Regulatory Update – Approval of the "Network Security Review Measures" (January 2022)

On 28 December 2021, the Cyberspace Administration of China announced that the "Network Security Review Measures" (the "Measures") approved on 16 November 2021 will come into effect from 15 February 2022. The Measures have been designed to ensure the safety of key information infrastructure facility supply chain, protect cyber and data security and maintain national security. The previous version of the Measures originally published on 13 April 2020 will become void.

A national cyber security review mechanism was also established with an office (the "Cyber Security Office") located at the Cyberspace Administration of China. The office has been established to review China's cyber security policy and implement cyber security review measures.

Reporting to the Cyber Security Office:

Key information infrastructure facility operators are expected to evaluate potential national security risks that might be posed by the products or services which they intended to purchase. If a risk has been identified that may impact national security, the key information infrastructure facility operator must report the product or service to the Cyber Security Office.

Key information infrastructure facility operators will be required to ensure that the product and/or service providers agree via a purchase agreement, among other things, not to obtain user data, control and/or manipulate user devices illegally, stop product supply or cease offering necessary technical supporting services without a suitable reason.

Online platform operators which hold the personal information of more than 1 million users and intend to get listed on a stock exchange outside of Mainland China must notify the Cyber Security Office so that a cyber security review can be conducted.

Any reports that are made to the cyber security office should include the following documentation:

1. The designated reporting form;
2. An analysis report on the impact or potential impact the product or service may have on national security;
3. Purchase documents, agreements, contract intended to enter or listing documents intended to submit such as IPO; and
4. Any other materials needed for a cyber security review.

Cyber Security Key Assessment:

When undertaking a cyber security key assessment, a key information infrastructure facility operator should look to critically assess the following:

1. The risk of a key information infrastructure being illegally controlled or disrupted or damaged caused by the products and services.
2. The continuous harm to the key information infrastructure brought by the disruption of product and/or service.
3. The security, publicity, transparency and reliability of the supply channel of the products and services. This should include the risk of supply disruption due to political, diplomatic factors, etc.

ComplianceAsia Consulting Ltd. Suite 1102, ChinaChem Tower, 34-37 Connaught Road, Central, Hong Kong
Tel: (852) 2868 9070 www.complianceasia.com

4. The risk of core data, key data or personal information being stolen, leaked, disrupted, or used illegally.
5. The risk of cyber security breaches and key information infrastructure, core data, key data or personal information being affected, controlled or used by foreign governments, as part of the listing.
6. Other potential factors harming key information infrastructure security, internet security and data security.

Procedure for Reporting

Where a report includes sufficient supporting documents, the Cyber Security Office will provide written confirmation on whether the case will be investigated within 10 business days upon of the receipt of the report.

If the Cyber Security Office believes the case warrants further review, it will undertake a preliminary review which must be completed within 30 business days. During this preliminary review, the Cyber Security Office will provide recommendations and send these recommendations to the cyber security review mechanism member unit and relevant departments for approval. If the case is deemed complicated the review is likely be expedited and the preliminary report will be completed within 15 business days.

The Cyber security review mechanism member unit and relevant departments must reply in writing within 15 business days upon the receival of preliminary review recommendations.

A review notice will be sent to applicant if the cyber security review mechanism member unit and relevant departments agree on a conclusion. Special review procedures will be followed, and the applicant will be informed if the cyber security review mechanism member unit and relevant departments disagree on the risk to national security.

Where a special review is required, the Cyber Security Office must obtain opinions from relevant units and departments, conduct an in-depth assessment, make further review recommendations, seek opinions from the cyber security review mechanism member unit and relevant departments, report to central cyber security and seek approval from the informational committee, then reach a review conclusion and inform the applicant. This processes typically takes 90 business days to conclude and longer for more complicated cases.

ComplianceAsia Consulting Ltd. Suite 1102, ChinaChem Tower, 34-37 Connaught Road, Central, Hong Kong
Tel: (852) 2868 9070 www.complianceasia.com

About ComplianceAsia Consulting Limited

ComplianceAsia Consulting Limited ("ComplianceAsia") is the longest established compliance consulting firm in Asia Pacific, established in 2003 with office in Hong Kong, Singapore, Shanghai, Tokyo and London. We have an unmatched track record of completing complex compliance consulting projects for financial firms in the APAC region. With 80 multilingual staff, including compliance experts with experience in dealing with the SFC, HKMA, MAS, CSRC, AMAC, JFSA and Asian exchanges, we provide independent, unbiased advice on Asian financial industry legislation and regulations.

The ComplianceAsia Group also includes AML Services Limited, OnlineCompliance.Training, CA College, CPTnow, and ComplianceAsia ESG Consulting.

Contact Us Today

MAINLAND CHINA
Room 132, Unit 1301-1308
13/F, Shanghai Tower
No.479 Lujiazui Ring Road
Pudong New Area Shanghai

T: +86 147 1431 1859

HONG KONG SAR
Suite 1102
ChinaChem Tower
34-37 Connaught Road
Central

T: +852 2868 9070

SINGAPORE
137 Telok Ayer Street
#03-06
Singapore 068602

T: +65 6533 8834

JAPAN
Level 2
Marunouchi Nijubashi Building
3-2-2 Marunouchi Chiyoda-ku
Tokyo 100-0005

T: +81 3 6837 5483

LONDON
1 St. Andrew's Hill
London
EC4V 5BY

T: +44 (0) 20 7236 0921
M: +44 (0) 7310 972435

Philippa Allen
CEO and Founder
E: philippa.allen@complianceasia.com

Alex Duperouzel
Managing Director
E: alex.duperouzel@complianceasia.com

Rachel Wu
Head of Mainland China Client Engagements
E: rachel.wu@complianceasia.com

www.complianceasia.com

ComplianceAsia