COVINGTON

China Seeks Public Comments for Draft Regulations on Cybersecurity Multi-level Protection Scheme to Implement the Cybersecurity Law

July 5, 2018

Data Privacy and Cybersecurity

On June 27, 2018, China's Ministry of Public Security ("MPS") released for public comment a draft of the Regulations on Cybersecurity Multi-level Protection Scheme ("the Draft Regulation"). The highly anticipated Draft Regulation sets out the details of an updated Multi-level Protection Scheme, whereby network operators (defined below) are required to comply with different levels of protections according to the level of risk involved with their networks. The comment period ends on July 27, 2018.

China's Cybersecurity Law ("CSL"), which took effect on June 1, 2017, requires the government to implement a Multi-level Protection Scheme ("MLPS") for cybersecurity (Article 21). The Draft Regulation, a binding regulation once finalized, echoes this requirement and provides guidance for network operators to comply with the Cybersecurity Law.

What is the MLPS?

In 2007, MPS (the lead agency tasked with combating cyber-crime and protecting cybersecurity) promulgated the initial MLPS regulation, entitled *Administrative Measures for the Multi-level Protection Scheme of Information Security*.

Designed to secure critical Chinese infrastructure information systems, the initial MLPS is a framework that classifies information systems physically located in China according to their relative impact on national security, social order, and economic interests if the system is damaged or attacked. The classification levels range from one to five, one being the least critical and five being the most critical. Information systems that are classified (initially self-assessed and proposed by operators and then confirmed by MPS) at level 3 or above are subject to enhanced security requirements.

The CSL incorporated the MLPS into its regulatory framework and designated it, as well as the protection of Critical Information Infrastructure ("CII"), as two fundamental schemes to protect network security in China. Under Article 21, "network operators," broadly defined to include all entities using a network (including the Internet) to operate or provide services, will be subject to different cybersecurity requirements corresponding to their MLPS classification level. Also, the MLPS protection was expanded from "information systems" to "networks."

What classification framework does the Draft Regulation propose?

When the CSL was promulgated, MPS was tasked with updating the MLPS to fit into the broader cybersecurity framework established by the CSL. As "MLPS 2.0," the Draft Regulation still proposes to follow the classification framework established by the initial MLPS regulation, but adds more detail on the classification process and other requirements for operators at different levels.

All network operators are responsible for determining the appropriate security level for their networks at the design and planning stage based on the chart below, taking into account the functions of the network, scope and targets of service, and the types of data being processed. When network functions, services scope and types of data processed are significantly changed, network operators are required to re-assess their classification level.

Damaged interest (if attacked or damaged)	**Potential degree of damage**		
	General Damage	Significant Damage	Especially Significant Damage
Legitimate interest of companies, legal persons and other organizations	Level 1	Level 2	Level 3
Social order and public interest	Level 2	Level 3	Level 4
National security	Level 3	Level 4	Level 5

Terms such as "national security" and what damage is considered "significant" or "especially significant" are not defined in the Draft Regulation. Further guidance on how to assess the impact level of networks is expected to be provided by a national standard, *Information Security Technology - Guidelines for Grading of Cybersecurity Multi-level Protection*. A draft version of this standard was issued by National Information Security Standardization Technical Committee on January 19, 2018 for public comments.

For networks classified level 2 or above, the operator is required to arrange for "expert review" of its classification level. If the operator is subject to the oversight of an industry regulator, the regulator has to approve the classification result. After the network operator determines the classification level, the network operator must submit its classification result with MPS within 10 days. MPS will issue the filing certificate to operators within 10 days if it determines the classification is accurate and supported by documents. Although there is no prescribed timeframe to complete this process, a network operator should presumably receive the MPS determination before the applicable network(s) is turned on. It is unclear how MPS will treat pre-existing networks and whether (or how long) the existing operators will be granted a grace period to complete the filing process.

The expert review (and the approval from regulators, if applicable) was not required by the initial MLPS regulation for operators at level 2 or below and the Draft Regulation does not elaborate on the process.

What are the general cybersecurity requirements imposed on network operators?

The Draft Regulation sets out requirements generally applicable to all network operators regardless of classification level, which largely track the requirements under Article 21 of the CSL.

As such, network operators are required to have a cybersecurity program that specifically accounts for the following:

- personnel management and training related to the implementation of cybersecurity measures;
- management of data rooms, servers and devices;
- prevention of malware and cyberattacks;
- monitoring and logging the network status, including retaining relevant logs—for at least six months—that can be used to trace illegal activities;
- data backup;
- encryption to protect personal information;
- measures to identify, block and eliminate illegal content in the network;
- access management and authentication, including measures to allow user real identity check; and
- security incidents reporting.

All network operators are required to conduct a self-review on their implementation of the cybersecurity MLPS system and the status of their cybersecurity at least once per year and should timely rectify identified risks and report such risks and remediation plans to MPS with which the operator is registered.

What security incident reporting obligations now exist?

For security incident reporting, the Draft Regulation briefly mentions that network operators are required to report incidents within 24 hours to MPS. Although the Draft Regulation does not elaborate the reporting process or the information required for such notifications, this requirement imposes a new reporting timeline on network operators because the CSL, itself, does not have a specific time frame for reporting. The CSL generally requires network operators to notify an incident to regulators and affected individuals when there has been actual or potential "leakage, damage, or loss" of *personal data*. It is not clear whether the Draft Regulation would subject a network operator to this reporting obligation if the breach occurs outside of China or within their data processors' network or to broader types of incidents (e.g., "potential" breaches of personal data or incident that do not involve personal data).

In addition, network operators will also have to reconcile the Draft Regulation will two other documents that contain references to incident reporting obligations of network operators. The national standard—*Information Security Technology - Personal Information Security Specification* ("Standard")—requires all network operators to adhere to the *National Network*

Security Incident Contingency Plan released by Cyberspace Administration of China ("CAC") for notification of incidents involving personal data to authorities. In addition, the Ministry of Industry and Information Technology ("MIIT") issued a *Response Plan for Unexpected Cybersecurity Incidents on Public Internet* ("MIIT Response Plan") requiring operators of "public Internet" (covering providers offering basic telecommunication services, domain name registration services and Internet services to the public) to notify MIIT of the security incidents. Again, no specific time period for reporting was expressly mentioned under the Standard or the MIIT Response Plan. It is unclear how various regulations and national standards will interact and how companies can comply with multiple requirements in practice.

What are the special cybersecurity requirements imposed on operators of networks graded level 3 and above?

Additional requirements apply for operators of networks graded level 3 and above—some of them are repetitive or overlap with general requirements above. These include:

- appointing a member of [senior] management to be responsible for cybersecurity;
- establishing a change management program;
- formulating an overarching cybersecurity plan and integrity protection strategy, which shall be reviewed and approved by "professional technical personnel";
- conducting background checks, including verifying "professional certification" of key individuals responsible for managing cybersecurity;
- conducting "security management" on organizations and personnel that provide network design, construction, operation and maintenance and technical support;
- monitoring network status, network traffic, user behavior, security incidents, and connecting the monitoring network with "MPS networks";
- implementing redundancy, back-up and recovery measures for important network equipment, communication lines and systems;
- conducting annual classification testing on networks and reporting the results and relevant rectification measures to MPS and relevant regulators;
- engaging testing agencies to conduct testing before launch of the network.

Note that new level 3 networks shall be tested by MLPS testing agencies accredited by MPS (a list of accredited testing agencies available here) before they can come online. (By way of comparison, network operators of networks level 2 and below can test their own new network before it comes online.) Operators of networks graded level 3 and above are also required to formulate cybersecurity emergency plans and regularly carry out cybersecurity emergency response drills (e.g., table top exercises).

Meanings of certain terms in these requirements, such as what qualifies as an "emergency" and what the appropriate interval for "regularly" carrying out drills, are at this point still not clear and may require further interpretation. Also, several requirements, such as connecting with "MPS networks" and reporting the substantive testing results (potentially including vulnerabilities) to MPS, are less clear in meaning and could be controversial, depending on how these requirements are implemented in practice.

What are other key requirements for operators of networks graded level 3 and above?

Products and service procurement

The Draft Regulation requires that operators of networks graded level 3 and above should use network products and services that match their classification level (as filed and approved by MPS), presumably by procuring products and services certified by MPS. In particular, for network products "used for important parts of networks," operators should engage accredited testing institutions to conduct tests for such products. The meaning of "important parts of networks" is yet unclear.

Also, if the procurement of network products and services may affect national security (defined expansively as the security of the regime, sovereignty, unity, territorial integrity, social welfare, sustainable economic and social development, and other major interests of China), the products and services must also go through a national security review conducted by the CAC, together with other agencies under the State Council.

Remote technical maintenance

Technical maintenance of networks graded level 3 and above is required to be conducted within China and overseas remote technical maintenance will not be permitted in general. If remote maintenance performed outside of China is necessary for business reasons, the maintenance must go through unspecified cybersecurity assessment and risk-management measures must be implemented. Operators are also required to record and retain the maintenance logs and provide them to MPS upon request.

Encryption protection

Network Operators for level 3 and above networks are required to adopt "encrypted protection" and use encryption technologies, products and services approved by Chinese encryption regulators. They are also required to engage accredited encryption security testing institutions by encryption regulators to carry out security assessment and conduct annual assessment after the network is launched for operation. The security assessment results should be filed for record with MPS and encryption regulators.

Defensive and offensive cybersecurity activities organized by foreign organizations

The Draft Regulation states that "personnel in key positions" and "personnel providing security services" at operators at level 3 and above are not allowed to attend offensive and defensive activities organized by foreign organizations "without authorization." It is unclear what activities "organized by foreign organizations" this provision is referring to and whether this restriction on "personnel providing security services" would extend to service providers.

Other aspects of the Draft Regulation

Data protection obligations

The Draft Regulation reiterate the data protection obligations of network operators on the collection, use, processing, and disclosure of personal data, which track the requirements under the CSL.

Technical assistance to law enforcement

Consistent with the requirement under the CSL, the Draft Regulation also requires network operators to provide support and assistance for national security and criminal investigation activities conducted by MPS and national security authorities. Similar to the CSL, the process and full extent of this support is not provided.

Cybersecurity protection on classified networks

A separate chart of the Draft Regulation specifies the cybersecurity protection requirements on "classified networks", which likely refer to networks that contain China's state secrets. Operators of classified networks could face more stringent cybersecurity and encryption requirements.

Enforcement and Liability

The Draft Regulation stipulates a wide array of investigative powers of MPS and sanctions for non-compliant companies, ranging from on-site inspection, investigation, "summon for consultation" to monetary fines and criminal liability. For instance, among other things, MPS has the power to:

- conduct the security inspection on networks graded level 3 and above at least once per year by itself or together with other industry regulators;
- if necessary, order network operators to block the information transmission, suspend network operations and backup relevant data during the process of security incident investigation;
- if the network vulnerabilities will affect national security, social order or public interest, order network operators to disconnect networking and shut down the relevant facilities; and/or
- interview the network operator's China legal representative or senior management responsible for cybersecurity, or industry regulator if security vulnerabilities are identified or security incidents occurred.

* * * * *

Multinational companies operating in China may wish to closely follow developments relating to the Draft Regulation and understand how recent developments may affect their business operations. Companies have until July 28 to provide feedback to the Chinese government on possible amendments.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our firm:

Tim Stratford	+86 10 5910 0508	tstratford@cov.com
Yan Luo	+86 10 5910 0516	yluo@cov.com
Ashden Fein	+1 202 662 5116	afein@cov.com
Ted Karch	+44 20 7067 2346	tkarch@cov.com