ASIALLIANS

December 17, 2025

I. Newly revised Cybersecurity Law to boost digital governance

Background

On October 28, 2025, the Standing Committee of the 14th National People's Congress passed the decision on revising **the Cybersecurity Law,** which will come into effect on January 1, 2026. This is the first major revision since its implementation in 2017 to adapt to the rapid development in cybersecurity.

Key content

1) AI governance

The new Cybersecurity Law emphasizes that the State supports and improves:

- Fundamental research in AI,
- Development of key technologies such as algorithms,
- Construction of infrastructure including training data resources and computing power,
- Ethical standards for AI,
- Risk monitoring, assessment, and safety.

The new Cybersecurity Law adopts AI governance for the first time. It is a signal that supervision on AI governance will be focused more from the legal hierarchy of law.

2) Legal liabilities for breaching network protection obligations

Network operators and CIIOs ("Critical Information Infrastructure Operators") who breach cybersecurity protection obligations will be sanctioned. Comparing to prior regime, penalties are increased. In particular, those who refuse to rectify illegal behaviors or causing harm to network security consequences can only be fined in the past. Now, first violation will be fined. The upper and lower limits of fines have increased as well. Additionally, other directly responsible personnel will also be fined comparing to the past without sanctions.

Type of violation	Sanctions
A network operator fails to: • Fulfill requirements for the Network Security Level Protection System; • Develop emergency response plans for network security incidents, or promptly address security risks and report to relevant regulatory authorities;	• First violation: Fine of RMB 10,000-50,000. • First violation causing massive data leakage: Fine of RMB 500,000–2,000,000; • Responsible persons: Fine of RMB 50,000–200,000.
A CIIO fails to: • Establish specialized safety management agencies and managers; • Regularly provide cybersecurity education, technical training, and skill assessments to practitioners; • Perform disaster recovery backup for important systems and databases; • Develop emergency plans for cybersecurity incidents and conduct regular drills;	• First violation: Fine of RMB 50,000–100,000 • Serious consequences (massive data leakage, partial loss of CII functions): Fine of RMB 500,000–2,000,000; Responsible persons: Fine of RMB 50,000–200,000; • Particularly serious consequences (e.g., total loss of CII functions):

• The procurement of network products and services that may affect national security shall go through a national security review; • Conduct at least one annual inspection and assessment.	Fine of RMB 2,000,000–10,000,000; Responsible persons: Fine of RMB 200,000–1,000,000.

3) Coordination for personal information protection

Network operators shall comply with the Civil Code, the Cybersecurity Law and the Personal Information Protection Law when processing personal information. Personal information protection is restated in the Cybersecurity Law.

4) Extraterritorial jurisdiction for activities endangering cybersecurity

Overseas institutions, organizations, and individuals engaged in activities that endanger the cybersecurity of the state shall be held legally responsible. For serious consequences, the public security department and relevant departments may freeze the assets or take other necessary sanctions. Under prior regime, those who engaging in attacks, intrusions, interference, damage, or other activities that endanger the critical information infrastructure of China will be held legally responsible, whereas under new regime, those who engaging in any activities that pose a threat to China's cybersecurity will be sanctioned.

This broad and open-ended formulation significantly expands the scope of the provision, transforming it into a catch-all clause that grants wide discretionary powers to the authorities.

Conclusion

The revised Cybersecurity Law signals a higher level of regulatory scrutiny and a more demanding compliance environment for all companies operating in or with China. Businesses should anticipate stricter enforcement, higher financial exposure, and increased accountability of management and key personnel.

In practice, companies are advised to (i) review and update their cybersecurity compliance frameworks, including network security level protection and incident response mechanisms; (ii) ensure consistency between cybersecurity, personal information protection, and AI-related governance policies; and (iii) assess potential cross-border and extraterritorial risks, particularly for group-wide digital operations.

Early gap assessments and proactive compliance measures will be critical to mitigate enforcement risks and to maintain operational resilience in China as the revised law enters into force in 2026.

II. Easier Compliance: New Customs Rules Benefit Overseas Food Businesses

Background

On October 14, the GACC (General Administration of Customs of China) has issued **the Administrative Provisions of the Customs on the on the Registration of Overseas Manufacturers of Imported Food (Order No. 280 of the GACC)**(the "Provisions", "Order No. 280") , which will become effective on June 1, 2026.

If you are an Overseas Manufactures of Imported Food ("OMIC"), the Provisions will officially apply to you from June 1, 2026. You must complete registration with the GACC before conducting export business to China. The optimized new rules simplify procedures via classification management and List registration while strengthening full-chain food safety supervision to better align with actual trade needs.

Key content

1) Registration method for classification management

The GACC will implement a Registration method for classification management system for OMIC, which refers to specific registration methods, application materials, evaluation procedures and other registration management requirements will be determined by the GACC taking into account of the following two points:

- Evaluation results of the food safety management system and inspection situation on the food safety status of the country (region) where the OMIC is located;
- Risk level of the relevant food products.

2) List registration method

If the food safety management system of the country (region) where the OMIC is located has been recognized by GACC and meets one of the following conditions, the GACC may agree in writing with the competent authority of the country (region) where it is located to adopt a list registration method for its enterprise:

(1) Those who have signed an import and export food safety cooperation agreement with the General Administration of Customs;

(2) Those who have signed cooperation agreements, memoranda, joint statements and other cooperation documents with China;

(3) Other situations possible to adopt the list registration method after risk assessment.

3) Automatic renewal of registration validity

The prior regime requires OMICs to submit an application for renewal of registration to GACC within 3 to 6 months prior to the expiration of the registration validity period. The new regime specifies the registration will be automatically renewed for a period of 5 years except for the following circumstances :

- Imported food is included in the list of foods that are not automatically renewed for registration;
- Enterprises do not meet registration requirements and are in the process of rectification;
- GACC suspended the import of relevant food from the country (region) where the OMIC is located.

Such revision will ease the burden of OMICs seeking to extend the registration validity without going through lengthy formalities.

3. Conclusion

Order No. 280 introduces a more differentiated and pragmatic registration framework for overseas manufacturers of imported food, combining procedural simplification with risk-based supervision. For eligible enterprises, the classification management and list registration mechanisms may significantly reduce administrative friction and improve predictability in access to the Chinese market.

In practical terms, overseas food businesses should (i) assess their eligibility for simplified registration or list-based registration depending on product risk and the regulatory status of their home jurisdiction; (ii) review the robustness of their food safety management systems in anticipation of enhanced risk assessments; and (iii) monitor whether their products fall within the scope of automatic renewal or excluded categories.

Early preparation ahead of the June 1, 2026 effective date will allow OMICs to secure continued market access to China while benefiting from streamlined procedures under the new regime.