China Marches into Cybersecurity Classified Protection 2.0

May 2019

Hogan Lovells

China Marches into Cybersecurity Classified Protection 2.0

The cybersecurity classified protection regime attracted significant attention when it was included in the PRC Cyber Security Law promulgated in 2017 (the "**CSL**"). The CSL mandates that Network Operators[1] follow certain security requirements based on the levels of risk associated with their networks. However, the CSL did not provide much detail as to how the classification should work in practice, nor did it specify how the security obligations and requirements attached to different levels vary. The Ministry of Public Security, released a draft *Regulations for Cybersecurity Classified Protection* (the "Classified Protection Regulations") for public comment in June 2018. The Classified Protection Regulations provided some degree of guidance, but industry has been very interested to see more detailed technical guidance to ensure compliance with the general and vague requirements of the CSL in this area.

The publication in May 2019 of three new national standards, namely the *Information Security Technology - Baseline for Classified Protection of Cybersecurity (GB/T 22239-2019),* the *Information Security Technology - Evaluation Requirement for Classified Protection of Cybersecurity (GB/T 28448-2019),* and *the Information Security Technology – Technical Requirements of Security Design for Classified Protection of Cybersecurity (GB/T 25070-2019)* (the "New Standards") are intended to bridge the practical compliance gap.

The three New Standards, although non-binding are critical to the interpretation of the Classified Protection requirements, and effectively bring these requirements forward to a "version 2.0", applicable to local companies and international businesses alike with operation in mainland China.

From 1.0 to 2.0

"Classified Protection" is actually not a new concept in China. Its origin can trace back to 1994 when the *Regulations on Security Protection of Computer Information Systems* first introduced such requirement. This requirement remained vague for some time until a mandatory national standard, the *Classified Criteria for Security Protection of Computer Information System (GB 17859-1999)* published in 1999, which introduced the five levels of IT system protection requirements. The later promulgation, in 2007, of the *Administrative Measures for Classified Protection of Information Security* together with some further national standards have together come to constitute the Multi-Level Protection Scheme ("MLPS") in China, which established a grading scale for information security, assigning the five grade classifications based on the degree of harm to national security, public order, public interests and the legitimate rights and interests of the PRC if the system were subject to a breach or disruption. Such MLPS is also known as "Classified Protection 1.0".

The standards forming Classified Protection 1.0 have served a critical role in guiding the market. However, with the introduction of the CSL, it is clear that there has been a significant increase in regulatory focus on information security in China. Closer monitoring and stricter controls over the cyber space has been a key policy priority, as continuously emphasized by President Xi and his administration[2]. At the same time the relentless advance of technology has meant that the risks that Classified Protection was designed to address have changed significantly. The proliferation of cloud computing and mobile technologies, together with innovations in data analytics and artificial intelligence have called the standards under the

[1] "Network operators" shall refer to the owners and managers of cyberspaces and the cyberspace service providers, pursuant to the Article 67 of the Cyber Security Law

[2] Please see HERE for our previous client alert regarding the Cyber Security Law.

old regulations and standards into question, hence the move to Classified Protection 2.0[3].

What's new in Classified Protection 2.0?

The following are changes made through Classified Protection 2.0:

1. "Cyber" vs. "Computer Information System"

In order to match the terminology of the CSL, the New Standards have changed from referencing "Classified Protection of Information Systems" to "Classified Protection of Cybersecurity". However, this change is merely formal and does not change the objective of these standards, which continue to protect "Systems", as broadly defined. A notable change is that the new standards have been amended to specifically address recent advances in technology, such as cloud platforms and systems, big data applications, platforms and resources, the Internet of Things ("IoT"), industry control systems and mobile systems.

2. The Five Levels

Same as the old approach, the three New Standards still set forth requirements based on five different levels of security protection.[4] Pursuant to the New Standards, especially GB/T 22239-2019, which sets forth the protection baseline, classification levels should follow the *Information Security - Technology Classification Guide for Classified Protection of Information System (GB/T 22240)*. GB/T 22239-2019 doesn't specify the year version of GB/T 22240 as the current effective 2008 version is outdated and in early 2018 an updated version was released for public comment.

The difference between the 2008 and the 2019 version of GB/T 22240 is that the criteria to designate "Level 3" under the classification have been slightly changed. Serious damage to the lawful rights of the citizens, entities and other organizations became one of the criteria for a system to be classified as "Level 3". This is consistent with the draft Classified Protection Regulations, hence we believe going forward, it's very likely that the old "Level 3" criteria will be replaced once the draft Classified Protection Regulations and GB/T 22240 have become effective.

Considering the changes, we summarized the current five levels of protection under the Cybersecurity Classified Protection 2.0 based on harm, if the system is damaged, to national security, public order, public interests and the legitimate rights and interests of the PRC the as below:

The object damaged	Harm to the object		
	Minor Harm	**Serious Harm**	**Extremely Serious Harm**
Lawful rights of the citizens, entities and other organizations	Level 1	Level 2	Level 3
Public order and public interests	Level 2	Level 3	Level 4
National Security	Level 3	Level 4	Level 5

3. General Requirements Restructured

Classified Protection 2.0 has inherited the majority of the requirements and control points for the five protection levels from its

[3] The legal basis of Classified Protection 2.0 is commonly believed to include: 1) the Cyber Security Law; 2) the *Regulations of Cybersecurity Classified Protection; 3) the three New Standards, GB 17859-1999, GB/T 28449-2018, GB/T 36627-2018, GB/T 36959-2018 and GB/T 36958-2018, and 4) two new standards that are in the process of updating – GB/T 22240 and GB/T 25058.*

[4] Though level 5 is included in both Classified Protection 1.0 and 2.0 documents, neither of the versions discusses the actual requirements. The requirements are specified by separated regulations managed by national security and confidentiality related authorities.

predecessor, but with some reorganization and slightly expanded scope. More specifically, detailed items and the control points required by the GB/T 22239 have been changed as below:

	GB/T 22239-2008	GB/T 22239-2019
Technical Requirement	Physical Security	Secured Physical Environment
	Network Security	Secured Communication Network
		Secured Area Boundary
	Host Security	Secured Computing Environment
	Application Security	
	Data Security and Backup Recovery	
	N/A	Secured Management Center
Management Requirements	Security Management System	Security Management System
	Security Management Institute	Security Management Institute
	Personnel Security Management	Security Management Personnel
	System Establishment Management	Security Establishment Management
	System Maintenance Management	Security Maintenance Management

On the other hand, the total number of control points in the 2019 standard has been notably reduced. For example, the control points for "Level 3" have been reduced from 291 to 226. Though the drop in the number of control points suggests a more relaxed standard, the 2019 standard includes new requirements that Network Operators must pay heed to. For instance, under the Security Maintenance Management section of "Level 3", the 2019 standard added requirements for the management of bugs, configurations and outsourcing, none of which were included in the 2008 version.

Further, the 2008 version required systems classified above "Level 3" to be tested regularly (annually for "Level 3" and twice a year for "Level 4" and "Level 5"), whereas the 2019 version removed specific frequencies for testing but generally imposes a requirement for regular checking, the draft Classified Protection Regulations on the other hand, stipulate that Network Operators of "Level 3" and above should conduct cybersecurity tests annually. Once the requirements are effective, Network Operators should refer to the Classified Protection Regulations to confirm the required frequency of testing.

Lastly, the 2019 version added specific requirements for personal information protection, and imposed progressive standards of "reliable verification" based on the applicable protection level.

4. Extended Requirements

The other major change introduced by Classified Protection 2.0 is in the form of the "Extended Requirements for Cloud Computing, Mobile Network, IoT and Industry Control Systems to all levels. Network Operators with business in mainland China should pay close attention to these requirements, not only because they may have a direct impact on their business but also because these requirements have touchpoints with other laws and

regulations, such as the CSL, which, if breached, could result in penalties.

Taking cloud computing as an example, the new 2019 standard requires the basic facilities of cloud computing to be located in mainland China. The 2019 standard also requires operators of cloud computing in mainland China to store customer data in China and follow the applicable cross-border data transfer rules if it is proposed to transfer data overseas. These requirements are in line with the CSL and the draft *Personal Information and Important Data Cross-Border Transfer Assessment Measures*, with penalties for non-compliance.

The Extended Requirements are structured in a way that is similar to the general requirements but with specific requirements intended to address risk factors specific to these four applications.

Connection to the CSL and other laws and regulations

Classified Protection 2.0 is understood to be a critical tool for the implementation of the CSL, but it is important to note that some requirements of the CSL are not reflected in the three New Standards.

Article 21 of the CSL requires Network Operators to maintain logs for network operations and security incidents for at least 6 months. Yet GB/T 22239 only requires the maintenance of records but doesn't specify a period. We suggest when implementing these New Standards, companies should also make reference back to the CSL and other applicable laws and regulations to ensure full compliance with all control points.

The other connection between Classified Protection 2.0 and the CSL is in how the new standards aid in the interpretation of some critical concepts in the CSL, in particular the scope of the definition of "Critical Information Infrastructure" ("CII") and specific requirements in relation to personal information protection.

- CII: The new draft of GB/T 22240 suggests that CII should be classified as at least "Level 3" under Classified Protection 2.0. We continue to hold the view that not all "Level 3" organizations will necessarily be categorized as operators of CII under the CSL.

- Personal information protection: GB/T 22239 added some very general personal information protection requirements to organizations classified "Level 2" and above. It is worth referencing other government guidelines such as the *Internet Personal Information Security Protection Guide* and *Information Security Technology — Personal Information Security Specification (GB/T 35273—2017)* [5] for more detailed information to implement the personal information protection requirements.

In addition, comparing the general and extended requirements of GB/T 22239 to the Classified Protection Regulations, it is obvious that the New Standards are guidelines as to how to implement the high-level requirements in the Classified Protection Regulation. It is important to note that the Classified Protection Regulations cover a broader range of activity than the New Standards, and currently several other Classified Protection related standards are still in the process of drafting or approval. Classified Protection 1.0 is composed of a series of regulations and standards, and we anticipate the update to 2.0 will involve the revision of other regulations as well.

What should my organization be doing?

[5] See HERE for our previous article with respect to this standard. Please also note this standard is now in the process of updating and a new draft has been released for public opinion on February 1, 2019.

The New Standards will have important ramifications for Network Operators under the CSL, which includes most if not all organizations operating network infrastructure in mainland China.

The three New Standards will not take effect until December 1, 2019, which leaves the market at least some time to prepare, noting, however, that it may take time to remediate deficiencies against the updated standards. As non-binding standards, the New Standards do not have mandatory legal effect. However, the requirements are to serve as an important supplement and interpretive aid to the Cyber Security Law and the upcoming Classified Protection Regulations. There is no doubt that the Chinese government has a sharp focus on fully implementing the Classified Protection regime as part of its administration of the CSL.

It is clear that there continue to be a number of missing pieces to the puzzle of Chinese cyber security compliance. We expect the remaining supporting regulations and guidelines will be issued in the short term. In the meantime, the New Standards represent an important point of reference for organizations reviewing their information security programs in mainland China.

Contacts

Roy Zou
Office Managing Partner, Beijing
roy.zou@hoganlovells.com

Mark Parsons
Partner, Hong Kong
mark.parsons@hoganlovells.com

Andrew McGinty
Partner, Hong Kong
andrew.mcginty@hoganlovells.com

Liang Xu
Partner, Beijing
liang.xu@hoganlovells.com

Sherry Gong
Partner, Beijing
sherry.gong@hoganlovells.com

Jessie Xie
Senior Associate, Beijing
jessie.xie@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices

www.hoganlovells.com