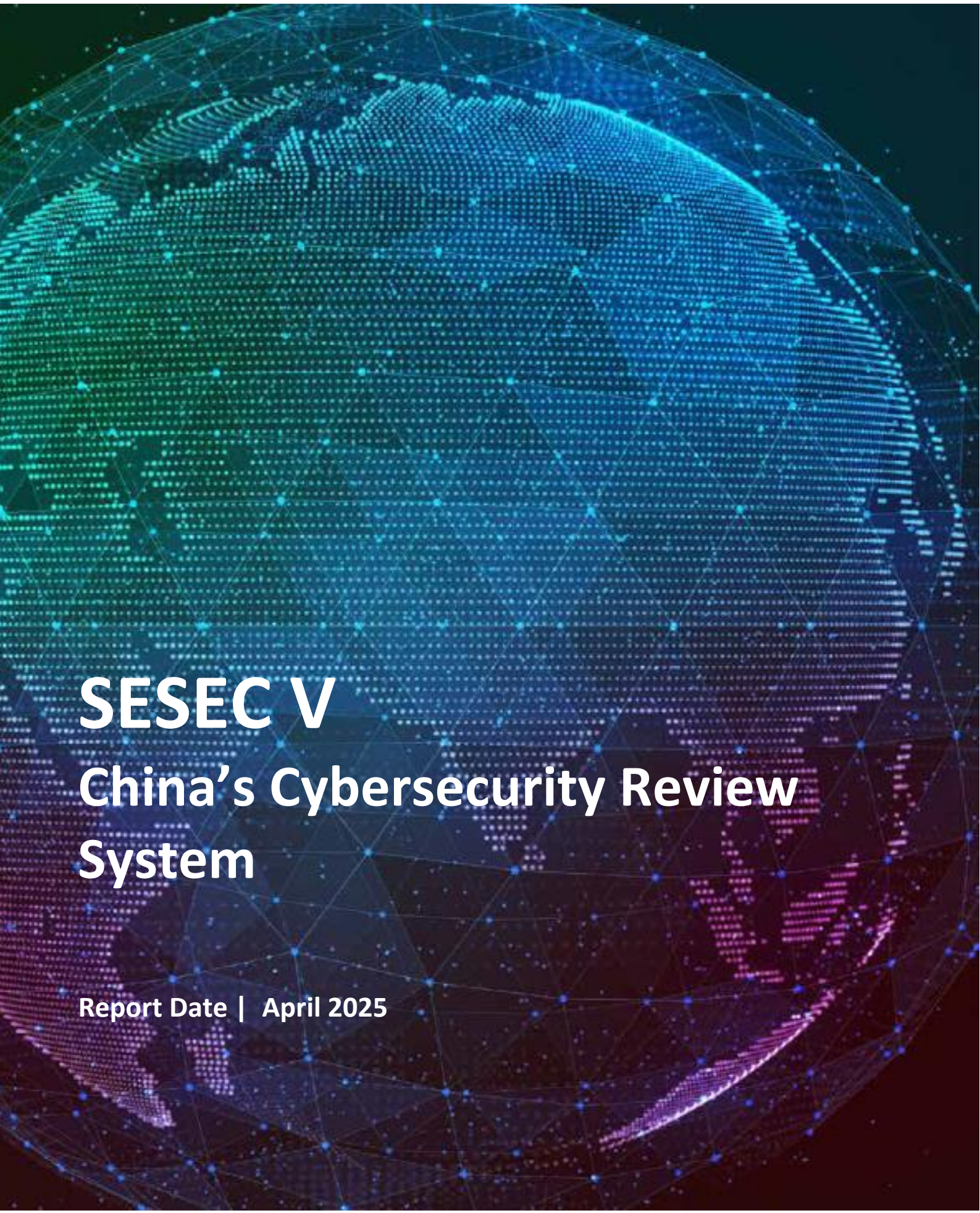

SESEC V

China's Cybersecurity Review System

Report Date | April 2025

Seconded European Standardisation Expert in China
(SESEC)

China's Cybersecurity Review System

1. Background

1.1 An Overview of China's Cybersecurity Legal System

Over the past decade, China has developed one of the world's most comprehensive cybersecurity legal frameworks. In contrast to the decentralized, consumer-oriented models seen in many Western countries, China adopts a **centrally coordinated, security-driven approach**, with enforcement carried out by national and local authorities under strong central oversight. In line with the *Cybersecurity Law*, the **Cyberspace Administration of China (CAC)** introduced the ***Cybersecurity Review Measures***, which formally established the country's cybersecurity review system.

The measures specify that the primary subjects of review are Critical Information Infrastructure Operators **(CIIOs)**—entities that are typically domestic and unlikely to be foreign-owned. However, the measures also stipulate that **network product providers engaged in business with CIIOs**, as well as **online platform operators managing the personal information of over one million users**, may also be subject to review. In 2023, the CAC launched a cybersecurity review against **Micron Technology**, a U.S.-based semiconductor company, citing concerns that its products posed significant national security risks to China's CIIOs.

This case highlights the need for **foreign enterprises to adopt a cautious and informed strategy** when operating in China's digital ecosystem. It also underscores the importance of raising internal awareness, strengthening compliance capabilities, and gaining a deeper understanding of China's evolving and complex cybersecurity review system.

As a core component in this legal system, the cybersecurity review system must be understood in the context of the broader legal architecture. This legal framework is built on **three foundational laws** and a key administrative regulation:

1. ***Cybersecurity Law*** **(CSL)** – effective since 2017 and currently under its second amendment (draft released in March 2025), the CSL establishes baseline requirements for network operation security, critical infrastructure protection, and legal liability.
2. ***Data Security Law*** **(DSL)** – effective since 2021, this law introduces a data classification regime and sets obligations for "important data" across sectors, especially in contexts related to national economy and public interests.
3. ***Personal Information Protection Law*** **(PIPL)** – also enacted in 2021, this law is often seen as China's equivalent to the EU GDPR, regulating the collection, processing, and transfer of personal information, with special rules for cross-border transfers.
4. *Regulations for the Administration of Network Data Security* - effective since 2025, a foundational administrative regulation that standardizes data processing activities and safeguards data security, providing detailed implementation rules for the *Data Security Law*.

Together, these laws establish a robust and interlocking framework covering all aspects of digital governance—from physical network equipment to platform operations and data flows.

1.2 Introducing China's Cybersecurity Review System

China's cybersecurity review system centers on the ***Cybersecurity Review Measures*** (hereinafter referred to as "the review measures"). The review measures are designed to **safeguard national security** in the digital domain. It is positioned as a risk-control mechanism specifically designed to assess and prevent national security risks arising from the procurement or use of network products and services by CIIOs, overseas IPOs and other data processing activities involving at least one million individuals. The aforementioned **three cornerstone law** and ***Security Protection Regulations for Critical Information Infrastructure*** which is an administrative regulations designed for regulating CIIOs make up the legal basis for the review measures.

The first trial version of the review measures was first released in 2017. CAC spearheaded drafting of the review measures along with other 11 national regulatory bodies. However, the U.S. IPO case of the Chinese ride-hailing APP Didi exposed new scenarios lacked in the review measures, prompting a revision in 2021 with enrollment of the Securities Association of China into the drafting committee. As a result, the current version was issued and took effect in April 2022.

2. The Cybersecurity Review Measures

2.1 The Scope and Target of the Review Measures

The review measures were initially designed to regulate procurement of network products and services by CIIOs, which is why many provisions appear to focus exclusively on them. However, as digital technologies becomes increasingly embedded in the daily lives of Chinese citizens, the volume of personal information collected and processed by online platforms has mounted to a level that raised concerns within Chinese government. Recognizing this trend, the authorities have extended the scope and focus of the cybersecurity review system to strengthen national security safeguards.

Currently, the review measures primarily apply to three categories of stakeholders:

(1) CIIOs;
(2) Online Platform Operator;
(3) Network Product and Service Providers.

And cover three key scenarios:

(1) Purchase of Network Products and Services;
(2) Data processing activities, particularly on cross-border data transfer,are albeit not stated explicitly;
(3) Overseas IPO for those with personal information of at least 1 million online users.

It is important to note that while the provisions explicitly address the first two categories of stakeholders, **network products and service providers** are not directly referenced in most clauses. However, if they are involved in the procurement and data processing activities conducted by CIIOs or online platform operators, they must also comply with the review process. The case of Micron Technology illustrates this concern in practice. In March 2023, the CAC announced that Micron had sold products to China's CIIOs without undergoing a security assessment, prompting the launch of a formal cybersecurity review. After 50 days of review, in May 2023, the review concluded that Micron's products posed national security risks, and as a result, the company was prohibited from supplying products to any CIIOs in China thereafter.

To reduce the likelihood of such incidents, SESEC recommends that foreign stakeholders carefully study Articles 6, 10, and 15 of the Measures, which clarify the responsibilities of network product and service providers during the cybersecurity review process.

2.2 Triggering Mechanism

The review measures outline two triggering mechanisms for cybersecurity review:

(1) Voluntary Review
(2) Reactive Audit.

2.2.1 Voluntary Review

The review measures adopt a principle of **pre-approval review** (Article 3). Accordingly, CIIOs or online platform operators managing personal information of more than 1 million users must conduct a national security risk analysis prior to initiating procurement or data processing activities(Article 5). CIIOs are expected to follow guidelines issued by their respective supervisory authorities during the assessment. If operator identifies potential national security risk, they are required to report the situation to the **Cybersecurity Review Office(CRO)** under the **CAC**. The CRO will decide **within 10 working days** whether a cybersecurity review is warranted. A written notice will be issued to inform the of the outcome. If a review is deemed necessary, the CRO will initiate a **preliminary review lasting 30 working days.**

2.2.2 Reactive Audit

However, if the operators failed to voluntarily report and any member authority involved in drafting the review measures discovers a potential national security risk, the relevant regulator has the power to launch a cybersecurity review (Article 16). CIIOs and online platform operators are strongly advised to comply with the voluntary review, as penalties under a reactive audit are likely to be more severe.

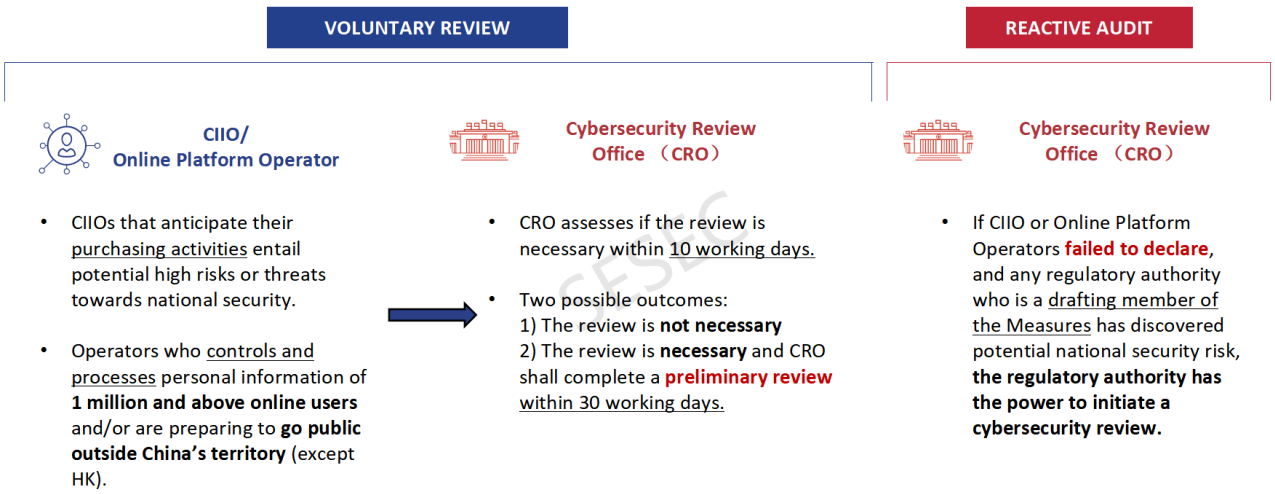

Figure 1. Visualization of the Two Triggering Mechanisms

2.3 Review Process and Timeline

The cybersecurity review process in China follows a structured, multi-phase timeline managed by the CRO. The process begins when a CIIO or online platform operator submits a review request. The CRO has up to **10 working days** to assess the submission and decide whether a formal cybersecurity review is required. If a review is necessary, the CRO conduct a **preliminary review**, which is typically completed within **30 working days** for general cases. For **complicated cases**, the CRO may extend the review by an additional **15 working days** to allow for further risk analysis. Once the CRO completes its review, the case is transferred to the Review Committee, which issues a written opinion within **15 working days**.If the Review Committee cannot reach a conclusion, a **special review procedure** is triggered. This phase, led by the committee and relevant industry authorities, can take up to **90 working days** to complete. This staged process ensures that cybersecurity risks—especially those involving national security—are carefully assessed before critical technologies or data processing activities proceed.

However, the Cybersecurity Review Measures extend beyond the initial review phase. Article 3 establishes that the review process follows the principle of **ongoing supervision**, covering the **entire lifecycle** of the products and services

under review. Enterprises subject to the review are therefore expected to remain vigilant, maintain a prudent approach, and continuously strengthen their **data protection mechanisms** to ensure long-term compliance.

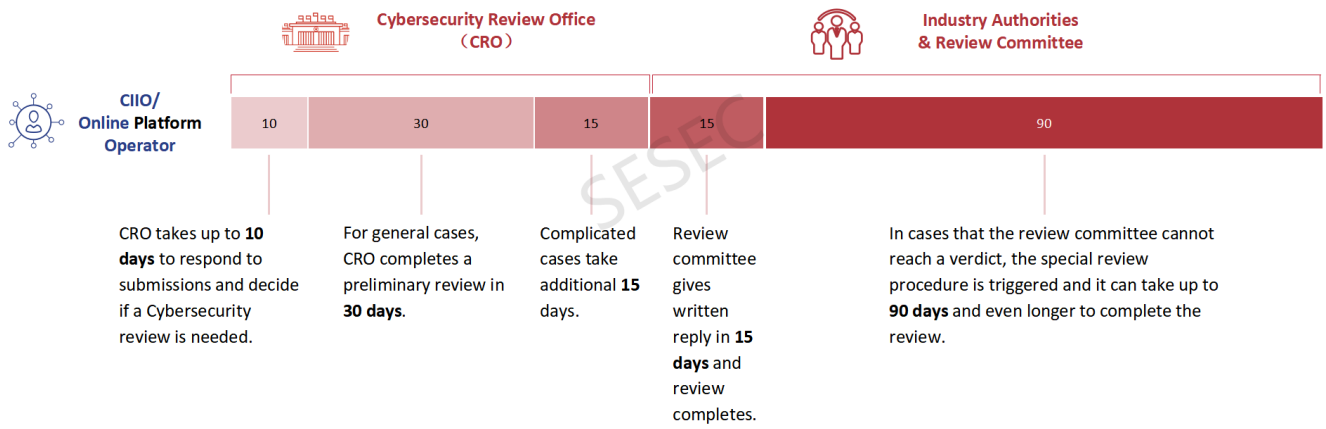

Figure 2. Timeline of the Cybersecurity Review

2.4 Assessment Risk Factors of the Review

Article 10 of China's *Cybersecurity Review Measures (2022)* outlines the key risk factors assessed during a cybersecurity review. The focus is on **national security**, particularly the risk of foreign interference in Critical Information Infrastructure (CII), supply chain disruptions, and loss of control over core or personal data.

The review also considers the provider's compliance with Chinese law, the geopolitical risks tied to product sourcing, and the potential for foreign governments to access or influence Chinese data—such as the context of Overseas IPOs in which foreign governments have laws and regulations that grant themselves rights to obtain users' data for investigation.

1. *Risk that the use of products and services could lead to **illegal control** of, **interference** with, or **destruction of CII**;*
2. *Harm to **CII business continuity** arising from product and service supply disruptions;*
3. ***Security, openness, transparency,** and **diversity** of sources of products and services; the **reliability** of supply channels, as well as the **risk of supply disruption** due to **political, diplomatic, and trade factors**;*
4. *Product and service providers' **compliance** with Chinese national laws, regulations, and department rules;*
5. *Risk that core data, critical data or large amounts of personal information are **stolen, leaked, damaged, or illegally used or illegally exported**;*
6. *Risk that CII, core data, important data, or large amounts of personal information are affected, controlled, or maliciously used by **foreign governments** due to listing overseas, as well as cybersecurity risks;*
7. *Other factors that could harm CII security cybersecurity and data security.*

--- Cybersecurity Review Measures(Revised)

Figure 3. Seven Assessment Risk Factors Stipulated in the Review Measures

These clauses are **intentionally broad**, enabling authorities to consider any factor they deem relevant to cybersecurity or data security. This grants regulators wide discretionary power in determining review outcomes. However, despite the open-ended language, three core areas of focus—each reflecting the priorities of China's three cornerstone laws (the *Cybersecurity Law*, the *Data Security Law*, and the *Personal Information Protection Law*)—can still be clearly identified in practice:

(1) Data Localization

This focal area is particularly useful for clarifying why enterprises that require overseas IPO still need to take cybersecurity reviews seriously. In line with China's *Cybersecurity Law*, the review process closely examines whether data-related activities (defined in *Data Security Law*)—including **collection, storage, use, processing, transmission , provision, disclosure and deleting**—are conducted entirely within mainland China. A key concern is the risk of cross-border data transfer or leakage, particularly under foreign legislation such as the U.S. CLOUD Act, which could compel access to overseas-stored data. The review also seeks to prevent overreliance on foreign suppliers, with particular scrutiny on cases where there is 100% dependence on non-Chinese technology or infrastructure.

(2) Data Classification - The review measures are particularly concerned with cases where CIIOs or online platform operators underestimate or misclassify the importance of certain data types. For instance, some enterprises may incorrectly consider geographic or transportation data as "unimportant," despite such data being explicitly

protected under Chinese law. To address these challenges and assist stakeholders in accurately identifying core and important data, China has introduced ***GB/T 43697-2024, Data Security Technology—Rules for Data Classification and Grading***. This national standard establishes a state-led framework for classifying data by sensitivity and potential impact, aligning with the Data Security Law and promoting risk-based protection measures across all sectors.

(3) Data Protection Mechanism - The review measures place strong emphasis on evaluating whether operators have adequate data protection mechanisms, and whether their products, services, or components may contain malicious logic or be vulnerable to hidden remote control functions—such as the unauthorized shutdown of critical systems not disclosed in official specifications.

3. Conclusion

China's cybersecurity review system is intentionally broad and grounded in national security priorities, contrasting sharply with the EU's more transparent, rights-based approach. As a result, the process may seem less predictable, with implicit factors potentially influencing whether a review is triggered. This creates compliance risks for foreign stakeholders unfamiliar with China's legal and regulatory landscape. Companies operating in or exporting to China should assess whether their business partners fall within the scope of review and ensure they have robust cybersecurity protection mechanisms in place. This is especially critical for firms in sectors such as **cloud services**, **industrial connectivity**, and **digital infrastructure**, which must become well-versed in China's cybersecurity review framework, learn to interpret regulatory signals, and ensure their products, data practices, and supply chains align with Chinese requirements.

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).