



Llinks Corporate and M&A Bulletin
October 2018

上海
上海市银城中路 68 号
时代金融中心 19 和 16 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话：+852 2969 5300
传真：+852 2997 3385

伦敦
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

SHANGHAI
19/F&16/F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING
4/F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

HONG KONG
27/F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2969 5300
F: +852 2997 3385

LONDON
1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

master@llinkslaw.com

MPS Issued MLPS Regulation to Strengthen Cyber Security Protection Requirements in China

By Xun Yang | Jianqi Yang

The PRC Ministry of Public Security (the “MPS”) released the *Draft Regulations on Multi-level Protection of Cyber Security* (the “MLPS Regulation”) for public consultation on 27 June 2018. The MLPS Regulation is supposed to become an implementing rule of the PRC Cyber Security law effective in June 2017. It also aims to replace the *Administrative Measure for Multi-level Protection of Information Systems* (the “MLPS Measure”) issued by the MPS jointly with other authorities in 2007, which was not well enforced. This essay will briefly discuss the key developments of MLPS Regulation from the MLPS Measure and its potential implications on the network operators in China.

1. Overview of MLPS Regulation

Source of Laws

Although MPS is leading the drafting of the MLPS Regulation, according to its name, the MLPS Regulation is expected to be adopted by the State Council and then issued as an administrative regulation. Different from managerial measures which only bind the government agencies which

.....
If you would like other Llinks publications, please contact:

Roy Guo: (86 21) 3135 8756
Publication@llinkslaw.com

Llinks Law Offices
www.llinkslaw.com

MPS Issued MLPS Regulation to Strengthen Cyber Security Protection Requirements in China

issue the measures, administrative regulations bind all government agencies, private parties, and courts..

The MLPS Measure provides for a multi-level protection scheme (“**MLPS Scheme**”), by which network operators are required to assess the security levels which their networks fall into and apply to such networks technical and managerial standards corresponding to such levels. However, the MLPS Measure is a ministerial rule made by MPS, which, according to the PRC Legislation Law, is not a formal source of laws. In theory, the MLPS Measure only provides for how MPS will exercise its power to protect public security in the cyberspace. Absent clear authorization from congress-made laws when the MLPS Measure was promulgated, it cannot directly impose obligations on private parties to implement the MLPS Scheme. As a result, the MLPS Measure was not strictly enforced until the effectiveness of the Cyber Security Law. Article 21 of the Cyber Security Law provides that a multi-level protection scheme will be implemented to protect cyber security. This article essentially endorses the MLPS Scheme as set out in the MLPS Measure and, consequently, MPS started to enforce the MLPS Measure in practice.

MPS is not the only government agency regulating cyber security matters. Regulators of various industries have the responsibilities to enforce cyber security requirements in their respective industrial area. The upgrade of the MLPS Scheme onto an administrative regulation level is one of the efforts to coordinate the enforcement of cyber security standards by all government agencies. If the MLPS Regulation is adopted by the State Council and finally issued in the form of an administrative regulation, all government agencies and the courts will be required to respect it.

Scope of Application

The MLPS Regulation expands the scope of application of the MLPS Scheme. Generally speaking, operators of all types of networks, including computer networks and mobile networks, are required to implement the MLPS Scheme.

The MLPS Measure provides that “operators of information systems” are required to implement the MLPS Scheme. It, however, does not clearly define the term “operators of information systems.” MPS, jointly with other government agencies, issued the *Opinions for Performing the Works Relating to Multi-level Protection of Information Systems* in September 2004, in which the term ‘information system’ is defined as the systems or networks that are made of computers (emphasis added) and related equipment to store, transmit and process in accordance with certain practical purpose and rules.

The draft MLPS Regulation provides that all network operators are required to implement the MLPS Scheme and the term “network” is defined under the MLPS Regulation as a system that consists of computers or other information terminals (emphasis added) and related equipment to collect, store, transmit,

MPS Issued MLPS Regulation to Strengthen Cyber Security Protection Requirements in China

exchange and process information according to certain rules and procedures, the same as the definition under the Cyber Security Law. As such, the scope of application of the MLPS Regulation is expanded to capture the operations of mobile networks and other possible public networks, in addition to computer networks. This expansion reflects obviously the fast development of mobile applications, with an allowance to cover all information systems which may be developed in the future.

2. Strengthened Cyber Security Standards

Generally speaking, under a MLPS Scheme, network operators are required to (i) assess the security levels of their networks according to the criticalness of such networks and the sensitivity of the data processed in such networks; (ii) apply technical and managerial measures to their networks corresponding to the security levels; and (iii) have their networks certified by testing institutions and file the certification reports with the government. The MLPS Regulation strengthened these requirements.

Change of Five Security Protection Levels

Both the MLPS Measure and the MLPS Regulation divide networks into five security levels according to the criticalness of these networks, i.e., the level of impacts on private rights, public interests, and national security should the relevant networks be prejudiced. Comparing to the MLPS Measure, the MLPS Regulation imposes higher security standards.

Please see below criticalness criteria and the corresponding security levels under the MLPS Measure and MLPS Regulation.

Criticalness			Security Level under MLPS Measure	Security Level under MLPS Regulation
Impact on private rights	Impact on public interest	Impact on national security		
Causing damages	No impact	No impact	Level 1	Level 1
Causing serious damages	Causing damages	No impact	Level 2	Level 2
Causing particularly serious damages	/	/	Level 2	Level 3
/	Causing serious	Causing damages	Level 3	Level 3

MPS Issued MLPS Regulation to Strengthen Cyber Security Protection Requirements in China

Criticalness			Security Level under MLPS Measure	Security Level under MLPS Regulation
Impact on private rights	Impact on public interest	Impact on national security		
	damages			
/	Causing particularly serious damages	Causing serious damages	Level 4	Level 4
/	/	Causing particularly serious damages	Level 5	Level 5

Attention should be given to security level 3 under the MLPS Regulation. If a failure of or leakage from a network may cause particularly serious damages to private interest, such network will be considered falling within security level 3 even if it does not impact public interests or national security. The same network would only be considered security level 2 under the MLPS Measure.

This change has significant implications. Quite a number of networks operated in China possess and process significant amount of personal information. Consequently, the security of these networks is critical for protecting private interest but probably not quite relevant to public interest or national security. These networks fall with security level 2 under the current MLPS Measure but would fall within security level 3 under the MLPS Regulation should it be adopted in its current form. As a result, stricter security and managerial rules would apply.

Strengthened Procedural Rules for MLPS Scheme

The MLPS Regulation strengthens the procedural rules for the MLPS Scheme as provided for under the MLPS Measure.

Firstly, network operators are required to determine the security level of their networks at an earlier stage. According to Article 11 of the MLPS Measure, operators of information systems are required to determine the MLPS level of their networks when they completed the development of information systems. However, the MLPS Regulation requires that network operators to determine the security measures during the design of the networks.

Secondly, MLPS Regulation introduces a classification review and verification procedure. According to the MLPS Regulation, network operators which consider that their networks be classified as security level 2 or above must engage experts to review their classifications and, then, to report such classifications and

MPS Issued MLPS Regulation to Strengthen Cyber Security Protection Requirements in China

expert review to their regulators for verifications.

Thirdly, the MLPS Regulation requires that operators of networks at security level 2 or above to file their classifications with the local public security bureaus. This requirement is stricter than that under the MLPS Measure where only operators of networks falling with security 3 or above are required to file their classifications with the local public security bureaus.

Fourthly, the MLPS Regulation requires that operators of networks at security level 2 or above test the security of their networks before the official launch of the networks. If the relevant networks fall within security level 3 or above, such testing must be performed by certified external institutions.

Security Measures

Network operators are required to adopt certain protective measures corresponding to the security levels of their networks. These security measures under the MLPS Regulation are much more comprehensive and stricter than those under the MLPS Measure. Under the MLPS Regulation, these protective measures are divided into two categories: general security measures and special security measures. The former refers to the security measures all the network operators must adopt and the latter refers to the measures which operators of networks at security level 3 or above must adopt.

The general security measures include:

- To designate a person or a team who is responsible for network security protections;
- To establish and implement a responsibility system for the network protection;
- To deliver training relating to cyber security for employees;
- To formulate implementing rules and procedures to maintain the security of networks;
- To adopt managerial and technical measures to verify identities of users and prevent malicious code;
- To monitor the operation of networks and to record cyber security incidents and attempted attacks;
- To preserve the network operation records relating to criminal activities for at least six months;
- To protect personal information collected or generated during the operation of networks;
- To adopt technical measures to find out or to block illegal information;
- To adopt managerial and technical measures to prevent illegal information from being spread to a wide extent and to prevent evidence for violations and offences from being destroyed or lost;
- To perform filing and real name verification obligations; and
- To report cyber security incidents within 24 hours to the relevant authorities.

MPS Issued MLPS Regulation to Strengthen Cyber Security Protection Requirements in China

The special security measures include:

- To establish a specific department responsible for the management of cyber security matters and to formulate an escalating approval procedure relating to operation of networks;
- To formulate and implement an overall plan for cyber security and a strategy for security protections;
- To conduct background check against cyber security managers and other key personnel involved in operating networks;
- To formulate a management system for the relevant agencies and individuals providing services relating to the design, development, operation and technical support to the networks;
- To build and operate a system for monitoring cyber security accidents, which system must be connected to relevant public security bureaus;
- To implement redundancy, back-up and recovery measures for important network equipment, communications connections and systems; and
- To carry out security level assessment at a regular interval and report the result of such assessment to the relevant public security bureaus and industrial regulators.

Reporting Obligation

Under current PRC legal framework on cyber security, network operators are imposed a number of reporting obligations. For example, network operators are report any malicious code or any illegal information found on the networks. They are also required to report any significant data leakage from their networks. Similar reporting obligations exist in industry-specific regulations. For example, financial institutions are requires to report to their regulators any failure of their networks.

The MLPS Regulation imposes a higher reporting obligation on operators of network t security level 3 or above, that I the operator must build and operate a monitoring system which my detect network incidents occurred on their platforms and report the incident to the relevant public security bureau on a real time basis. In other words, the monitoring system must be connected to the local public security bureaus' system.

Conclusion

The issuance of the draft MLPS Regulation is an effort of China government, especially of the public security department, to strengthen the enforcement in the cyber security areas. If the MLPS Regulation is adopted in its current form, there would be following three implications:

- (1) The public security bureau will become a key enforcement agent to supervise cyber security

MPS Issued MLPS Regulation to Strengthen Cyber Security Protection Requirements in China

protections by network operators, including those operators engaged in a regulated business (such as the finance business). All government agencies, such as the banking regulators, will be required to respect the MLPS Scheme developed by the public security department and cooperate with the enforcement of the MLPS Scheme.

- (2) The security standards which network operators are required to meet under the MLPS Regulation is higher and the security protection obligations which network operators are required to perform under the MLPS Regulation are stricter. Network operators will need to invest more resources to maintain the security of their networks.
- (3) The MLPS Regulation gives rise to great opportunity for network security testing institutions. Under the MLPS Regulation, operators of networks concerning no national security but only public interest may be required to have their networks tested, certified and filed before the launch of the networks. This means greater demand for security testing services.

MPS Issued MLPS Regulation to Strengthen Cyber Security Protection Requirements in China

Contact Details

If you would like to know more information about the subjects covered in this publication, please feel free to contact the following people or your usual Llinks contact.

Author	
Xun Yang Tel: +86 21 3135 8799 xun.yang@llinkslaw.com	
Shanghai	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Bernie Liu Tel: +86 21 3135 8678 bernie.liu@llinkslaw.com
Selena She Tel: +86 21 3135 8770 selena.she@llinkslaw.com	Nicholas Lou Tel: +86 21 3135 8783 nicholas.lou@llinkslaw.com
Dali Qian Tel: +86 21 3135 8676 dali.qian@llinkslaw.com	Kenneth Kong Tel: +86 21 3135 8777 kenneth.kong@llinkslaw.com
David Wu Tel: +86 21 6043 3711 david.wu@llinkslaw.com	David Pan Tel: +86 21 3135 8701 david.pan@llinkslaw.com
Elyn Jiang Tel: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
Beijing	
David Yu Tel: +86 10 8519 2266 david.yu@llinkslaw.com	Bernie Liu Tel: +86 10 8519 2266 bernie.liu@llinkslaw.com
Yuhua Yang Tel: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
Hong Kong (in Association with Vivien Teu & Co LLP)	
David Yu Tel: +86 21 3135 8686 david.yu@llinkslaw.com	Sandra Lu Tel: +86 21 3135 8776 sandra.lu@llinkslaw.com
London	
Yuhua Yang Tel: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	