Unofficial Translation.

Cybersecurity Review Measures

(Draft for Comments)

Article 1 These measures are established in accordance with the National Security Law of the People's Republic of China, the Cybersecurity Law of the People's Republic of China and other laws and regulations, with an aim to enhance the secure and controllable level of critical information infrastructure (hereinafter referred to as "CII") and safeguard national security.

Article 2 Purchase of network products and services by CII operators (hereinafter referred to as "operators" or "operator"), which affects or may affect national security, shall be subject to cybersecurity review in accordance with these Measures. Where laws and administrative regulations provide otherwise, such provisions shall prevail.

Article 3 Cybersecurity review shall adhere to the principle of balancing cybersecurity risk prevention with advanced-technology promotion, and increased fairness and transparency with intellectual property protection, as well as to the principle of combining proactive security review with continuous government supervision, and businesses' commitment with public oversight. It shall make comprehensive analysis and judgement

based on, among others, the security level of products and services and the potential risk to national security.

Article 4 Cybersecurity review work shall be conducted under the unified leadership of the Central Cyberspace Affairs Commission.

Article 5 A cybersecurity review working mechanism shall be established by the Cyberspace Administration of China, together with the National Development and Reform Commission, the Ministry of Industry and Information Technology, the Ministry of Public Security, the Ministry of National Security, the Ministry of Commerce, the Ministry of Finance, the People's Bank of China, the State Administration for Market Regulation, the National Radio and Television Administration, the National Administration of State Secrets Protection, and the State Cryptography Administration. The Cybersecurity Review Office, responsible for developing cybersecurity review related rules and procedures, organizing cybersecurity reviews and supervising the implementation of findings, is located at the Cyberspace Administration of China.

Article 6 Where an operator purchases a network product or service, it shall make an ex-ante judgement of the potential security risks that could emerge once the product or service is put into operation, and produce a security risk report accordingly. Where there is a possibility of leading to

(i) complete shutdown or main function failure of CII,

(ii) leakage, loss, corruption or cross-border transfer of massive personal information and important data,

(iii) supply chain security threats compromising the operation and maintenance, technical support and upgrading of CII, or

(iv) other potential risks that could severely jeopardize CII,

the operator shall apply to the Cybersecurity Review Office for a cybersecurity review.

Article 7 With regard to the purchase into which the cybersecurity review is applied for, the operator shall require the product and service provider to cooperate with the review by reflecting such cooperation in the purchase document, contract or through other binding means, and make the Pass finding in the review a precondition for the contract to take effect.

Article 8 When applying for the cybersecurity review, the operator shall submit the following materials:

(i) A declaration;

(ii) The security risk report produced pursuant to Article 6 herein;

(iii) Procurement contract, agreement, etc.;

(iv) Other materials requested by the Cybersecurity Review Office.

Article 9 The Cybersecurity Review Office shall complete its preliminary review within 30 working days after acceptance of the application, with a 15-working-day extension possible for complicated cases.

Article 10 The cybersecurity review shall focus on evaluating the national security risks the purchase could bring by looking at:

(i) The implications of the purchase on the continuous, secure and stable operation of CII, including the possibility of the CII getting manipulated, interfered or its business continuity disrupted;

(ii) The possibility of the purchase leading to the leakage, loss, corruption or cross-border transfer of massive personal information and important data;

(iii) The controllability, transparency and supply-chain security of the product and service, including the possibility of supply disruptions as a result of non-technical factors like political, diplomatic and trade reasons;

(iv) The influence of the purchase on technologies and industries related to national defense, military industry and CII;

(v) The track record of the product and service provider's compliance with national laws and administrative regulations, as well as the responsibilities and obligations it pledges to undertake;

(vi) Whether the product and service provider is funded or controlled by foreign governments;

(vii) Other factors that could compromise CII security and national security.

Article 11 After completing the preliminary review, the Cybersecurity

Review Office shall circulate its suggested finding among members of the cybersecurity review working mechanism for comments. There are 3 types of finding: Pass, Conditional Pass, and Fail.

Members of the cybersecurity review working mechanism shall provide their feedbacks in writing within 15 working days. If unanimous agreement on the suggested finding is reached by the members, the Cybersecurity Review Office shall feed the review finding back to the operator in writing. If not, the Cybersecurity Review Office shall move the purchase in question into special review process and notify the operator.

Article 12 Regarding the purchase cases that have entered the special review process, the Cybersecurity Review Office shall further listen to the opinions of relevant departments, specialized agencies and experts, conduct in-depth analysis and evaluation, and then produce a suggested finding, which shall be reported to the Central Cyber Affairs Commission for approval after being circulated among the members of the cybersecurity review working mechanism for comments.

Article 13 In principle, the special review process shall be completed within 45 working days. Extension is allowed for complicated cases.

Article 14 The operator shall cooperate with Cybersecurity Review Office's request for the submission of supplementary materials. The review period starts as of the date of the submission of supplementary

materials.

The operator shall be responsible for the authenticity of the materials provided. Refusal to provide materials as required or deliberate provision of false materials will lead to the Fail result.

Article 15 Cybersecurity review personnel shall undertake confidentiality obligations for any information learned in the review, and shall not use such information for any purpose other than the cybersecurity review.

Article 16 The operators shall enhance security management, and urge product and service providers to earnestly fulfill the pledges they made during the cybersecurity review.

The Cybersecurity Review Office shall strengthen supervision during and after the review by carrying out spot checks and responding to public reports.

Article 17 Operators that violate the provisions of these Measures shall be dealt with in accordance with Article 65 of the Cybersecurity Law of the People's Republic of China.

Article 18 For the purpose of these Measures, a "CII operator" refers to an operator that has been designated by relevant CII protection departments.

"Secure and controllable" means that the product and service provider does not take advantage of the convenience of providing the products and services to illegally access users' data, illegally control and

manipulate users' devices, or exploit users' dependence on their products and services for unjustified gains or to force users into upgrading.

Article 19 Where a purchase of network products and services or an information technology service is believed by a member of the cybersecurity review working mechanism to affect or possibly affect national security, the Cybersecurity Review Office shall seek approval from the Central Cyber Affairs Commission for a cybersecurity review into such purchase or service, and then organize the review in accordance with these Measures.

Article 20 Where state secret information is involved, relevant national confidentiality provisions shall prevail.

Article 21 These Measures shall come into force as of [DATE], and Measures for the Security Review of Network Products and Services (for Trial Implementation) shall be repealed simultaneously.