Brief Review of Provisions on Administration of Security Vulnerabilities in Network Products

Authors: Kevin DUAN | Angus XIE

On July 12, the Ministry of Industry and Information Technology ("**MIIT**"), the Cyberspace Administration of China ("**CAC**") and the Ministry of Public Security jointly promulgated the *Provisions on Administration of Security Vulnerabilities in Network Products* (the "**Provisions**"), which will come into effect as of September 1, 2021. These provisions add new rules for cybersecurity—a field that has recently attracted much attention.

According to the Provisions, CAC will be responsible for coordinating the supervision of network product security vulnerabilities, MIIT will be responsible for the comprehensive supervision of network product security vulnerabilities as well as the supervision and management of network product security vulnerabilities in the telecommunications and Internet industries, and the Ministry of Public Security will be responsible for the supervision and management of network product security vulnerabilities and take actions against illegal and criminal activities committed by taking advantage of network product security vulnerabilities in accordance with the law.

The Provisions will apply to network product providers (including hardware and software products), network operators, and organizations or individuals that engage in the discovery, collection, and publication of information regarding network product security vulnerabilities. The Provisions stipulate legal obligations for these three categories of persons subject and relevant consequences for violating those obligations. Further, the Provisions also prohibit other organizations and individuals from engaging in any activities that involve: endangering cybersecurity by taking advantage of network product security vulnerabilities; illegally collecting, selling, or publishing information on network product security vulnerabilities; or providing technical support, advertising, or settlement services to entities that engage in activities that endanger cybersecurity by taking advantage of network product security vulnerabilities.

Given the *Measures for Cybersecurity Review (Revision Draft for Comment)*, which emphasize a notification regime for cybersecurity review and considers the risk of data leakage, theft, and damage potentially arising from data processing activities, the Provisions, in relevant part, provide a strong reference for enterprises to conduct internal reviews and benchmarking in view of cybersecurity reviews. (For more insights, please see Han Kun's *Analysis of Revised Draft Cybersecurity Review Measures*.

In the table below we summarize the relevant provisions of the Provisions that apply to each category of persons subject:

Persons Subject	Encouraged Activities	Legal Obligations	Consequences for Breach
Network product providers	Establish a reward mechanism for providing network product security vulnerabilities and give rewards to any organization or individual that discovers and notifies of network product security vulnerabilities.	■ Establish and maintain open channels for receiving reports on security vulnerabilities in network products, and keep logs of reported security vulnerabilities for no less than six months; ■ Upon detection or becoming aware of security vulnerabilities in provided network products, immediately organize to verify suspected vulnerabilities, assess the extent of damage and scope of impact, and organize to rectify such vulnerabilities in a timely manner; ■ File relevant security vulnerabilities within two days with the Network Security Threat and Vulnerabilities Information Sharing Platform of the Ministry of Industry and Information Technology; ■ Notify the relevant upstream providers if there are upstream products or components that have security vulnerabilities; ■ Notify downstream users (including downstream manufacturers) of potential security vulnerabilities and rectification methods and provide technical support if it is necessary for product users (including downstream manufacturers) to take	■ Be ordered to make corrections and given warnings; ■ Be imposed with a fine of CNY50,000 to CNY500,000 if they refuse to make corrections, or severe consequences are caused therefrom such as endangering cybersecurity; ■ The person directly in charge shall be subject to a fine of CNY10,000 to CNY100,000.

Persons Subject	Encouraged Activities	Legal Obligations	Consequences for Breach
		remedial measures such as software and firmware upgrades.	
Network operators		■ Establish and maintain open channels for receiving reports on network security vulnerabilities, keep logs of reported security vulnerabilities for no less than six months; ■ Upon detection or becoming aware of any security vulnerabilities in networks, information systems and equipment, take immediate measures to verify such vulnerabilities and repair the same in a timely manner.	General network operators: ■ Be ordered to make corrections and given warnings; ■ Be imposed with a fine of CNY10,000 to CNY100,000 if they refuse to make corrections, or severe consequences are caused therefrom such as endangering cyber security; ■ The person directly in charge shall be subject to a fine of CNY5,000 to CNY50,000; Critical information infrastructure operators: ■ Be ordered to make corrections and given warnings; ■ Be imposed with a fine of CNY10,000 to CNY1,000,000 if they refuse to make corrections, or severe consequences are caused therefrom such as endangering cyber security; ■ The person directly in charge shall be subject to a fine of CNY10,000 to CNY100,000.
Organizations or individuals engaged in activities such		■ Establish a platform for collecting network product security vulnerabilities and file the platform with MIIT; and ■ Establish and maintain open channels for	■ Be ordered to make corrections and given a warning; ■ Be imposed with a fine of CNY10,000 to CNY100,000 if they refuse to make

Persons Subject	Encouraged Activities	Legal Obligations	Consequences for Breach
as discovering, collecting and disclosing security vulnerabilities in network products		receiving reports on security vulnerabilities in network products, and keep logs of reported security vulnerabilities for no less than six months; ■ Strengthen internal management and take measures to prevent the leakage and unlawful disclosure of vulnerability information; ■ Publication of vulnerability information to the public through network platforms, media, meetings, contests or otherwise shall be consistent with principles of necessity, authenticity, objectivity and conducive to the prevention of cybersecurity risks; and ■ Shall not publicize vulnerability information before the network product provider takes measures to rectify the security vulnerabilities in the network products; if it is deemed necessary to publicize such information in advance, negotiate and cooperate with the network product provider to conduct a joint assessment, and report the same to the MIIT and the Ministry of Public Security, which shall be responsible for the publication of such information after assessment; ■ Shall not publicize details of security vulnerabilities in networks, information	corrections, or severe consequences are caused therefrom such as endangering cyber security; ■ Be ordered by the competent department to suspend the relevant business, cease business for rectification, close websites, and revoke relevant business permits or business licenses; ■ The person directly in charge and any other person directly liable shall be subject to a fine of CNY5,000 to CNY50,000.

Persons Subject	Encouraged Activities	Legal Obligations	Consequences for Breach
		systems, and equipment that are currently in use by network operators; ■ Shall not deliberately exaggerate the hazards and risks of security vulnerabilities in network products, and shall not conduct illegal or criminal activities by using the information of security vulnerabilities in network products, such as malicious speculation, fraud, extortion, etc.; ■ Shall not publicize or provide programs and tools specifically for use in activities that endanger cybersecurity by taking advantage of security vulnerabilities in network products; ■ Shall publicize security vulnerability remedial or preventive measures at the same time when publicizing security vulnerabilities in network products; ■ Shall not publicize security vulnerabilities in network products during major national events without the approval of the Ministry of Public Security; and ■ Shall not provide undisclosed information about security vulnerabilities in network products to overseas organizations or individuals other than to the network product provider.	

Persons Subject	Encouraged Activities	Legal Obligations	Consequences for Breach
Other organizations or individuals	■ Notify network product providers of security vulnerabilities in their products; ■ File security vulnerabilities information of network products with the Network Security Threat and Vulnerabilities Information Sharing Platform of the Ministry of Industry and Information Technology, the Vulnerabilities Platform of the National Network and Information Security Information Notification Center, the Vulnerabilities Platform of the National Computer Network Emergency Response Technical Team/Coordination Center, and the Vulnerabilities Database of the China Information Security Assessment Center.	■ Shall not engage in activities endangering cybersecurity by using security vulnerabilities in network products; and ■ Shall not unlawfully collect, sell or publicize information of security vulnerabilities in network products; and ■ Shall not provide technical support, advertising and promotion, payment or settlement services or any other assistance to any other person who they know to be using security vulnerabilities in network products to engage in activities that endanger cybersecurity.	**Where the case does not constitute a crime:** ■ Be confiscated of illegal gains, detained for fewer than 5 days; may concurrently be subject to a fine of CNY50,000 to CNY500,000; ■ In serious cases, be detained for 5 to 15 days and subject to a fine of CNY100,000 to CNY1,000,000. **Where an entity commits any of the acts specified in the preceding paragraph:** ■ Be confiscated of illegal gains; ■ Be subject to a fine of CNY100,000 to CNY1,000,000; ■ The person directly in charge and any other person directly liable shall be penalized in accordance with the provisions of the preceding paragraph. **Relevant personnel:** ■ Any person who has been subject to public security administration penalty shall not serve in key positions concerning cyber security management and network operation within 5 years; and ■ Any person who has been subject to criminal penalty shall not serve in key positions concerning cyber security management and network operation for life.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123
Email: kevin.duan@hankunlaw.com

Angus XIE

Tel: +86 10 8524 5866
Email: angus.xie@hankunlaw.com