CLIENT ALERT | January 14, 2026

China's Cybersecurity Law Amendments Increase Penalties, Broaden Extraterritorial Enforcement

The Amendments, which took effect on January 1, 2026, will impact network operators and CIIOs within China and overseas.

Key Points:

- The Amendments **broaden the scope of overseas activities that could be subject to enforcement** by PRC authorities to include any activities overseas that endanger the PRC's cybersecurity. Overseas enforcement under the CSL previously only applied to overseas activities that endangered critical information infrastructure.
- **Increased fines and new penalties** for cybersecurity violations. Fines for violations of cybersecurity obligations and failure to remove illegal content under the CSL is set to increase, with the highest fine reaching RMB 10 million for network operators and CIIOs and RMB 1 million for that violator's directly responsible individuals where the violation causes "particularly serious consequences" in the PRC. New financial penalties are introduced for other violations of the CSL, namely, the sale and provision of critical network equipment and dedicated cybersecurity products that are uncertified or have not passed the relevant security certification/testing requirements.
- The Amendments **outline circumstances where penalties may be mitigated or waived** under the PRC Administrative Penalty Law, such as where the violator cooperates with investigations or takes steps to mitigate the harm. Penalties could also be waived for first-time violations that cause minor harm and were promptly corrected.

On October 28, 2025, the Standing Committee of the PRC National People's Congress (NPC) introduced amendments to the Cybersecurity Law (CSL) (the Amendments). The Amendments, which took effect on January 1, 2026, tighten enforcement and broaden the CSL's extraterritorial reach.

Legislative Intent of the Amendments

In September and October 2025, the NPC published a number of statements[1] revealing the legislative intent of the changes. To address the rapid evolution of information technology, AI, and growing cybersecurity risks, the Amendments aim to:

- **Strengthen legal liability and enforcement deterrence** by (i) imposing stricter, tiered penalties for violations of cybersecurity obligations, (ii) imposing stricter measures for the certification, testing, and review of critical network equipment and dedicated cybersecurity products, and (iii) broadening the range of enforcement measures for related violations
- **Harmonize rules and responsibilities with other PRC laws,** namely the Data Security Law, the Personal Information Protection Law, and the Administrative Penalty Law
- **Promote compliance** by introducing grounds for leniency, mitigation, or waiver of administrative penalties and encouraging proactive remediation
- **Balance security and innovation** by embedding AI principles into the CSL's core legislative requirements and improving regulatory oversight to promote the healthy development of AI

Overall, the Amendments aim to safeguard national cyberspace sovereignty, security, and development interests; protect the lawful rights and interests of all parties involved; and foster a healthy cyber ecosystem.

Overview of the Amendments

Broadened Extraterritorial Effect

The CSL is the PRC's dedicated cybersecurity law and applies to "network operators" in connection with their construction, operation, maintenance, and use of networks within the territory of the PRC. Due to the broad definition of "network operator" (i.e., network owners, administrators, and network service providers), most entities in the PRC will likely be subject to and need to comply with the CSL.

The CSL only regulates activities occurring on networks that are physically within the territory of the PRC. However, the CSL does authorize PRC authorities to investigate and take actions to defend against network activities (e.g., attacks, intrusions, interference, or other damage) occurring outside of the PRC that endanger critical information infrastructure in the PRC.

The Amendments broaden the scope of activities overseas that could be subject to enforcement to include any activity overseas that endangers the PRC's cybersecurity and subsequently causes serious consequences in the PRC. In such cases, PRC authorities may impose sanctions, such as freezing assets or other punitive measures. This broadened scope could potentially result in increased enforcement activities against offshore individuals or organizations whose activities are deemed to endanger the PRC's cybersecurity.

Increased or Newly Introduced Financial Penalties

The Amendments increase existing financial penalties under the CSL and introduce tiered penalties based on the severity of consequences caused by the violations. For example, the highest maximum fine is RMB 10 million for violations that cause "particularly serious consequences" (such as loss of the main

functions of critical information infrastructure) and RMB 1 million for the violator's directly responsible personnel.

In practice, only critical information infrastructure operators (CIIOs) are likely to face such fines (a type of network operator that operates critical information infrastructure), given the example in the Amendments used to describe "particularly serious consequences". For non-CIIO network operators, the highest fine imposed in practice will likely be RMB 2 million. This will apply in cases where the network operator fails to perform its cybersecurity obligations and, as a result, causes large amounts of data to be leaked or other serious consequences that endanger the PRC's cybersecurity. As this tiered approach is based on the severity of the violations, network operators and CIIOs should focus on promptly containing and mitigating the harmful effects of any violation.

The Amendments also broaden the range of violations that are subject to penalties under the CSL to include the sale or provision of critical network equipment and dedicated cybersecurity products that are uncertified, have not passed the relevant security certification/testing requirements, or otherwise do not comply with mandatory national standards. Such violations will be subject to a maximum fine of RMB 100,000 if there are no illegal gains or if the illegal gains are less than RMB 100,000. If the illegal gains exceed RMB 100,000, the fine shall be no more than five times the amount of illegal gains. If the consequences of the violation are serious, other penalties may be imposed, including an order for suspension of business and/or revocation of business license.

The table in section 5 maps out the new penalties introduced by the Amendments.

Leniency for Penalties

The Amendments outline circumstances where penalties may be mitigated or waived under the PRC Administrative Penalty Law.

- Examples of circumstances where fines could potentially be mitigated:
    - Violator takes steps to mitigate the harmful consequences caused
    - Violation is committed under coercion or inducement by others
    - Violator voluntarily confesses unlawful acts not yet known to the administrative authority
    - Violator provides assistance and cooperates with authorities during the investigation
- Examples of circumstances where fines could potentially be waived:
    - Violations are minor, promptly corrected, and have caused no harmful consequences
    - The facts of the violation cannot be established

- Violation is discovered after the statute of limitation (generally two years, or five years for violations involving life and health or financial security that have harmful consequences)

Other Amendments

Other notable changes introduced by the Amendments include:

- **Alignment with other PRC laws** by clarifying that network operators must comply with the CSL and other relevant PRC laws and regulations, including the PRC Civil Code and the Personal Information Protection Law when processing personal information.
- **AI governance** through the introduction of a new provision on AI, signalling the state's support for AI development and the use of AI for enhancing cybersecurity protection. The new AI provision explains that the state will improve ethical norms for AI, strengthen AI security risk monitoring and assessment, and promote the healthy development of AI. While the Amendments do not provide further details, such as obligations or requirements that network operators must follow, the inclusion of the new AI provision suggests that AI is front of mind for state authorities and will likely be an important consideration in their supervision of cyber and data security matters.

Summary of Amendments to Penalties Under CSL

Relevant Violations	New CSL Article (as amended)	Baseline Penalties	Escalation Tiers
General cybersecurity obligations — failure to perform network security protection obligations set forth in Art. 23–27 CSL, e.g., conduct security certification, testing, and risk assessments; provide real identity information; formulate cybersecurity incident emergency plans; and promptly address security risks	Art. 61 (formerly Art. 59)	**Network operators:** • warning; • rectification order; and/or • fines of RMB 10,000 to RMB 50,000 **CIIOs:** • warning; • rectification order; and/or • fines of RMB 50,000 to RMB 100,000	*Refusal to rectify or harmful consequences caused (e.g., endangering cybersecurity)*: **Network operators:** fines of RMB 50,000 to RMB 500,000; and fines of RMB 10,000 to RMB 100,000 for directly responsible personnel **CIIOs:** fines of RMB 100,000 to RMB 1 million and fines of RMB 10,000 to RMB 100,000 for directly responsible personnel *Serious consequences (e.g., result in large-scale data leakage and partial functional outages of critical information infrastructure)*: **Network operators / CIIOs:** fines of RMB 500,000 to RMB 2 million and fines of RMB 50,000 to RMB 200,000 for directly responsible personnel *Particularly serious consequences (e.g., result in main functional outages of critical information infrastructure)*:

			Network operators / CIIOs: fines of RMB 2 million to RMB 10 million and fines of RMB 200,000 to RMB 1 million for directly responsible personnel
Content obligations — failure to stop transmission, delete, preserve records, and report illegal content	Art. 69 (merged and amended)	**Network operators / CIIOs:** • rectification order; • warning; • public notice; and/or • fines of RMB 50,000 to RMB 500,000	**Network operators / CIIOs:** *Refusal to rectify or in serious circumstances (no definition or example specified)*: Fines of RMB 500,000 to RMB 2 million; may order suspension, rectification, closure, or revocation; and fines of RMB 50,000 to RMB 200,000 for directly responsible personnel *Particularly serious impact or consequences (no definition or example specified)*: Fines of RMB 2 million to RMB 10 million; plus order suspension, rectification, closure, or revocation; and fines of RMB 200,000 to RMB 1 million for directly responsible personnel
Uncertified critical network equipment/dedicated cybersecurity products — sale/provision without required certification/testing or noncompliance with mandatory national standards	Art. 63 (new)	**Network operators / CIIOs:** • order to cease sales/provision; • warning; and/or • confiscation of illegal gains	**Network operators / CIIOs:** *If no illegal gains or gains less than RMB 100,000*: Fines of RMB 20,000 to RMB 100,000 *If illegal gains above RMB 100,000*: Fines of one to five times illegal gains *In serious circumstances (no definition or example specified)*: Order suspension of relevant business; rectification; and/or revocation of permits or business license
Cybersecurity activities and public vulnerability releases — unauthorized certification/testing/risk assessment or public releases of vulnerabilities, malware, attacks/intrusions	Art. 65 (amended; formerly Art. 62)	**Network operators / CIIOs:** • rectification order; • warning; and/or • fines of RMB 10,000 to RMB 100,000	**Network operators / CIIOs:** *Refusal to rectify or in serious circumstances (no definition or example specified)*: Fines of RMB 100,000 to RMB 1 million; may order suspension, rectification, closure, or revocation of business license; and fines of RMB 10,000 to RMB 100,000 for directly responsible personnel *If serious consequences caused*:

			Penalties per the serious tier under Art. 61 above. *If particularly serious consequences result*: Penalties per the highest tier under Art. 61 above
CIIO security review violations — use of network products/services without required security review or where review fails	Art. 67 (amended; formerly Art. 65)	**CIIOs:** • order to rectify within a time limit; • suspend use; and/or • eliminate impact on national security	**CIIOs:** *Escalation*: Fines of one to 10 times network product procurement amount and fines of RMB 10,000 to RMB 100,000 for directly responsible personnel

Next Steps

The Amendments reflect a shift toward outcome-driven enforcement and higher monetary penalties, paired with broader extraterritorial exposure and avenues for leniency on penalties. Network operators and CIIOs within the PRC should strengthen and review their cybersecurity compliance controls for compliance with the CSL and ensure that prompt remediation actions are taken to mitigate the harmful effects of any violations. Entities outside of the PRC should also review whether their activities could potentially have the effect of endangering the cybersecurity of the PRC.

This Client Alert was prepared with the assistance of Zurui Yang and Kenneth Wang in the Beijing office of Latham & Watkins.

Contacts

Rhys McWhirter
rhys.mcwhirter@lw.com
+852.2912.2686
Hong Kong

Hui Xu
hui.xu@lw.com
+86.10.5965.7006
Beijing

Bianca H. Lee
bianca.lee@lw.com
+852.2912.2500
Hong Kong

Endnotes

[1] http://www.npc.gov.cn/npc/c2/c30834/202510/t20251028_449057.html; http://www.npc.gov.cn/npc/c2/c30834/202509/t20250916_448013.html; http://www.npc.gov.cn/npc/c2/c30834/202510/t20251025_448658.html.