LLINKS Law Offices
通力律师事务所

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

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

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +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 2592 1978
传真：+852 2868 0883

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

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

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

www.llinkslaw.com
master@llinkslaw.com

Llinks Corporate and M&A Bulletin
May 2019

An Overview of Key Points and Compliance Advice for MLPS 2.0

By David Pan | Susan Deng

On May 13, 2019, Multi-level Protection Scheme ("MLPS") 2.0 was officially issued, two years after the issuance of its draft for comments. Compared to MLPS 1.0, MLPS 2.0 made considerable changes, focusing on active defense protection mechanism and the full coverage of the protected subject. MLPS 2.0 will take effect from December 1, 2019. This article will analyze the cybersecurity multi-level protection scheme under MLPS 2.0 and the difference between MLPS 1.0 and 2.0, and will advise on MLPS-related compliance issues accordingly.

I. History of MLPS 2.0

The full name of MLPS 2.0 is *Information Security Technology - Baseline for Cybersecurity Classified Protection* (GB/T 22239-2019). From 2008 to 2017, China's MLPS technologies mainly complied with MLPS 1.0 (*Information Security Technology - Baseline for Information Security Classified Protection* (GB/T 22239-2008)).

如果您需要本出版物的中文本，
请与下列人员联系：

郭建良: +86 21 3135 8756
Publication@llinkslaw. com

For more Llinks publications,
please contact:

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

Llinks Law Offices
www. llinkslaw. com

With the fast development of the society, network has been expanded from computer information systems to areas such as cloud computing, mobile internet, Internet of Things and big data. The original MLPS of computer information system security gradually fails to cover these areas. Therefore, since March 2014, the Ministry of Public Security took the lead in drafting key standards for MLPS covering the new fields of information technology and submitting such standards as national standards. Relevant draft and draft for comments were successively published since 2015, and then came the term MLPS 2.0. After the issuance of the *Cybersecurity Law* in 2016, the Secretariat of the National Information Security Standardization Technical Committee issued *Information Security Technology - Baseline for Cybersecurity Classified Protection (Draft for Comments)* ("Draft for Comments") on November 3 in the same year, so as to match the new network environment and legal system of network governance. Now, MLPS 2.0 is the official version after the Draft for Comments.

The MLPS 2.0 framework also includes other national standards such as *Information Security Technology - Evaluation Requirement for Cybersecurity Classified Protection* (GB/T28448-2019), *Information Security Technology - Technical requirements of Security Design for Cybersecurity Classified Protection* (GB/T 25070-2019).

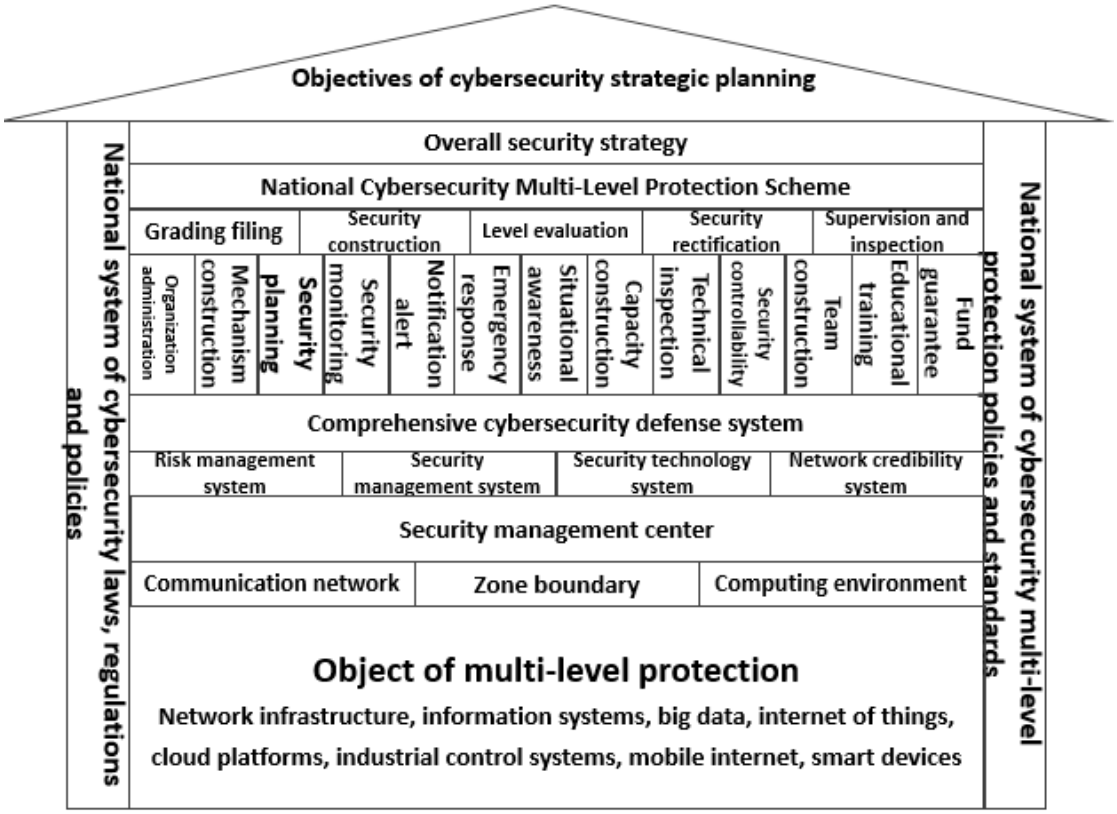
II. Enhancement of Legal Effects

According to the introduction and formulation/revision basis of MLPS 1.0 and MLPS 2.0, the two versions refer to totally different regulatory documents. The era of MLPS 1.0 was for information security multi-level protection, where the *Regulations on Computer Information System Security Protection*, the administrative regulation of the State Council, was the upper law source, and its core system was based on *the Administrative Measures on Information Security Multi-Level Protection*, which was jointly promulgated by the Ministry of Public Security, the State Secrecy Bureau, the State Cryptography Administration Bureau, the Informatization Office of the State Council. The core system of MLPS 2.0, the upper law sources of are *Cybersecurity Law* and the *Law on Guarding State Secrets* are the top design, and the *Regulations on Cybersecurity Multi-Level Protection* (the draft for comments of which was issued in

June 2018).

MLPS 2.0 is superior to MLPS 1.0 in legal effects and the hierarchy of its legal basis. The transition from MLPS 1.0 to MLPS 2.0 is the revision of policies, improvement of technology, as well as the enhancement of legal effects.

The Framework of Cybersecurity Multi-Level Protection Scheme



III. Expansion of Protected Subjects

MLPS 1.0 mainly applied to security of information systems based on traditional structures, while the scope of the protected subjects in MLPS 2.0 is expanded from information system to cyberspace by including new technologies and application scenarios such as cloud computing, big data, Internet of Things and industrial control. Compared to the Draft for Comments, MLPS 2.0 no longer establishes the five

separate standards for different subjects. Instead, it establishes a uniform standard for all subjects, while adding serial identification -based expanded requirements for different subjects. These expanded requirements include general security requirement and expanded security requirements on cloud computing, mobile internet, Internet of Things and industrial control system. Also, the contents of each expanded requirement are simplified.

Corresponding to *Information Security Technology - Grading Guidance of Cybersecurity Multi-Level Protection*, the requirements for grading subjects are also refined according to the above expanded requirements:

1. With regards to cloud computing platform, grading subjects are the service providers and users;

2. With regards to Internet of Things, characteristic elements such as inception, network transmission and processing application are not graded separately. Instead, they are graded as an integrated object;

3. As for mobile internet, mobile terminals, mobile applications, wireless networks and relevant wired networks will be graded in integrity;

4. As for big data, the platforms and applications with the same security responsibility subjects will be graded as a whole; others will be graded separately.

IV. Changes of Protection Approaches

Protection under MLPS 1.0 focused more on the security protection of systems, staff and physical environment, while protection under MLPS 2.0 has been amended to emphasize security of cyberspace systems surrounding data, networks, systems and staff. Statements such as “technical requirements” or “management requirements” have been eliminated in MLPS 2.0. It is foreseeable that technology and management will comprehensively intertwine with each other in cybersecurity construction in the future. In advising clients on cybersecurity and data compliance, we discovered that it is extremely hard for

cybersecurity management staff to perform their duties without technical knowledge, and that technical staff cannot undertake cybersecurity compliance work without management knowledge. Cybersecurity compliance will hinge on effective construction of cybersecurity management system and exquisite selection of qualified staff for operation and maintenance management.

Compared to MLPS 1.0, MLPS 2.0 emphasizes more on the concept of security operation and maintenance: premised on traditional management and operation of assets and devices, the scope of security operation and maintenance is expanded to security incident response and discovery of high security risks. The scope of security operation and maintenance will be further expanded when considering regular audits and verification of effectiveness. Therefore, we can see that the concept of security operation and maintenance mentioned in MLPS 2.0 is gradually changed to the concept of security operation.

V. Changes in Requirements for Grading and Assessment

MLPS is the fundamental mechanism for the safeguard information security in China, and is a mechanism that protects networks and information systems according to their different levels of importance. The higher the level of security protection, the stronger the required capability of security protection. Security protection can neither be insufficient nor excessive.

Affected object	Degree of damage to the object		
	Ordinary	Serious	Very serious
Users' own interest	Level one	Level two	Level three
Public interest, social order	Level two	Level three	Level four
National security	Level three	Level four	Level five

The relationship between the rating factors of MLPS 2.0 and the level of security protection

Compared to the "self-grading and self-protection" requirement of MLPS 1.0, MLPS 2.0 changes the grading mechanism to "application for approval". Enterprises shall state in writing the level of safety protection of the protected object and the methods and reasons for determining the level, and organize relevant departments and relevant safety technical experts to verify and confirm the reasonableness and accuracy of the grading result, which shall be submitted to relevant authorities for approval.

In addition, in principle the security protection level of supportive networks such as basic information network, cloud computing platform, and big data platform shall not be lower than the security protection level of the object which they support. By this standard, the level of big data security protection shall not be graded lower than level three; for critical information infrastructure, the level of security protection in principle shall not be graded lower than level three.

VI. Positions and Functions of Security Management Organizations

Both MLPS 1.0 and MLPS 2.0 provide for requirements on the establishment of cybersecurity management function departments in the section of "security management organization", and set forth the establishment of other positions such as security supervision and security management, and define the duties of each responsible person. In MLPS 2.0, the main positions are changed from "system administrator", "network administrator" and "security administrator" to "system administrator", "audit administrator" and "security administrator", and such positions are further refined. For example, in the newly added control point, "security management center", detailed requirements for the duties and responsibilities, system access rights, and work specifications of the aforementioned personnel are set as follows:

1. System management
    a) System administrators shall be identified and shall only be permitted to conduct system management operations through specified orders or operating interfaces, and such operations shall be audited;

b) System resources and operations shall be configured, controlled and managed by system administrators, including user identity, system resource configuration, system loading and launching, abnormal system operation handling, data and device backup and recovery.

2. Audit management

a) Audit administrators shall be identified and shall only be permitted to conduct security audit operations through specified orders or operating interfaces, and such operations shall be audited;

b) Audit records shall be analyzed by audit administrators, and be processed according to analysis results, including storage, administration and retrieval of audit records in accordance with security audit strategies.

3. Safety management

a) Safety administrators shall be identified and shall only be permitted to conduct security administration operations through specified orders or operating interfaces, and such operations shall be audited;

b) Security strategies of the system shall be configured by security administrators, including the configurations of security parameters, unified security identification of subjects and objects, authorization of subjects, configuration of credibility verification strategies, etc.

VII. Addition of "Personal Information Protection"

MLPS 2.0 adds personal information protection to its requirements. With the issuance of the *EU General Data Protection Regulation* (GDPR) and the recent frequent occurrence of personal information security incidents, personal information protection has become the focus of law enforcement agencies. It is worth noting that the Network Security Protection Bureau of the Ministry of Public Security, the Beijing Network

Industry Association and the Third Research Institute of the Ministry of Public Security jointly issued the *Guidelines for Internet Personal Information Security Protection* ("Guidelines") on April 10, 2019. The technical requirements of the Guidelines have incorporated the contents of MLPS 1.0 and MLPS 2.0. The Guidelines are formulated by the public security organs based on their law enforcement experience gained from a massive number of cases. The Guidelines can be used not only by enterprises in the protection of personal information, but also by **network security supervision departments** in the **supervision and inspection** of personal information protection according to law. Therefore, although there are only a few words about the protection of personal information in MLPS 2.0, enterprises should still pay attention to the implementation of personal information protection in strict accordance with the technical requirements of MLPS 2.0. (For more information on the contents and impact of the Guidelines, please refer to Llinks law review article *A Brief Review of the Guidelines for Internet Personal Information Security Protection.*)

VIII. Other major changes

Taking the requirements for Grade III provided in *Information Security Technology - Baseline for Cybersecurity Classified Protection* and *Information Security Technology - Baseline for Information Security Classified Protection* as examples, we summarize the new requirements of MLPS 2.0 as follows.

Chapter Name	New Requirements of MLPS 2.0
Technical Requirements	
Secure Physical Environment	The requirement of video surveillance system in computer room is clearly put forward, which is not mentioned in MLPS 1.0.
	Anti-static requirements are clearly illustrated by the use of electrostatic eliminators and anti-static wrist straps; the requirements for electrostatic protection are more detailed.
	The backup power supply system is no longer required for power supply, but the requirements for redundant power cables are retained.
	A new requirement is added for cloud computing expansion: physical Computer

	Room must be located within the territory of China.
Secure Communication Network	The three control points of structural security, boundary integrity check and network device protection are removed, two control points of network architecture and communication transmission are added, and "requirements of credibility verification" are added.
	The requirement that important systems cannot directly connect to external network is deleted, and the SLA service that allocates bandwidth according to business priority is deleted; the new standard only requires the redundancy of the communication line and the key network device.
	In the boundary integrity check, the security requirements of the wireless network are put forward, and the wireless network access must pass through the controlled boundary.
	Content filtering management is added to access control, which requires filtering information content in and out of the network at key network nodes to achieve content access control.
	A new requirement is added for intrusion prevention that it can detect attacks from inside to outside and from outside to inside.
	For the first time, malicious code prevention explicitly requires protection against spam.
	The requirements for log auditing have changed: from the previous “six months of retention” to “compliance with laws and regulations”.
Security Zone Boundary	Border protection, access control, intrusion prevention, malicious code prevention and security audit are integrated as sub- categories requirements of security zone boundary, and requirements of credibility verification are added.
Secure Computing Environment	The requirements of device and computing security, application and data security are combined into the requirement of secure computing environment.
	Device Computing and Security Sub-categories: a) There are obvious changes in two authentication methods in identity

	authentication. Users are identified by two or more combination authentication technologies, and at least one of them should be implemented by dynamic password, cryptography or biotechnology; b) Malicious code prevention requirements have also changed significantly. Technical measures against malicious code attacks or active immune credibility verification mechanism should be adopted to identify and effectively block intrusions and viral activities in a timely manner.
	Application and Data Security Sub-categories: a) Three control points of communication integrity, communication confidentiality and non-repudiation are removed; and a control point of personal information protection is added; b) A new requirement is added: it is compulsory for users to modify their initial password at the first login; c) A new requirement is added: when new user identity authentication information is lost or invalid, technical measures shall be taken to ensure the security of the authentication information reset process; d) A new requirement is added: when a fault occurs, the volatile data and all status should be automatically saved to ensure that the system can recover; e) A new module is added: personal information protection; f) Only user personal information necessary for business should be collected and saved;

	g) Unauthorized access to and illegal use of user personal information should be prohibited.
Management Requirements	
Security Management Center	New controls are added, including: system management, audit management, security management, and centralized management. The specific responsibilities of system administrators, audit administrators, and security administrators are clarified in detail, and the importance of positions is emphasized, including identity authentication, special operation permissions, and resource allocation, etc.
Security Management System	In terms of formulation and publication, it is no longer required to demonstrate and verify the process, to specify the scope of publication or to register the receipt and delivery of documents. As long as the version is well controlled, it can be officially and effectively released. In terms of review and revision, the requirement for review by the leading group is removed.
Security Management Organization	In terms of authorization and approval, the requirement of process documentation is removed. In terms of communication and cooperation, it is no longer required to maintain communication with suppliers, experts, and security companies; and it is not necessary to hire security consultants to guide security work every year.
Security Management Personnel	The requirement of personnel assessment is deleted.
	A new requirement is added: external personnel should gain permission to access network access systems.
Security Construction Management	The requirements of system security scheme design is simplified: it is no longer required to make short-term and long-term security construction plan of the system, to regularly adjust and revise supporting documents such as overall security strategy and framework.
	New requirement are added for self-developed software:

	a) Ensure the availability of documentation and usage guidelines for software design, and control the use of documents; b) Ensure that security is tested during software development and that possible malicious code is detected before the software is installed; c) Ensure that developers are full-time staffs and their development activities are controlled, monitored, and reviewed.
	The importance of safety at the development level is emphasized; and security testing is required.
	The process of outsourcing development, engineering implementation, test and acceptance, and system delivery is simplified.
Security Operation and Maintenance Management	Under the control point of asset management, it is no longer required to build an asset security management system.
	Media management requirements are reduced from 6 items to 2 items: a) Ensure that media are stored in a safe environment, all kinds of media are controlled and protected, storage environment is management by specially-assigned person, and archiving media are periodically checked according to the catalogue list; b) Personnel selection, packaging and delivery of media in the process of physical transmission should be controlled, and media archiving and query should be registered and recorded.
	Two new requirements are added for device maintenance and management: a) Ensure that the information processing device must be approved before it can be taken out of the device room or office. Important data must be encrypted when the device containing storage media is taken out of the working environment;

	b) Devices containing storage media should be completely erased or securely covered before they are scrapped or reused, to ensure that sensitive data and licensed software on the device cannot be restored and reused.
	The management and security management center is removed; vulnerability and risk management is added.
	In the malicious code prevention management, the requirement to save the records of detecting and killing is removed, the requirement to analyze and record the process of upgrading and antivirus is removed; the requirement to periodically check the effectiveness of technical measures is added.
	A new configuration management control point is added. Backup of System configuration information is required, including at least: network topology, components installed by the device, software version and patch information, and configuration parameters of the device and software.

Conclusion

MLPS 2.0, together with other mechanisms, builds up China's network security multi-level protection scheme.

Network Security Multi-Level Protection Scheme	Hierarchy of Authority
Cybersecurity Law	Law
Regulations on Cybersecurity Multi-Level Protection	Administrative Regulations
Measures for Filing of Cybersecurity Multi-Level Protection	Departmental Rules
Network Security Multi-Level Protection National Standards: ➢ Information Security Technology - Baseline for Cybersecurity Classified Protection (GB/T 22239-2019)	National Standards

➢ Information Security Technology - Evaluation Requirement for Cybersecurity Classified Protection (GB/T28448-2019) ➢ Information Security Technology - Technical requirements of Security Design for Cybersecurity Classified Protection (GB/T 25070-2019)	

With the deepening of Cybersecurity Law enforcements, not only multinational corporations but also domestic companies shall place emphasis on network security and MLPS compliance issues.

Taking state-owned enterprises as an example, last year WannaCry worm launched a worldwide ransom attack that affected nearly 150 countries in a few hours. Government agencies, universities, and hospitals were among the main targets in China, which play a pivotal role in the stable operation of society.

In response to the repetitive occurrence of cybersecurity incidents related to Chinese state-owned enterprises (SOEs), government-owned enterprises and institutions, the State-owned Assets Supervision and Administration Commission ("SASAC") added "cybersecurity incidents" as a new key performance index in the *Measures for Operation Performance Assessment of Centrally-Administered Enterprises Responsible Persons* (Revised in 2019), which came into effect on April 1, 2019. The legal representative of a SOE and relevant person in charge of the enterprise will be degraded or have their points deducted by the SASAC in the event that their violations of laws, regulations and rules result in cybersecurity incidents of a serious nature or above, and cause major adverse effects or loss of state-owned assets.

In this context, the centrally-administered SOEs shall be on the watch of the new requirements of MLPS 2.0 and carry out compliance work in a timely manner; at the same time, they shall appoint the responsible person for network security and fulfill the obligations of network security protection. Critical information infrastructure operators must fulfill the additional obligations of disaster recovery backup for important systems and databases.

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	
David Pan Tel: +86 21 3135 8701 david.pan@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 Dennis Fong & Co., Solicitors)	
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	