SESEC Observation on TC260 2nd Standards Week in 2024

SESEC, December 2024

I. Introduction

China National Information Security Standardization Technical Committee (SAC/TC260) is a key standardization body in China responsible for the development and management of national standards related to cybersecurity, data security, and information protection. It operates under the leadership of the Cyberspace Administration of China (CAC), Standardization Administration of China (SAC), and the Ministry of Industry and Information Technology (MIIT). It plays a central role in shaping China’s cyber and data security regulatory and standardization landscape.

TC 260 initiated its biannual "Standards Week" events since 2017, marking a significant milestone in advancing cybersecurity and data security standardization in China. Over the years, these events have evolved into a premier platform for collaboration among Chinese stakeholders, including government agencies, industry leaders, academic institutions, and technical experts. The primary goal is to drive the development and refinement of cybersecurity and data security standards while showcasing the nation's progress in policies, standardization efforts, and technological advancements.

II. The 2nd Standards Week of TC260 in 2024

The 2nd Standards Week of TC260 in 2024 took place from December 8th to 11th, 2024, in Haikou City, drawing participation from over 900 experts representing more than 300 public and private organizations. The event provided a platform to discuss emerging technologies, future industry hotspots, and standardization projects and proposals.

The four-day event featured a diverse range of activities, including conference, forums, training session, and working group discussions, aimed at fostering collaboration and advancing cybersecurity standardization.

Agenda (More details has been attached with this report):

Day 1 (8th December):

- Plenary Session: Inauguration and keynote addresses.
- Forums: Discussions on AI, E-government, data and consumer privacy, and new industrialization.

Day 2 (9th December):

- Cybersecurity Standardization Training: Skill-building sessions focused on practical aspects of standardization.
- Working Group Meetings: Sessions for seven working groups under TC260.

Day 3 and Day 4 (10th and 11th December):

Continued Working Group Meetings to advance the development of cybersecurity standards.

Keynote Speech

The event commenced with a Plenary Session, during which Mr. Wang Jingtao, Vice-Administrator of CAC and Chairman of TC260, delivered a keynote address. His speech underscored the critical role of standards in enhancing China's cybersecurity infrastructure and emphasized the following priorities:

- Leverage standards to support the construction of a national cybersecurity defense system. Expedite the publication and implementation of standards such as methods for determining the boundaries of critical information infrastructure, metrics for security protection capabilities, formats for cybersecurity product alert information, and asset information formats, thereby accelerating the development of a systematic defense capability.

- Use standards to enhance data security governance and regulation. Accelerate the development of standards for data classification and grading protection requirements, as well as compliance auditing for personal information protection, ensuring the orderly and secure flow of data.

- Employ standards to guide the secure and orderly development of new technologies and applications such as artificial intelligence (AI). Expedite the development and release of standards such as the mandatory standard *Cybersecurity technology —Labeling method for content generated by artificial intelligence*, and strengthen research on cybersecurity standards related to intelligent connected vehicles and autonomous driving, effectively safeguarding the secure development of emerging future industries.

- Leverage standards to enhance China's international influence in cybersecurity. Continue to promote the global adoption of Chinese cybersecurity standards and make comprehensive preparations to host the ISO/IEC/JTC1 SC27 Meeting in the second half of 2025.

Experts from industry also shared their thoughts and practices on the development of cybersecurity technologies and standards in various fields like intelligent driving, post-quantum cryptography, consumer IOT, unman aerial vehicles in the plenary meeting.

In the Seminar on Artificial Intelligence Security Standards Research and Applications, Mr. Ren Kui from Zhejiang University and one of drafters of the mandatory standard *Cybersecurity technology - Labeling method for content generated by artificial intelligence* introduced the progress of the standard and cutting-edge technologies in this area. Mr. Hao Chunliang from CESI presented the application of Chinese AI security/safety standards in recent years. Experts from research institutes and enterprises shared their practices in addressing the risks brought about by the application of AI.

In the working group meetings, participants from seven working groups, namely WG3 on cryptography, WG4 on identification and authorization, WG5 on security assessment, WG6 on communication, WG7 on security management, WG8 on data, SWG-ETS on new technologies, discussed nearly a hundred ongoing standard projects and standard proposals.

III. Key Takeaways and SESEC Observations

- **AI safety and security standards are a key focus of TC260's ongoing standardization efforts.**

  Among the various activities during the event, those related to AI garnered the most attention, reflecting the increasing importance of AI standards in supporting regulatory frameworks.

  China is actively establishing a comprehensive governance regime for AI, with many ongoing standardization projects and proposals expected to play a critical role in its implementation. Several of the standards discussed at the event are directly aligned with the regulatory framework outlined in the *Interim Administrative Measures for Generative Artificial Intelligence Services.*

  In this context, TC260 is also developing a comprehensive *AI safety and security standards system*, which, once finalized, is expected to be endorsed by the government and released as an official policy document.

  Additionally, TC260 is working on China's first mandatory AI standard: *Cybersecurity Technology – Labeling Method for Content Generated by Artificial Intelligence.* This standard will have a significant impact on all generative AI services operating in China, shaping the future regulatory landscape for these technologies.

  For more detailed information about China's AI governance framework, refer to the SESEC Report, *Landscape of Artificial Intelligence Safety Standards in China.*

- **Data Security Standards with Potential Implications for European Stakeholders**

  During the WG8 meetings, several standardization projects advanced to the next development stage. These projects are expected to play a pivotal role in supporting China's personal information protection and data security legislation.

  - ➢ *Data Security Technology – Personal Information Protection Compliance Audit Requirements:* This standard aims to assist in implementing compliance audit requirements outlined in China's *Personal Information Protection Law*, the *Regulations on Network Data Security Management*, and the *Administrative Measures for Personal Information Protection Audit*.
  - ➢ *Data Security Technology – Requirements for Data Security Protection:* This standard, together with *Data Security Technology – Rules for Data Classification and Grading*, supports the implementation of China's *Data Security Law*. It focuses on establishing a data security protection mechanism based on data classification and grading.

  In addition to ongoing projects, several new standard proposals were discussed during the meetings, and these are expected to be approved as formal standard projects:

  - ➢ *Guidelines for Data Cross-Border Transfer Security Management:* This standard addresses the cross-border data transfer security management requirements set out in the CAC's *Rules on Promoting and Regulating the Cross-Border Flow of Data.*
  - ➢ *General Requirements for Battery Data Security:* This standard is designed to address the data provision requirements under the EU's battery regulations while establishing China's own

framework for battery data security.

- **New Standard Proposals to Support the Upgrade of the Cybersecurity Graded Protection Scheme**

  During the WG5 meetings, discussions were held regarding the need to revise the current standards for the Cybersecurity Graded Protection Scheme. The proposed revisions aim to introduce new requirements to address emerging technologies, including edge computing, big data systems, and generative AI security. Additionally, the revisions will encompass requirements related to cryptography, data security, and supply chain security.

  One significant addition in the proposals is the introduction of a fifth protection grade, which will specifically focus on identifying and safeguarding systems critical to national security, regional stability, national welfare, and public well-being.

  These proposals are expected to be approved as new projects, marking a key step in upgrading China's Cybersecurity Graded Protection Scheme from version 2.0 to 3.0.

IV. Conclusions

China's evolving regulatory landscape is increasingly shaped by the development and implementation of TC260' standards. These standards are designed to align with national priorities and international trends while addressing emerging technological risks. The revisions and new proposals will also play a pivotal role in supporting China's digital economy and enhancing its data protection and cybersecurity frameworks. For European stakeholders, staying abreast of these developments is essential, as they may impact both market access and regulatory compliance.

Introduction of SESEC Project

The Seconded European Standardization 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 Standardization 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 standardization information exchange and EU-China standardization cooperation.

The SESEC project supports the strategic objectives of the European Union, EFTA and the European Standardization 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 standardization bodies;**
- **Improve the visibility and understanding of the European Standardization System (ESS) in China;**
- **Gather regulatory and standardization intelligence.**

The following areas have been identified as sectoral 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 ofbuildings).