



[Security Review Procedures for Online Products and Services](#)

(Draft Seeking Comment)

Released February 04, 2017

In order to enhance the level of “secure and controllability” for online products and services, prevent security risks to supply chains, and safeguard national security and public interests, and as according to the “Cybersecurity Law of the PRC,” the Cyberspace Administration of China issues the “Security Review Procedures for Online Products and Services” for public comment. Relevant units and personnel can submit feedback on this draft before March 04, 2017.

Clause 1 The security and controllability of online products and services directly influences user interests and is related to national security. These measures are formulated in order to enhance the security and controllability of online products and services, prevent security risks to supply chains, and safeguard national security and public interests, and in accordance with the “National Security Law of China” and the “Cybersecurity Law of the PRC.”

Clause 2 Important online products and services that are used by information systems related to national security and public interests should be subject to a cybersecurity audit.

Clause 3 The measures will combine the commitment made by enterprises to work with society on combined supervision, the combination of third party assessments and government regulatory supervision, as well as a combination of laboratory testing, on-site inspections, online monitoring, and background inspections, to implement a cybersecurity review for online products and services and their providers.

Clause 4 Key areas of the review on security and controllability for online products and services will focus on:

- 1) The risk of whether the product and service could be unlawfully controlled, interfered with, or have their operations interrupted;
- 2) Risks associated with the development, payment delivery, or technical assistance of the product or critical components;
- 3) Risks associated with the illegal collection, storage, processing, or use of relevant user information by the product or service provider;
- 4) Risks associated with whether product or service providers use products or services to create user dependency, engage in unfair competition, or harm user interest;
- 5) Other risks that may harm national security or public interests.

Clause 5 The Cyberspace Administration of China in conjunction with other relevant departments will establish a Cybersecurity Review Commission, which will be responsible for deliberating important policies related to the cybersecurity review, unifying and organizing work on the cybersecurity review, and coordinating relevant questions related to the cybersecurity review.

The Cybersecurity Review Office will concretely organize and implement the cybersecurity review.

Clause 6 The Cybersecurity Review Commission will hire relevant experts to organize the commission, and on the basis of a third party review mechanism will carry out comprehensive assessments of security risks for



online products and services, as well as assessments on the “secure and trustworthiness” of product and service providers.

Clause 7 A nationally recognized third party institution for the cybersecurity review will assume responsibility for third party assessment work within the Cybersecurity Review.

Clause 8 As according to the requests of relevant departments, recommendations from national and industry associations, reactions from the market and applications from enterprises, etc., results from the cybersecurity review on online products and services as organized by third parties and experts under the Cybersecurity Review Office, will be released within a defined scope.

Clause 9 Regulatory agencies for finance, telecommunications, energy and other important industries will, as according to the requirements of work related to the cybersecurity review, organize and develop security reviews for online products and services used in their own industries and domains.

Clause 10 Government and Party agencies, as well as key industries must give priority to procuring online products and services that have undergone the cybersecurity review, and may not procure products or services that have not passed this review.

Clause 11 Online products and services used by operators of critical information infrastructure (CII), or which may influence national security, should be subject to this review. Agencies in charge of CII protection will make the determination of whether online products and services used by CII may or may not impact national security.

Clause 12 Third party institutions responsible for the cybersecurity review should be objective, equal, and impartial, and may consult relevant standards, with a focus on controllability, transparency, and trustworthiness, among other areas. These institutions will be responsible for the results of assessments related to providers of online products and services.

Clause 13 Providers of online products and services should cooperate with cybersecurity review work. Third party institutions and other relevant units and personnel have an obligation to keep any information obtained from the security review secure and secret, and are not permitted to use this information for purposes outside of the cybersecurity review.

Clause 14 The Cybersecurity Review Office will issue security assessment reports of online products and services providers on an un-fixed schedule.

Clause 15 The Cyberspace Administration of China is responsible for the interpretation of these regulations.

Clause 16 These regulations will go into effect on XXX (date not determined).