Newly Released PRC Measures for Cyber Security Review [1]

On April 27, 2020, the Cyberspace Administration of China ("CAC") and other 11 departments[2] jointly released the Measures for Cyber Security Review (the "Measures") which will be implemented since June 1, 2020. The core idea of the Measures is to require Critical Information Infrastructure Operators ("CIIO") procuring network products and services that affect or may affect national security or network security launch the cyber security review process. Further, the Measures emphasize the legislative intent is to protect national security and the safety of Critical Information Infrastructure supply chain without restricting or discriminating against foreign products and services. Finally, the Measures design a review procedure along with protecting intellectual property of enterprises. We hereby summarized the most eye-catching contents for your kind reference.

I. Implementing proactively reporting system—take CIIO as the initiator to launch the review process

The Measures impose an obligation upon CIIO[3] to report Cyber Security Review Office[4] where the CIIO procures network products and services[5] and predicts such products and services may bring national security risks.

To conduct risk assessment, CIIO may consider the following aspects:

• ***Relevant industrial standards***: relevant industrial standards can be made by critical information infrastructure protection department to serve as an important guidance for CIIO to predict the risks. Companies may conduct risk assessment by referring these guidance.

• ***Factors balanced by Cybersecurity Review Office during the preliminary review:***

1. the risks of illegal control, interference or damage to the Critical Information Infrastructure caused by the use of products and services, and the theft, leakage and damage to the important data;
2. the damage to business continuity of Critical Information Infrastructure caused by the disruption of the supply of products and services;
3. the security, openness, transparency, source diversity of products and services, the reliability of supply channels and the risks of supply disruption due to political, diplomatic and trade factors, etc.;
4. product and service providers' compliance with Chinese laws, administrative regulations and department regulations;
5. other factors that may jeopardize the security of Critical Information Infrastructure and national security.

To fulfill reporting obligation, the CIIO shall submit the following materials:

• Declaration;
• Analysis report on the impact or possible impact on national security;
• Purchase documents, agreements, contracts to be signed;
• Other materials required for network security review.

In addition, the Measures impose an obligation upon CIIO to require the network product and service provider to cooperate with the network security review through signing procurement documents, agreements. To be specific, the provider shall commit not to illegally obtain user data by using the convenience of providing products and services, not to illegally control and manipulate user equipment, and not to interrupt the product supply or necessary technical support services without justifiable reasons.

II. The review process and timeframe

Kick-off	CIIO proactively reports to the Cybersecurity Review Office where the CIIO predicts the national security risks that the product and services may bring.
Acceptance	The Cybersecurity Review Office determines whether it is necessary to review and notify the CIIO in writing within 10 working days after receiving the review application.
Preliminary Review	For the application accepted, the Cybersecurity Review Office complete the preliminary review within 30 working days from the date of sending the written notice; in case of complex circumstances, 15 working days may be extended.
Feedback	The Cybersecurity Security Review Mechanism Members[6] and relevant Critical Information Infrastructure Protection Departments shall reply in writing within 15 working days after receiving the preliminary review opinions from the Cybersecurity Review Office. • If the reply is consistent with the preliminary review opinion, the Cybersecurity Review Office shall notify the applicant of the review conclusion in written form. • If there is any inconsistency, the ***special review procedure*** shall be followed and the operator shall be notified.
Special Review Procedure	The special review procedure should be completed within 45 working days in general; in case of complex circumstances, 15 working days may be extended.
Supplementary Materials	If the cybersecurity Review Office requires supplementary materials, the time for Critical Information Infrastructure operators and suppliers to submit supplementary materials shall not be included in the review time limit

III. IP protections during the cybersecurity review

The Measures emphasize the business secrets and intellectual property rights protection by imposing confidential obligation upon departments and personnel participating in the network cybersecurity review:

• They shall strictly protect the unpublished materials submitted by CIIO, products and services providers, as well as other unpublished information learned in the review work.
• They shall not disclose these unpublished materials to the unrelated parties or use for purposes other than the cybersecurity review.

If the CIIO or the network product and service provider consider that the relevant departments or personnel fail to perform the confidentiality obligation, they may report to the Cybersecurity Review Office or other relevant departments.

IV. Administrative liabilities for failing to comply with the Measures

In the scenario of CIIO using network products and services without undergoing or has failed to pass cybersecurity review, it might face dual-liability penalty:

Dual-liability Penalty	
Unit liability	**Individual liability**
• The relevant competent department may order the CIIO to cease using the network products and services; • a fine of not less than one time but not more than ten times the purchase amount.	• The person in charge and other directly responsible persons shall be imposed a fine of not less than 10,000 RMB but not more than 100,000 RMB.

We will keep following up the implementation of the Measures and other details. Should you have any inquiries, please contact asiallians@asiallians.com. As always, Asiallians remains at your services and our teams are currently mobilized in all our offices in China, but also in Hong Kong, Taipei.

1. See: http://www.cac.gov.cn/2020-04/27/c_1589535450769077.htm (last visited on May 7, 2020).

2. The 11 departments include: 1) National Development and Reform Commission, 2) Ministry of Industry and Information Technology, 3) Ministry of Public Security, 4) Ministry of National Security, 5) Ministry of Finance, 6) Ministry of Commerce, 7) People's Bank of China, 8) State Administration of market supervision, 9) State Administration of Radio and Television, 10) State Security Administration, 11) State Password Administration

3. CIIO is generally defined as enterprise-operators that run critical information infrastructure. According to the CAC spokesperson's remarks on Measures, operators of important networks and information systems in the fields of telecommunications, radio and television, energy, finance, road and waterway transportation, railway, civil aviation, post, water conservancy, emergency management, health and health, social security, national defense science and technology industry shall comply with obligations under Measures when they are purchasing network products and services. http://www.cac.gov.cn/2020-04/27/c_1589535446378477.htm (last visited on May 7, 2020).

4. Cyber Security Review Office is set up in CAC.

5. Network products and services mainly refer to core network equipment, high-performance computers and servers, large capacity storage equipment, large database and application software, network security equipment, cloud computing services, and other network products and services that have an important impact on the security of key information infrastructure.

6. Cybersecurity Security Review Mechanism Members include all authorities jointly issue the Measures.

Feel free to contact **asiallians@asiallians.com** for more information.