SESEC VI

SAC/TC260 First Standards Week of 2026

Report Date | April 2026

Seconded European Standardisation Expert in China
(SESEC)

TC260 First Standards Week of 2026: AI Safety Takes Center Stage

April 2026

From 31 March to 3 April, the National Standardization Technical Committee on Cybersecurity (SAC/TC260) held its first "Standards Week" of 2026 in Zhuhai, Guangdong province. The event comprised **one plenary session, nine working group meetings, and six thematic technical exchanges**.

Nine working groups	Six thematic technical exchanges
WG3 (Cryptography) WG4 (Authentication & Authorization) WG5 (Cybersecurity Assessment) WG6 (Communication Security) WG7 (Network Security Management) WG8 (Data Security) **WG9 (AI Security)** SWG-ETS (Emerging Technologies) **SG1 (International Cybersecurity Standardization)**	Cybersecurity product interconnectivity AI security standards and applications Personal information protection: interpretation and practice Low-altitude equipment cybersecurity Closed-door RH seminar Guangdong-Hong Kong-Macau standards coordination

Based on the sessions attended by SESEC (see attached agenda), **AI security** emerged as a clear priority. Four of the eight plenary speeches addressed the topic, covering AI security mechanism design, standardization pathways, international standardization trends, and large model security practices. This focus was reinforced by the launch of WG9 on AI security and by two AI-related data security proposals introduced under WG8 (Data Security).

Two New Working Groups Established

During the Standards Week, SAC/TC260 formally established two new bodies: **Working Group 9 on AI Security (WG9) and Study Group 1 on International Cybersecurity Standardization (SG1)**.

WG9 on AI Security is tasked with surveying the current state and trends of AI security standards, proposing a standardization framework, and developing AI security standards. The group is chaired by Zhou Bowen, Director of the Shanghai Artificial Intelligence Laboratory. The working group currently has 89 member organizations, including several foreign-invested companies in China such as **Microsoft (China), Amazon Web Services Technology (Beijing), Dell (China), Siemens (China), and Fujifilm Business Innovation (China)**. The inclusion of several foreign-invested companies reflects the growing international engagement in China's AI security standardization process.

During Standards Week, WG9 held its first working group meeting, discussing the AI security standardization framework, eight new project proposals for 2026, five standards under development, and two translation projects into foreign languages. Notably, **2 mandatory standards** projects were introduced at the session (See the latter part).

SG1 on International Cybersecurity Standardization is responsible for tracking international cybersecurity standardization developments, conducting comparative analysis between domestic and international standards, and facilitating China's proposals for international standards. The study group is chaired by Lin Ning, a senior standardization expert at the China Electronics Standardization Institute (CESI).

Selected Standardization Highlights

In addition to the institutional developments, several newly proposed standards deserve attention.

Cybersecurity technology — Cybersecurity label — Part 1: Consumer connected cameras (WG5)

In November 2025, the Cyberspace Administration of China (CAC) released for public comment the draft ***China Cybersecurity Labelling Management Measures***, proposing a cybersecurity identification system for internet-connected products under a catalogue-based approach (See more details from our news coverage and the English version of the draft is available here). Consumer connected cameras have been designated as the **first product category** to implement this system.

In March 2026, the TC260 Secretariat (namely the CESI) issued for public comment the draft *Practice Guide on Cybersecurity Identification – Security Requirements for Consumer Connected Cameras*, which serves as the testing basis for the scheme. Building on this practice guide, a **proposal for a new national standard** within WG5 (Cybersecurity Assessment) was introduced during this Standards Week "*Cybersecurity technology — Cybersecurity label — Part 1: Consumer connected cameras*", to provide technical underpinning for the implementation of the cybersecurity identification system.

The draft standard is expected to establish security technical requirements for consumer connected cameras across five dimensions: physical and hardware security, system and software security, network and communication security, data security and personal information protection. It defines three progressive security levels – basic, enhanced and leading. The standard applies to the design, development, use, maintenance and testing of consumer connected cameras – defined as standalone, internet-enabled audio/video capture devices purchased by consumers for personal and household use, excluding cameras used in public security contexts.

Data security technology – Data processing security requirements for AI agents (WG8)

The proposed standard specifies full-lifecycle security requirements for data processing activities carried out by AI agents, including collection, storage, use, processing, retrieval, extraction, transmission, provision, disclosure and deletion. It applies to organizations involved in the design, development, deployment, operation and maintenance of AI agent applications.

To address the emerging risks associated with AI agent data processing, the proposed standard establishes four core security logics:

- **Runtime validation.** Real-time checks at key points such as retrieval, tool calls and long-term memory writes to ensure alignment with authorization boundaries and data minimization.
- **Zero-trust boundaries.** Whitelist-based access control and minimal context transmission to prevent exposure of full session histories or irrelevant background information.
- **Penetrating control and data tracing.** Security requirements apply equally to derived data (summarized, vectorized or tagged) as to original data. Compliance status must pass from original data to all derivative carriers and memory entries.
- **Scenario-based intervention.** High-impact scenarios involving critical infrastructure, state authorities or automated high-risk operations require enhanced controls, including mandatory human dual verification where necessary.

The proposed standard marks a shift from static governance of traditional systems to dynamic, penetrating governance of AI agent data processing.

Data security technology – Guidelines for protecting personal information of AI users (WG8)

The proposed standard specifies security guidelines for the processing of user input data and personal information when AI systems, including generative AI and AI agents, provide services to users. It covers personal information collection, model design and development, model operation, protection of data subject rights, and governance.

The proposal is aligned with international frameworks. The EU's GDPR and AI Act, the US NIST AI Risk Management Framework, and international standards such as *ISO/IEC 27701 Information security, cybersecurity and privacy protection - Privacy information management systems - Requirements and guidance* all place personal information protection at the core of AI governance. This standard will help align China's rules with global practices.

The standard establishes three core principles – minimization, dynamic control and graduated protection – and sets out requirements across five areas:

- **Collection**: Only collect data necessary for basic functions, obtain separate consent for sensitive personal information, and prohibit crawlers from collecting unauthorized or non-public data.
- **Model design**: Build in privacy safeguards and erasure mechanisms, embed explainability, and conduct regular security audits and backdoor detection.
- **Operations**: Offer a privacy mode that prevents cloud transmission, training and long-term storage, encrypt data, prevent filter bubbles, and protect minors.
- **User rights**: Provide a one-click opt-out for data training within four clicks, allow users to query and export their data, and ensure deleted data no longer appears in outputs.
- **Governance**: Establish a personal information protection management system with regular impact assessments and compliance audits.

Cybersecurity Technology - Basic Security Requirements for Anthropomorphic Interactive Services of Artificial Intelligence (WG9)

In December 2025, the CAC released a draft of the Interim Measures for Administration of Anthropomorphic AI Interactive Services. This **mandatory** standard was to be developed in parallel with the regulations to ensure alignment.

The proposed standard adopts a tiered approach (basic and enhanced levels), focusing on data security, content safety, and risk management. Key debates include difficulties in risk prevention, over-reliance on AI, insufficient classification granularity, privacy protection challenges (e.g., memory deletion controls), and child protection measures.

The Interim Measures were officially promulgated in April 2026, making the new mandatory standard inevitable. The standard will now undergo significant revisions to align with the final regulation. According to WG9 leaders, the standard is expected to be approved for publication in April 2027.

Basic Requirements for the Security of Intelligent Agent Applications (WG9)

The CAC has proposed a **mandatory** national standard on the basic security requirements for intelligent agent applications, with China Mobile leading the drafting. The standard specifies fundamental security requirements that apply throughout the entire lifecycle of intelligent agent applications—from design, R&D, and distribution to deployment and operational maintenance. Key technical provisions cover identity identification, system permission invocation, tool invocation, data collection and usage, human intervention for high-risk operations, input and output security protection, log retention and dynamic monitoring, as well as anomaly blocking and emergency shutdown.

The standard applies to intelligent agent applications deployed on terminal devices (including smartphones, tablets, computers, laptops, desktops, and wearables) or in the cloud that can invoke system or local tools to execute operations and fulfill user needs. All relevant parties—including manufacturers, developers, and operators—are required to implement effective security protections across the entire product lifecycle to ensure operational safety.

However, the mandatory nature has sparked debate: the definition of “intelligent agent” remains unclear, the technology is still immature, and some stakeholders worry that binding rules too early could hinder innovation.

Overview of TC260 Standards (as of April 2026)

As of April 2026, TC260 has published over 400 national standards on cybersecurity and data security. These cover areas ranging from fundamental cryptography and identity authentication to emerging fields such as AI security, personal information protection, data classification and grading, critical information infrastructure protection, and cloud computing security. Another 80+ standards are currently under development. A full list of TC260 standards as of April 2026 is attached to this news update for reference.

AI security took center stage throughout TC260’s first Standards Week of 2026 — from the plenary sessions to the newly launched WG9 and the proposed mandatory standards for anthropomorphic AI services and intelligent agents. With over 400 national standards already published and more than 80 under development, TC260 is rapidly building a comprehensive security framework that addresses both traditional cybersecurity challenges and emerging AI risks. As China deepens its engagement with international standardization through SG1, the rules being written today will have lasting implications for the future of AI security — both domestically and globally.

For European stakeholders, TC260’s first Standards Week signals China’s growing role as a rule-maker in AI security standardization. New mandatory standards and the cybersecurity labeling scheme will have practical implications for market access. While foreign firms like Siemens and Microsoft have already joined TC260’s AI security working group as members, European stakeholders should stay engaged through channels such as SESEC and EU-China dialogues to track these developments and manage compliance.

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).