



Tighter Controls Over Business and State Secrets, But Little Clarification:

— *Analysis of the Recent Developments in China's Regulation of Business and State Secrets*

Friven Yeoh

Hong Kong
+852-3512-2369

Singapore
+65-6593-1800
fyeoh@omm.com

Bingna Guo

Beijing
+86-10-6563-4224

Shanghai
+86-21-2307-7000
bguo@omm.com

China has recently taken a series of measures to amend its laws and regulations on state and business secrets. On March 25, 2010, the State-owned Assets Supervision and Administration Commission (“**SASAC**”) issued the *Interim Measures on Protection of Business Secrets of Centrally Administered Enterprises* (the “**SASAC Measures**”), which are aimed at strengthening the administration and protection of business secrets of centrally administered state-owned enterprises (“**CAEs**”). On April 29, 2010, the Standing Committee of the People’s Congress issued an amended *Law on Safeguarding State Secrets* (the “**Amended State Secrets Law**”), which will become effective on October 1, 2010. The existing *Law on Safeguarding State Secrets*, issued in 1988, is considered inadequate to deal with the rapid development of technology for the transmission and storage of information.

Although the definition and scope of state and business secrets remain broad, the *SASAC Measures* and the *Amended State Secrets Law* have introduced changes to the law that carry important ramifications for multinational companies, especially those operating in sensitive industries and those who interface regularly with CAEs and other state-owned enterprises (“**SOEs**”). This article summarizes the salient aspects of these changes and discusses their potential ramifications.

I. The SASAC Measures

The *SASAC Measures* are applicable to the 123 CAEs¹ that are directly administered by SASAC. CAEs are usually key SOEs operating in the pillar industries of China, such as Baosteel, Anshan Steel, China National Petroleum Corporation, Sinopec, CNOOC and Minmetals. Although the *SASAC Measures* do not apply to other SOEs, they are likely to be looked upon as guidance by those SOEs in relation to their own practice in protecting business secrets.

1. Current as at August 18, 2010. The list of the 123 CAEs is available at the following link <http://www.sasac.gov.cn/n1180/n1226/n2425/index.html>.





The Definition and Scope of Business Secrets

Pursuant to the *SASAC Measures*, “business secrets” refer to “operational information and technical information that are unknown to the public, that can bring economic benefits to CAEs and are functional and for which CAEs have taken confidentiality measures” (Article 2). This is essentially a restatement of the existing definition of business secrets under the *PRC Criminal Law* and the *Anti-Unfair Competition Law*.

Nevertheless, the *SASAC Measures* explain what information may be considered as “operational information and technical information” falling within the scope of business secrets. The scope of such information is broad. Operational information that may constitute business secrets mainly includes information with respect to “strategic planning, management methods, commercial modes, reform and listing, mergers and acquisitions and restructuring, equity transactions, financial information, investment and financing decisions, production, purchase and sale strategies, resource reserve, client information and bid invitation and tendering issues” (Article 10). Technical information that may constitute business secrets mainly includes information with respect to “design, programs, product formulas, manufacturing processes, manufacturing methods and technical know-how” (Article 10). It is important to note that not all information belonging to CAEs which falls under the foregoing categories is a business secret; only those information which is “unknown to the public”, “can bring economic benefits to CAEs”, is “functional” and “for which CAEs have taken confidentiality measures”, will be regarded as a business secret.

Whereas many businesses had in the past assumed that only core technical information is capable of constituting a business secret, the *SASAC Measures* make it clear that operational information of CAEs may also constitute business secret, and dealing with such information in contravention of the law attract civil, administrative and even criminal liabilities.

Furthermore, pursuant to the *SASAC Measures* certain business secrets of CAEs may also be categorised as “state secrets”. Article 3 provides that “if any operational information or technical information of CAEs falls within the scope of state secrets, such information shall be protected as state secrets in accordance with the law.” Given the strategic importance of CAEs to the national economy, it is likely that business secrets of CAEs

will also be considered as state secrets. Companies should therefore consider the laws and regulations governing state secrets when dealing with CAEs. (See discussions on *Amended State Secrets Law* below.)

It is also noteworthy that notwithstanding a recent high profile case involving the arrest of a number of individuals in connection with the gathering of market information, the *SASAC Measures* do not shed further light as to whether market intelligence gathering activities may contravene the latest guidelines on business secrets. As noted above, one essential element of “business secrets” is that the information must be unknown to the public. However, while certain market information may be known within a specific industry circle, it is not known to the public at large. The question remains as to how widely circulated the market information must be to be considered as public information. Companies should therefore adopt a cautious approach when gathering market intelligence in China.

Classification and Labeling Requirements

The *SASAC Measures* also impose a new requirement on the classification and labeling of CAEs’ business secrets. (Previously, only state secret documents needed to be classified and labeled). As a result of this requirement, CAEs’ business secrets should now become more identifiable. Business secrets of CAEs may now be classified as either “core business secrets” (核心商密) or “ordinary business secrets” (普通商密) (Article 13). By contrast, state secret documents are classified as “top secret” (绝密), “highly secret” (机密) or “secret” (秘密). The classification of CAEs’ business secrets will have to be approved by “relevant personnel in charge” at the CAE and filed with the business secrets office of CAEs for record.

All documents and media storing those documents must bear conspicuous marks as to its secrecy, and the identity of the owner of the secret, the level of secrecy and the time period for which the “secrecy” classification is to apply must be expressly stated (Article 15). However, documents and materials that are not clearly marked as secret may still be regarded as business secrets if they fall within the definition of business secrets under the *SASAC Measures*. Therefore, companies dealing with CAEs should not simply assume that unmarked documents may be freely distributed or dealt with.

Confidentiality Agreements with CAEs

The SASAC *Measures* further require CAEs to sign confidentiality agreements with business counterparties whenever CAEs are engaged in activities where business secrets may be involved. In reality, CAEs often require confidentiality agreements to be signed for transactions involving mergers & acquisitions and public listings. The SASAC *Measures* now specifically enumerate a wide range of other types of business dealings requiring confidentiality agreements, where business secrets of CAEs are involved. Such business dealings include any consultation, negotiation, technical evaluation, achievement appraisal, cooperative development, technology transfer, joint equity investment, external audit, due diligence and asset and capital liquidation and verification (Article 21).

Penalties

The SASAC *Measures* appear to focus more on providing guidance on the protection of business secrets for CAEs rather than implementing disciplinary actions and penalties. The Rewards and Penalties section of the SASAC *Measures* is accordingly brief. It only addresses penalties for CAE personnel who illegally discloses or uses business secrets and provides broadly that legal liabilities will be investigated in accordance with the law, and if a criminal offense is suspected, the case will be referred to judicial authorities for further action (Article 32). Although no specific legal liabilities are added to the SASAC *Measures*, the legal liabilities under the *PRC Criminal Law* and other existing laws and regulations remain applicable and the SASAC *Measures* may be relied upon as a basis for future judicial investigations and prosecutions.

II. The Amended State Secrets Law

Work on amending the *State Secrets Law* commenced in 1996, with several versions of the draft amendments having been circulated for public consultation. The call to amend the *State Secrets Law* strengthened with the implementation of the *Regulation of the Disclosure of Government Information* in May 2008, sparking discussions as to how the definition of state secrets should be aligned with the public's right to know. As such, maintaining a balance between the need to preserve state secrets and the need to promote transparency in governmental work is one of the major legislative objectives in promulgating the *Amended State Secrets Law*. The law was

also being amended out of a sense of urgency that technological development has made it easier to leak classified information. Whether the amended law in fact strengthens control over and oversight of the administration of state secrets remains to be seen. However, the following aspects of the *Amended State Secrets Law* have important implications for companies dealing with Chinese government agencies, CAEs, SOEs and other entities, as regards the handling of sensitive information.

The Definition and Scope of State Secrets


The *Amended State Secrets Law* restates the definition of state secrets under existing law, which is that state secrets are “matters that have a vital bearing on state security and national interests and, as specified by legal procedure, are only known to a limited number of people for a given period of time” (Article 2). The *Amended State Secrets Law* also lays out seven categories of information concerning state security and national interests that may constitute state secrets. In accordance with Article 9 of the *Amended State Secrets Law*, the seven categories of information are as follows:

- (1) secrets concerning major policy decisions on state affairs;
- (2) secrets in relation to national defense and activities of the armed forces;
- (3) secrets in diplomatic activities and in activities related to foreign countries, as well as secrets to be maintained as commitments to foreign countries;
- (4) secrets in national economic and social development;
- (5) secrets concerning science and technology;
- (6) secrets concerning activities for protecting state security and the investigation of criminal offenses;
- (7) other secrets that are identified by competent state administrations safeguarding state secrets.

In addition, secrets of political parties that fall within the prescribed categories above shall also be state secrets.

Stricter Classification and Labeling Requirements

The classification systems of state secrets remain unchanged under the *Amended State Secrets Law*. State secrets are still classified as “top secret” (绝密), “highly secret” (机密) or “secret” (秘密), depending on the degree of harm that may be caused by disclosure. However, the *Amended State Secrets Law* adopts new provisions on the duration of secrecy for each category of



secret and conditions for declassification. These new provisions are intended to enhance transparency in governmental work and facilitate the public's right to know. Generally, the maximum duration is 30 years for "top secrets", 20 years for state secrets classified as "highly secret", and 10 years for other "secrets" (Article 15). With respect to state secrets for which the duration of secrecy "cannot be fixed", the condition for declassification must be clearly stated (Article 15).

State secrets can only be classified by government agencies with authority to do so. Central government organs and provincial organs and their authorized organs and units may classify state secrets as "top secret", "highly secret" and "secret". Organs at the level of city divided into districts or autonomous prefectures and their authorized organs and units may classify state secrets as "highly secret" and "secret". The specific list of state organs authorized to issue classifications and the scope of their authority shall be stipulated by the state administrations safeguarding state secrets (Article 13). Under the *Amended State Secrets Law*, the authority of government agencies below the county level to classify state secrets is more restricted (Article 13). This should help prevent an arbitrary expansion of the scope of state secrets and provide greater predictability for companies when dealing with sensitive information.

In response to the development of technology for the storage of information, the *Amended State Secrets Law* further provides that all devices and objects carrying state secrets, whether they are stored in paper, ray, or electromagnetic forms or in other media, as well as equipment and products that are classified as state secrets, should be clearly marked as such.

The control over classification decisions and stricter labeling requirements should make state secrets more identifiable. However, as with the business secrets regime, the lack of a classification label does not necessarily mean that an information may not be a state secret. As a result of the broad definition adopted in relation to state secrets, there remain significant risks for companies who frequently deal with sensitive information in that it is often difficult to identify whether those

information or documents that are not clearly labeled are state secrets. Accordingly, it is critical for companies to design appropriate compliance rules to minimize the risk of inadvertent disclosure and unlawful handling of state secrets.

[New Liabilities for Internet and Network Operators](#)

The rapid development of the internet has provided significant challenges to the Chinese government in its efforts to protect state secrets. The *Amended State Secrets Law* now states that internet and other network operators and service providers (the "**Network Operators**") are under the obligation to cooperate with national and public security authorities in investigating cases relating to the unlawful divulgence of state secrets. In fact, these obligations are not new to Network Operators who are already subject to similar obligations under existing telecommunications laws and regulations.

Under the *Amended State Secrets Law*, Network Operators are required to cooperate with public and national security departments and procuratorial organs in their investigations of any unlawful divulgence of state secrets (Article 28). If the Network Operators discover that information involving state secrets is released through the internet and other public information network, they should immediately cease transmission, keep a copy of the relevant records, and report to the relevant public security organs, national security organs or the administrative departments safeguarding the secret (Article 28). At the request of the relevant public security organs, state security organs or the administrative departments safeguarding the secret, Network Operators should also delete any information which refers to the divulgence of state secrets (Article 28). Network Operators who violate the foregoing obligations will be subject to disciplinary actions.

The fact that the *Amended State Secrets Law* specifically and expressly states these obligations indicates that Network Operators are likely to be subject to greater scrutiny by public and national securities authorities and may be required to actively cooperate in criminal or administrative investigations.

III. Recommendations and Suggestions

It is important to emphasize that state secrets may still be legitimately acquired, so long as the disclosure of information is duly authorized, well documented and guidelines for storing and transmitting the information are properly adhered to. It is also not the case that companies would be held liable for obtaining business secrets *per se*. Such acts would only be illegal if the business secrets were obtained through theft, promise of gain, coercion or other improper means.

Under the current legal regime for the protection of state secrets and business secrets, it is important that appropriate compliance actions be taken to minimize exposure to legal risks associated with unlawful disclosure and handling of any such secrets. In this regard, it is recommended that companies should put in place compliance guidelines and hold regular trainings for members of their staff who may be exposed to, or who frequently deal with, politically or commercially sensitive information. It is also important for them to understand the internal control and procedures in place for the protection of state and business secrets adopted by CAEs, SOEs and other state entities, so as to better assess whether any information to be disclosed is duly authorized. Insofar as information volunteered by CAEs, SOEs or state entities in meetings or other occasions, especially in casual settings, it is important to clarify with the information provider whether he/she has the authority to disclose the information and whether there are any restrictions on the circulation of the information. Written records should also be kept on file to document the compliance measures undertaken.

Contacts

Friven Yeoh

Hong Kong
+852-3512-2369

Singapore
+65-6593-1800
fyeoh@omm.com

Bingna Guo

Beijing
+86-10-6563-4224

Shanghai
+86-21-2307-7000
bguo@omm.com



O'MELVENY & MYERS LLP

O'Melveny & Myers LLP is a foreign law firm registered with the Ministry of Justice of the People's Republic of China. Under current Chinese regulations, we are allowed to provide information concerning the effects of the Chinese legal environment, but we are not authorized to practice Chinese law or to render legal opinions in respect of Chinese law. We work in cooperation with a number of Chinese law firms. Should you require a legal opinion in respect of any Chinese law matter, we would be happy to assist you in obtaining one from a Chinese firm.

Portions of this communication may contain attorney advertising. Prior results do not guarantee a similar outcome. Please direct all inquiries regarding our conduct under New York's Code of Professional Responsibility to O'Melveny & Myers LLP, Times Square Tower, 7 Times Square, New York, NY, 10036, Phone: +1-212-326-2000. © 2010 O'Melveny & Myers LLP. All Rights Reserved.

Beijing

Yin Tai Centre, Office Tower, 37th Floor
No. 2 Jianguomenwai Ave.
Chao Yang District
Beijing 100022
People's Republic of China
+8610-6563-4200

Brussels

Blue Tower
Avenue Louise 326
1050 Brussels, Belgium
+32-2-642-4100

Century City

1999 Avenue of the Stars, 7th Floor
Los Angeles, CA 90067
+1-310-553-6700

Hong Kong

31st Floor, AIA Central
1 Connaught Road Central
Hong Kong S.A.R.
+852-3512-2300

London

Warwick Court
5 Paternoster Square
London, EC4M 7DX, England
+44-20-7088-0000

Los Angeles

400 South Hope Street
Los Angeles, CA 90071
+1-213-430-6000

New York

Times Square Tower
7 Times Square
New York, NY 10036
+1-212-326-2000

Newport Beach

610 Newport Center Drive, 17th Floor
Newport Beach, CA 92660
+1-949-760-9600

San Francisco

Two Embarcadero Center, 28th Floor
San Francisco, CA 94111
+1-415-984-8700

Shanghai

Plaza 66 Tower 1, 37th Floor
1266 Nanjing Road West
Shanghai 200040
People's Republic of China
+8621-2307-7000

Silicon Valley

2765 Sand Hill Road
Menlo Park, CA 94025
+1-650-473-2600

Singapore

9 Raffles Place
#22-01/02
Republic Plaza 1
Singapore 048619
+65-6593-1800

Tokyo

Meiji Yasuda Seimei Building
11th Floor
2-1-1, Marunouchi
Chiyoda-ku, Tokyo 100-0005,
Japan
+81-3-5293-2700

Washington, DC

1625 Eye Street, NW
Washington, DC 20006
+1-202-383-5300

www.omm.com