SESEC V

Report on TC260 Second Standards Week

Report Date | September 2025

Seconded European Standardisation Expert in China
(SESEC)

Report on TC260 Second Standards Week

September 2025

1. Introduction

From September 14 to 18, 2025, SAC/TC260 Second Standards Week of 2025 was held in Kunming, Yunnan province, showcasing key developments in China's cybersecurity standardization landscape. As the core national body for cybersecurity standards, TC260's activities provide critical supports to China's governance policies and technological direction. The five-day event featured **a plenary session, 7 specialized working group meetings, and a symposium on cybersecurity standards and industrial promotion**, addressing crucial areas including cryptography, data security, communications networks, and AI security.

Organized by TC260 and co-hosted by the China Academy of Cyberspace Studies, China Electronics Standardization Institute (CESI), and the Kunming Cyberspace Affairs Commission, it was attended by over 30 international registered experts from ISO/IEC JTC 1/SC 27 and SC 44, representing countries including Germany, the United States, the United Kingdom, and France, alongside more than 900 Chinese participants from TC260 committees, working groups, member organizations, and enterprises.

During the Plenary Session, Yang Xudong, Secretary-General of TC260 and President of CESI delivered a presentation "**Innovative Practices and Reflections on China's Cybersecurity Standardization**", outlining the committee's institutional mandate, its comprehensive "big cybersecurity" standard system, and its strategic advancements in key domains such as data security and AI.

2. TC260: Institutional Framework and Outputs

2.1 Governance Structure and Working Methods

TC260 (National Technical Committee 260 on Cybersecurity of Standardization Administration of China) serves as China's primary national standardization body for cybersecurity. Originally established in 2002 as the Information Security Standardization Technical Committee, it was renamed in 2024. The committee operates under the administration of the National Standardization Administration (SAC) with coordination from the Cyberspace Administration of China (CAC).

The committee maintains a mirror committee relationship with ISO/IEC JTC 1/SC 27 (Information security, cybersecurity, and privacy protection). Its organizational structure includes a Secretary Office (namely the CESI) as the permanent body responsible for routine works and nine specialized working groups responsible for development of standards. They are:

- WG1: Cybersecurity System and Coordination Working Group
- WG2: Confidentiality Standards Working Group
- WG3: Cryptographic Technology Standards Working Group
- WG4: Identification and Authorization Standards Working Group
- WG5: Cybersecurity Evaluation Standards Working Group
- WG6: Communication Security Standards Working Group
- WG7: Cybersecurity Management Standards Working Group
- WG8: Data Security Standards Working Group
- SWG-ETS: Special Working Group on Emerging Technology Standards Working Group

TC260 describes its working methods as emphasizing openness and broad participation. All national standards are made freely available online, with mandatory 60-day public comment periods for draft standards. The committee holds working group meetings twice annually for open discussion. Membership includes 112 committee members,

with five representatives for foreign-funded enterprises including **Intel, IBM, Amazon, Siemens, and Schneider.** Working group participation extends to over 800 member organizations, including approximately 50 foreign enterprises such as Philips and Infineon.

2.2 Standardization Outputs and Focus Areas

TC260 has developed what it characterizes as a comprehensive "big cybersecurity" national standard system. **By September 2025, the committee had published 405 national standards with 121 additional standards under development.** These standards cover multiple technical domains including cryptography, authentication and authorization, security evaluation, communication security, and data security. The standard system provides technical support for implementing national laws and regulations including the Cybersecurity Law, Cryptography Law, Data Security Law, and Personal Information Protection Law.

In emerging technology domains, TC260 has established initial standard frameworks for data security and personal information protection, having published 42 national standards in these areas. Significant progress has been made in AI security, including the development of an **AI Security Governance Framework** published in both Chinese and English. Six national AI security standards have been published covering areas such as machine learning algorithm security assessment, AI-generated content labeling, and generative AI security. Additional projects including standards for AI application security classification and AI security capability maturity assessment are currently under development.

Regarding international standardization, China has participated as a P-member of ISO/IEC JTC1/SC27 since 2004. More than 200 Chinese experts have contributed to international standardization work, with over 30 proposals accepted in areas including SM2/SM3/SM9/ZUC cryptographic algorithms, incident coordinated response, and quantum key distribution. TC260 has also adopted more than 60 international standards, representing over 15% of its published national standards, covering domains such as public key infrastructure PKI, information security management, security evaluation, and intrusion detection.

According to Yang, TC260's future work is expected to focus on several strategic priorities: enhancing the quality and practical implementation of cybersecurity standards, addressing the security requirements arising from digital and intelligent technologies, and strengthening international exchange and cooperation in standardization.

3. Key Meeting Proceedings

This section provides an overview of the TC260 meetings, covering both the broad strategic exchanges of the Plenary Session and the specific technical progress reported by the working groups.

3.1 Plenary Session

- **International Context**: Speeches from leaders of ISO/IEC JTC 1 SC 27 and SC 44 on global trends in privacy, AI security, and information security management system (ISMS).
- **Domestic Priorities**: Presentations on China's *New Generation Commercial Cryptography Algorithm* development and *Innovative Practices and Reflections on China's Cybersecurity Standardization*.
- **Global Engagement**: International roundtables on standardizing *AI Security* and *Data Security & Privacy Protection*.

3.2. Working Group Deliberations

The core technical work advanced across multiple fronts, with critical developments in the following areas:

- **Cryptography (WG3)**: The group reviewed **2 draft standards** and **6 standards for comments** and promoted **3 newly published standards**. and conducted research on the Cryptographic Standards Usage Guideline and Cryptographic Standards Framework. Work progressed on several standards such as *Cryptographic*

module security requirements (Draft) and *SM2/SM9 algorithm encryption signature message format* (Call for Comments).

- **Cybersecurity Evaluation (WG5)**: The meeting advanced **4 newly initiated standards**, **4 ongoing development/revision projects**, and reviewed **12 standards for comments**. Several standards align with global regulatory concerns, including *Security requirements for consumer smart connected devices* (Draft), *Cybersecurity protection capability maturity model of industrial control systems* (Call for Comments), and *Guidelines for categorization and classification of cybersecurity vulnerability* (Draft).
- **Communication Security (WG6)**: The session reviewed **1 draft standard** and **3 standards for comments** and discussed **2 research reports**. Work on future network architectures included *Satellite internet cybersecurity framework* (Draft), *6G endogenous and boundary security technology and standardization research* (Research Report), and *IoT security reference model and general requirements* (Call for Comments).

Data Security (WG8): The group deliberated on **8 standard development/revision projects** and **2 research projects**. Work on operationalizing data governance includes *Code of conduct for automated network data collection tools* (Under development) and *Personal information protection guideline for small processors* (Under development).

4. On-Site Analysis: Standardization Challenges

Based on observations of WG5 (Cybersecurity Evaluation), WG6 (Communication Security), and WG8 (Data Security) working group meetings, this chapter analyzes internal considerations and implementation challenges encountered during China's cybersecurity and data security standardization process through a detailed examination of specific standard discussions.

4.1 Scope Definition for 6G Security Standardization (Case 1)

In frontier technology domains, standardization work faces the challenge of balancing forward-looking vision with practical feasibility. During discussions of WG6 on the project "**6G endogenous and boundary security technologies and standardization research"**, participating experts offered suggestions regarding the research framework. Considering that core 6G technical parameters and architecture remain in early research stages, experts suggested caution in focusing standardization work on specific technical pathways such as "endogenous security" and "boundary security." Recommendations were made to adjust the research scope toward broader 6G cybersecurity standardization studies, emphasizing achievable standardization outcomes in the near future and focusing on framework development rather than premature definition of specific technical details. These discussions reflect the strategic choices facing standards development organizations when standardizing during early technology development phases, demonstrating the need to balance technical foresight with practical standardization feasibility.

4.2 Technical Alignment in Embedded System Security Standards (Case 2)

In more mature technical fields, standards development requires balancing security requirements with practical needs across different industry application scenarios. During technical discussions of WG5 on the recommended standard (call for comment) "***Cybersecurity technology — Security technical specification for embedded operating system***", a representative from Siemens (China) Co., Ltd. raised substantive concerns regarding the standard's technical applicability. The discussion revealed this recommended national standard establishes security requirements for embedded devices that exceed levels stipulated in the mandatory national standard ***GB40050 Critical network devices security common requirements***. While the standard's documentation includes implementation examples covering a wide spectrum of equipment, from PLCs to lower-performance data collection devices, its architectural requirements have raised concerns regarding their technical feasibility for resource-constrained devices. It has been noted that these requirements, in some aspects, exceed the levels mandated for certain types of specialized equipment, potentially establishing criteria that lower-performance devices may struggle to meet. The Siemens representative suggested this approach could create technical implementation challenges for lower-performance devices and recommended reassessing relevant technical requirements. In response, the standards drafting group acknowledged GB40050's role as a foundational security baseline but maintained that recommended standards should aim for more comprehensive security. Critically, they invited the Siemens

representative to specify the exact clauses posing challenges, committing to conduct targeted research on those specific technical indicators. This case demonstrates ongoing efforts to balance security objectives with industrial applicability, while highlighting the dynamic interaction between international industry stakeholders and Chinese standards development bodies.

4.3 Defining Applicability and Responsibility in Data Governance Standards (Case 3)

The WG8 working group is developing a suite of eight standards to operationalize China's data governance policies into practical technical specifications. Discussions revealed a strategic focus on creating a multi-layered governance system that addresses the diverse needs of different organizational scales and complex data processing scenarios.

Two standards drew significant attention for their novel approach. The ***Personal information protection guideline for small processors*** aims to lower compliance burdens for SMEs by simplifying requirements, embodying a risk-based and proportional approach. However, experts debated the practical definition of a "small processor" and corresponding risk levels, highlighting the challenge of balancing flexibility with clarity. The ***Security guidelines for data provision, entrusted processing, and joint processing*** seeks to clarify security responsibilities in complex, multi-party data activities. While welcomed for bringing structure, its definitions and operational measures were seen as needing more precision to be fully actionable. A key insight from the discussions is China's endeavour to move from broad legal principles to implementable rules. The ongoing challenge lies in crafting standards that are sufficiently detailed to ensure meaningful compliance, yet flexible enough to adapt to varied real-world contexts.

From these discussions, it becomes evident that China's cybersecurity and data security standardization work faces implementation challenges across domains of varying technical maturity. In cutting-edge technology areas, there is a need to balance the relationship between early standardization and technical uncertainty. In mature technical fields, coordination between standard requirements and industrial practicalities must be addressed. In the critical domain of data security, a central challenge lies in translating legal principles into actionable standards, which requires solving nuanced issues of applicability and responsibility allocation. These discussions and adjustment processes reflect how China's standardization system is evolving toward greater emphasis on practical application effectiveness, with professional discussions and feedback-based adjustment mechanisms during standards development continuously improving.

5. Core Insights

Building upon the specific challenges observed in the previous section and the TC260 working group proceedings, this segment identifies four principal strategic orientations in China's cybersecurity and data security standardization development: establishing comprehensive indigenous technological capabilities, implementing early-stage standardization for emerging technologies, building an agile governance system for data factor marketization**,** and fostering industry ecosystem integration to support effective implementation and competitiveness enhancement.

5.1. Strategic Pillar I: Building Indigenous Technological Capabilities

China is leveraging standardization to methodically reduce external dependencies in critical digital technology areas, building a self-reliant and controllable technological system.

Cryptography serves as the foundational cornerstone of China's cybersecurity standardization efforts. The work of WG3 extends far beyond algorithms, focusing on building a comprehensive cryptographic application ecosystem. By developing and revising standards for modules, device interfaces, and application identifiers, complemented by design guides and management systems, the objective is to deeply and mandatorily embed commercial cryptography into all information systems. This is not only about security but also about establishing a foundation of technological trust in the digital sphere, probably creating significant compliance barriers for ICT products entering China's critical sectors.

Parallel to this, China is advancing its security framework and developing independent assessment protocols for the ICT supply chain. This direction is reflected in WG5's standardization work on foundational technologies such as integrated circuit chips, BIOS, and operating systems. Together, these initiatives indicate a focus on addressing supply chain dependencies and risks. Through the establishment of proprietary assessment criteria and maturity models—such as those for Industrial Control Systems—China is building capacity to define and evaluate the security of critical products and systems according to its own technical standards.

5.2. Strategic Pillar II: Early-Standardization in Frontier Technologies

China's approach to cybersecurity standardization demonstrates a distinct pattern of developing security frameworks during early research and development phases across emerging technological fields. This methodology represents a notable shift toward aligning standardization timelines with technological innovation cycles.

WG6 has initiated cybersecurity standardization research for 6G networks while international standards remain in early development stages. This approach enables the early integration of security considerations during formative technology development phases. Similar standardization patterns are emerging in satellite internet security frameworks, where cybersecurity specifications are being developed concurrently with underlying technology architectures. This synchronization of standardization with technology development allows for the incorporation of security requirements at fundamental levels of technology design.

This methodology extends beyond communication technologies to encompass other strategic sectors. In fields such as intelligent driving, WG5 is conducting cybersecurity standardization research in parallel with technological advancement. This parallel development of technical specifications and security frameworks embeds protective measures during formative industry phases, establishing structured environments for technological maturation while facilitating early compliance with standardized security protocols.

5.3 Strategic Pillar III: Building an Agile Governance System for Data Factor Marketization

China's data security standardization is shifting toward establishing an agile governance framework capable of supporting the market-oriented allocation of data as a factor of production. This framework moves away from static, uniform, and rigid rules, instead striving to develop a "layered, categorized, and dynamically adaptive" governance capacity to address the inherent complexity and uncertainties of the digital economy. Its strategic focus is crystallized in three paradigm shifts: transitioning from building defensive perimeters to embedding security within operational workflows, from applying uniform obligations to all entities to implementing risk-proportionate accountability tiers, and from establishing rigid compliance rules to fostering a collaborative governance ecosystem. Collectively, these transitions mark the emergence of a characteristic in China’s data security governance—where the objective extends beyond risk prevention to include activating the value of data through a credible, controllable, and predictable regulatory environment, thereby laying an institutional foundation for sustainable growth of the digital economy.

5.4. Strategic Pillar Ⅳ: Fostering Industry-Standard Synergy

China's standardization system demonstrates a coordinated approach, where standard development progresses alongside industrial implementation. This integrated model creates a mutually reinforcing dynamic between technical specifications and market applications.

The Data Security Standards Enhancement Program (DSEP) illustrates this approach through its publication of exemplary implementation cases in the symposium on cybersecurity standards and industrial promotion. By showcasing successful adoption examples, TC260 encourages broader industry engagement with national standards, accelerating the transition from technical specifications to operational practice while supporting industrial security and development.

Concurrently, China's standardization engagement shows increasing orientation toward international standardization processes. The keynote speech on *Innovative Practice of Cybersecurity Standardization in China* and the following

international standardization roundtable discussions on AI security and data security clearly indicated China's aim to transform its domestically validated standardization practices into international norms. By contributing its "Chinese solutions" to international standards organizations, the country seeks to support the global expansion of its digital technologies and products.

6. Conclusions

6.1 Current State of Standardization Development

China's cybersecurity and data security standardization work has established a systematic development pathway. In foundational technology areas, complete ecosystem frameworks are being built through cryptographic technologies and other core standards. In emerging technology domains, early-stage standardization strategies demonstrate forward-looking planning. Concurrently, in cross-cutting areas such as data security governance, standardization efforts are increasingly focused on translating broad legal principles into actionable and technically specific rules. The standardization process shows a clear transition from technology following to active rule-making, while the professional discussions and feedback mechanisms within working groups reflect the continuous improvement of the standards system.

6.2 Observations on Implementation Characteristics

The standards development process demonstrates a dual characteristic of balancing technological innovation with industrial practicality. On one hand, early-stage planning awareness is evident in cutting-edge fields like 6G and satellite internet; on the other hand, continuous optimization is still needed for the alignment between standard requirements and industrial applicability in mature fields like embedded systems, as well as for ensuring clarity and operationalizability in governance-heavy domains like data security. Working group discussions indicate that the standards system is evolving toward greater emphasis on practical application effectiveness, with increasing consideration for industrial practical capabilities while maintaining technological advancement.

6.3 Future Development Trends

The continued development of China's cybersecurity and data security standards will significantly drive the evolution of the technical regulatory environment. It is recommended that relevant parties establish dynamic standards tracking mechanisms to stay informed about technical requirement changes; enhance technical research reserves to improve standards adaptability; and pay particular attention to the challenges of applicability and responsibility allocation in fast-evolving areas such as data governance.

China's cybersecurity and data security standards system remains in a phase of continuous improvement and iterative refinement. Its implementation effects and future development direction warrant ongoing attention. Through systematic standards tracking and sustained professional technical exchanges, stakeholders will be better positioned to understand and effectively respond to the evolving standardization landscape.

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).