Network Security Review Measures

Dan Young Business Consultancy — www.danyoungcpa.com

Unofficial English translation prepared for reference only. The official Chinese text prevails.

Contents

Table of Contents 1

Chapter I — General Provisions 1

Chapter II — Scope of Application 2

Chapter III — Review Procedures 2

Chapter IV — Review Decisions 2

Chapter V — Special Provisions for Procurement Review 3

Chapter VI — Legal Liability 3

Chapter VII — Supplementary Provisions 3

Adopted by the Cyberspace Administration of China and 12 other departments on December 28, 2021

Effective: February 15, 2022

Table of Contents

- Chapter I — General Provisions
- Chapter II — Scope of Application
- Chapter III — Review Procedures
- Chapter IV — Review Decisions
- Chapter V — Special Provisions for Procurement Review
- Chapter VI — Legal Liability
- Chapter VII — Supplementary Provisions

Chapter I — General Provisions

Article 1 — These Measures are formulated in accordance with the Cybersecurity Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Measures for the Security Review of Critical Information Infrastructure, and other laws and administrative regulations for the purposes of ensuring cybersecurity and national security, safeguarding the lawful rights and interests of citizens, legal persons, and other organizations in cyberspace, and regulating network security review activities.

Article 2 — These Measures shall apply to network security review activities for the following products and services:

Source: https://www.danyoungcpa.com/network-security-review-measures-prc-2021/

(1) Critical network equipment and specialized cybersecurity products purchased by operators of critical information infrastructure;

(2) Network products and services that affect or may affect national security.

Article 3 — Network security review shall adhere to the combination of prevention and control with risk management, combining enterprise commitment with public supervision, and combining industry self-regulation with government regulation.

Chapter II — Scope of Application

Article 4 — Operators of critical information infrastructure that plan to purchase network products and services shall, in accordance with the provisions of these Measures, file an application for network security review where such products and services, when put into use, affect or may affect national security.

Article 5 — A network security review shall focus on assessing the following risks that network products and services may pose to national security:

(1) The risk of illegal control, interference, or disruption of critical information infrastructure after the products are put into use;

(2) The harm caused to critical information infrastructure business continuity due to the suspension of supply of products and services;

(3) The risk of data security and personal information protection after the products are put into use, including the risk of a large amount of personal information and important data being stolen, leaked, destroyed, illegally used, or illegally exported;

(4) The risk that national security interests are harmed due to political, diplomatic, trade, or other factors;

(5) Other factors that may endanger the security of critical information infrastructure and national security.

Article 6 — Operators of critical information infrastructure shall, when purchasing network products and services, predict the possible risks to national security following the products being put into use. Where national security is affected or may be affected, an application for cybersecurity review shall be filed with the Cybersecurity Review Office.

Chapter III — Review Procedures

Article 7 — The cybersecurity review shall generally be completed within 30 working days from the date of acceptance of the application. If the circumstances are complex, the review period may be extended by 15 working days. If the parties concerned need to supplement materials, the time for supplementation shall not be counted in the review period.

Article 8 — During the cybersecurity review process, the Cybersecurity Review Office may require the product and service provider to provide supplementary materials. The product and service provider shall provide such supplementary materials in a timely manner.

Article 9 — The Cybersecurity Review Office may, as needed, conduct technical testing and inspection of products and services, and the relevant costs shall be borne by the applicant.

Article 10 — The parties participating in the cybersecurity review shall keep confidential the trade secrets and personal privacy that come to their knowledge in the review process, and shall not disclose them or illegally provide them to others.

Chapter IV — Review Decisions

Source: https://www.danyoungcpa.com/network-security-review-measures-prc-2021/

Article 11 — Based on the review findings, the Cybersecurity Review Office shall make one of the following decisions:

(1) Passing the review: where the product or service does not pose a security risk, the purchasing activity may continue;

(2) Failing the review: where the product or service poses a security risk that cannot be eliminated, the use of such product or service is prohibited;

(3) Conditional approval: where the risk can be mitigated through supplemental measures, the use is permitted subject to specific conditions.

Article 12 — For a conditional approval decision, the operator shall strictly implement the additional conditions specified in the decision. The Cybersecurity Review Office shall supervise the implementation.

Chapter V — Special Provisions for Procurement Review

Article 13 — Where the network security review involves procurement of products and services from foreign countries, the review shall take into full consideration the national security risk factors that may arise from international political, economic, and trade relations.

Article 14 — For network products and service providers that are under the control or influence of foreign governments, special attention shall be paid to assessing the risks of data being accessed, controlled, or manipulated by foreign governments, and the risks of supply chain disruption caused by international political, economic, and trade relations.

Chapter VI — Legal Liability

Article 15 — Where an operator of critical information infrastructure, in violation of these Measures, uses network products or services that should have undergone but have not undergone cybersecurity review, or fails to implement the additional conditions specified in the review decision, the Cybersecurity Review Office shall order the operator to cease use and impose correction within a specified period. The relevant competent department shall impose penalties in accordance with the provisions of the Cybersecurity Law.

Article 16 — Where an operator of critical information infrastructure, in violation of these Measures, provides false materials in the cybersecurity review, the Cybersecurity Review Office shall order correction within a specified period. Where the circumstances are serious, the operator shall be subject to administrative penalties in accordance with the law.

Article 17 — Where a product or service provider fails to cooperate with the investigation and evidence collection during the cybersecurity review or provides false materials, the relevant competent department shall impose penalties in accordance with the law.

Chapter VII — Supplementary Provisions

Article 18 — The cybersecurity review of network products and services referred to in these Measures shall not replace the daily cybersecurity management and protection obligations of operators of critical information infrastructure.

Article 19 — The Cyberspace Administration of China shall be responsible for interpreting these Measures.

Article 20 — These Measures shall take effect on February 15, 2022. The Measures for the Security Review of Network Products and Services (for Trial Implementation) issued on May 2, 2017, shall be repealed simultaneously.

Source: https://www.danyoungcpa.com/network-security-review-measures-prc-2021/

Disclaimer: This English translation is provided for informational and reference purposes only. It is not an official translation and has no legal effect. The original Chinese text of the Measures shall prevail in all legal matters. Operators of critical information infrastructure and network product and service providers should consult qualified legal professionals for advice on specific cybersecurity review matters. While every effort has been made to ensure accuracy, no warranty is given as to the completeness or accuracy of this translation. Dan Young Business Consultancy assumes no liability for any errors, omissions, or reliance on this translation.