security technology—Guidelines for cyber security information submission (draft for approval)***, ***GB/T 42453-2023 Information security technology—General technical requirements for network security situation awareness***, ***GB/T 42583-2023 Information security technology—Technical specifications for government network security monitoring platform***.

In addition to above standards and standard projects, TC260 has formulated or is formulating a series of standards to ensure the security of CIIs from the perspectives of cybersecurity service organizations, cybersecurity practitioners, infrastructure resilience, network attack statistics, and the application of new technologies. These standards include

- ***GB/T 32914-2023 Information security technology—Capability requirements of cybersecurity service,***
- ***GB/T 42461-2023 Information security technology—Guidelines for cyber security service cost measurement,***
- ***GB/T 42446-2023 Information security technology—Basic requirements for competence of cybersecurity workforce***,
- ***Information security technology—Cyber-resilience evaluation criteria (draft for comments),***
- ***Information security technology—Criteria for determinations of network attack and network attack incident (draft for comments),***
- ***Information security technology—Zero trust reference architecture (draft for approval), Information security technology—Artificial intelligence computing platform security framework (draft for comments),***
- etc.

3. Conclusions

It is evident that China is rapidly improving its CII standards to provide support for various relevant laws and regulations. However, due to the extensive business chains of CIIs, a lot of work is still needed before a comprehensive level of protection can be effectively achieved. The CII standard system in China is far from being fully developed. Additionally, it is noteworthy that some Foreign Invested Enterprises (FIE) still play a role in the supply chain of Chinese CIIs. The introduction of numerous CII standards will undoubtedly pose challenges to the operations of these FIEs in China.

Introduction of SESEC Project

The Seconded European Standardisation Expert in China (SESEC) is a visibility project co-financed by the European Commission (EC), the European Free Trade Association (EFTA) secretariat and the three European Standardisation Organizations (CEN, CENELEC and ETSI). Since 2006, there has been four SESEC projects in China, SESEC I (2006-2009). SESEC II (2009- 2012), SESEC III (2014-2017), SESEC IV (2018- 2022) and SESEC V (2022-2025). Dr. Betty XU is nominated as the SESEC expert and will spend the next 36 months on promoting EU-China standardisation information exchange and EU-China standardisation cooperation.

The SESEC project supports the strategic objectives of the European Union, EFTA and the European Standardisation Organizations (ESOs). The purpose of SESEC project is to:

- Promote European and international standards in China;
- Improve contacts with different levels of the Chinese administration, industry and standardisation bodies;
- Improve the visibility and understanding of the European Standardisation System (ESS) in China;
- Gather regulatory and standardisation intelligence.

The following areas have been identified as sectorial project priorities by the SESEC project partners: Internet of Things (IoT) & Machine-to-Machine(M2M) communication, communication networks & services, cybersecurity & digital identity, Smart Cities (including transport, power grids & metering), electrical & electronic products, general product safety, medical devices, cosmetics, energy management & environmental protection (including eco-design & labeling, as well as environmental performance of buildings).

Abbreviations

SAMR	State Administration for Market Regulation	国家市场监管总局
CAS	China Association	中国标准化协会
CCC	China Compulsory Certification	中国强制认证
CCSA	China Communication Standardization Association	中国通信标准化协会
CEC	China Electricity Council	中国电力企业联合会
CEEIA	China Electrical Equipment Industrial Association	中国电器工业协会
CELC	China Energy Labeling Center	中国能效标识中心
CESI	China Electronic Standardization Institute	中国电子标准化研究所
CMDSA	Center for Medical Device Standardization Administration	医疗器械标准管理中心
CNCA	Certification and Accreditation Administration of China	中国国家认证认可监督 管理委员会
CNIS	China National Institute of Standardization	中国国家标准化研究院
CNREC	China National Renewable Energy Center	中国国家可再生能源中 心
EPPEI	Electric Power Planning and Engineering Institute	电力规划设计总院
IEC	International Electrotechnical Commission	国际电工委员会
ITEI	Instrumentation Technology and Economy Institute	机械工业仪器仪表综合技术与经济研究所
MEE	Ministry of Ecology and Environment	中国生态环境部
MIIT	Ministry of Industry and Information Technology of People's Republic of China	中国工业和信息化部
MoH	Ministry of Health	卫生部
MoHURD	Ministry of Housing and Urban-Rural Development	住房与建设部
MOT	Ministry of Transport	中国交通运输部
MOST	Ministry of Science and Technology	中国科学技术部
NDRC	National development and reform commission People's Republic of China	中国国家发改委
NIFDC	National Institute of Food and Drug Control	中国食品药品检定研究 院
SAC	Standardization Administration of China	国家标准化管理委员
SGCC	State Grid Corporation of China	国家电网
TC	Technical Committee for Standard Development	标准化技术委员会