KING&WOOD MALLESONS
金杜律师事务所

Personal Information Protection under the Cybersecurity Law in China

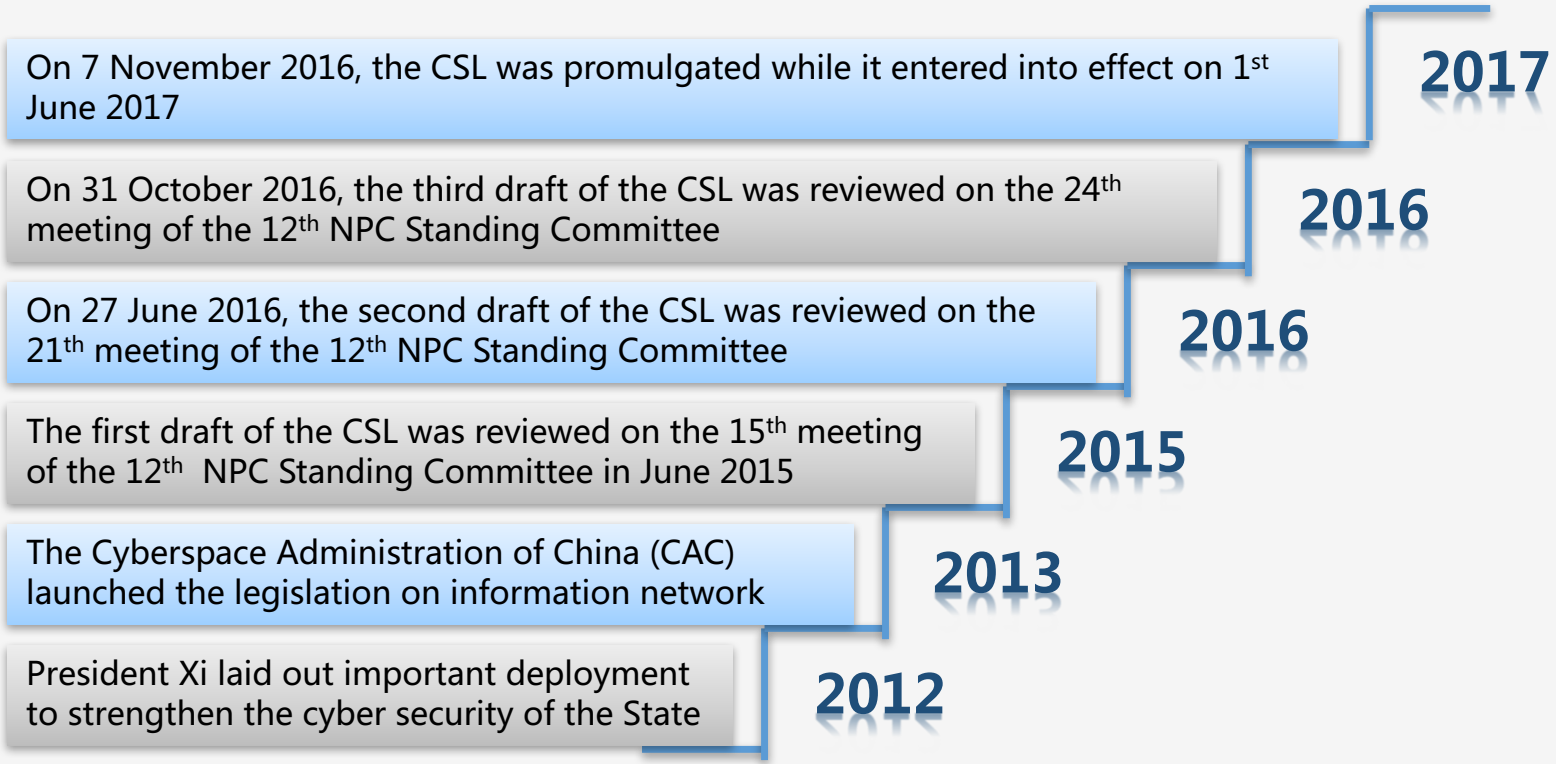
King & Wood Mallesons, Susan Ning (Senior Partner)

9 September 2017

Content

General Introduction of the CSL

Timeline of Legislation



Current Framework of the CSL

Network Security Review

Measures for the Security Review of Network Products and Services (Tentative)

Data Localization and Security Assessment for Cross-border Transmission

Draft Measures for the Security Assessment of PI and Important Data to be Transmitted Abroad (seeking public comments)

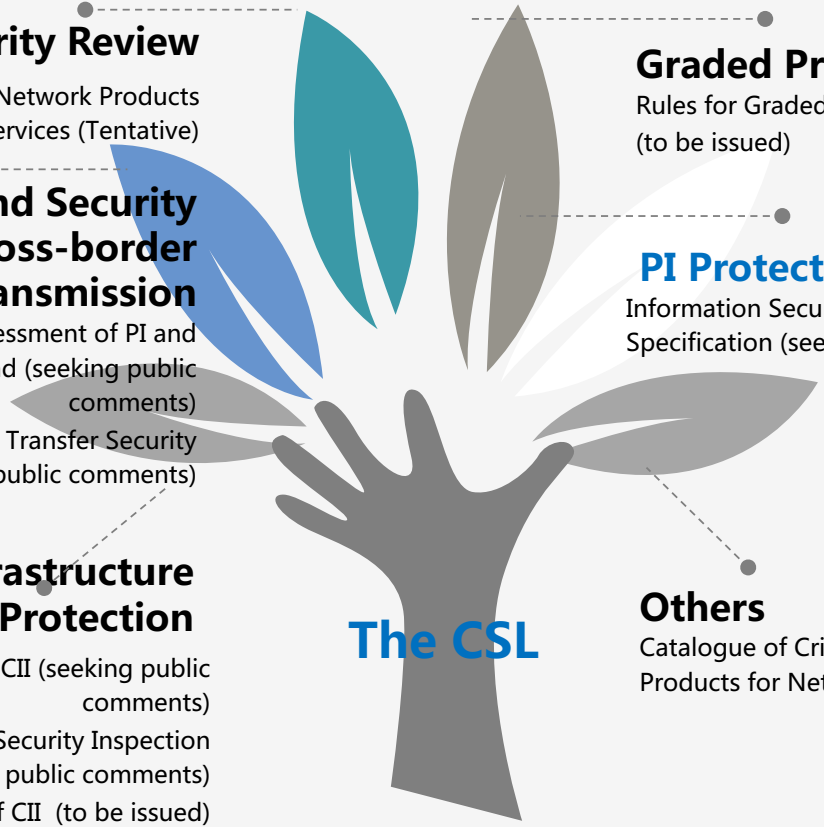
Guidelines for Data Cross-Border Transfer Security Assessment (seeking public comments)

Critical Information Infrastructure (CII) Protection

Regulations for the Security Protection of CII (seeking public comments)

Information security technology-Guide to Security Inspection and Evaluation of CII (seeking public comments)

Guidelines for Identification of CII (to be issued)



Graded Protection of Cybersecurity

Rules for Graded Protection of Network Security (to be issued)

PI Protection

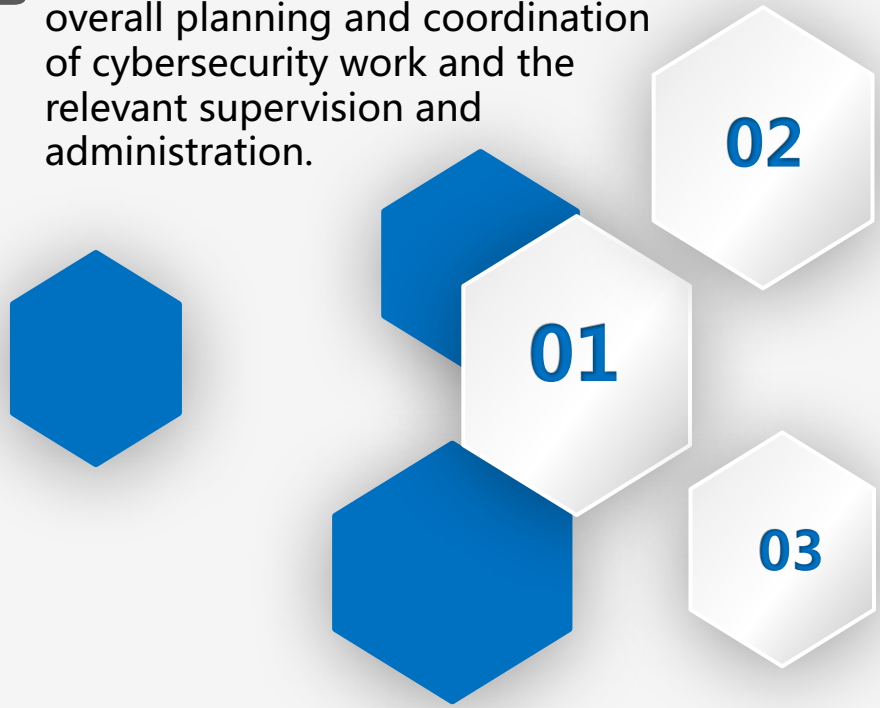
Information Security Techniques – Draft PI Security Specification (seeking final approval)

Others

Catalogue of Critical Network Equipment and Special Products for Network Security (1st Batch)

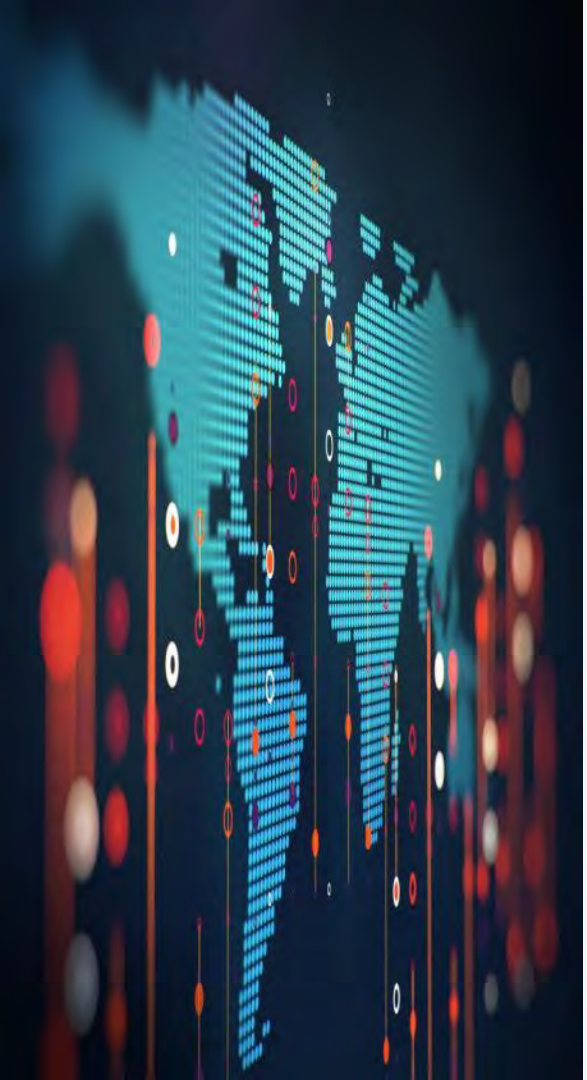
Law Enforcement Authority of the CSL

1. **The CAC** is responsible for the overall planning and coordination of cybersecurity work and the relevant supervision and administration.



2. **The authority in charge of telecommunication, the public security authority and other relevant authorities of the State Council** shall, within their respective scopes of responsibility, take charge of protection, supervision and administration of cybersecurity pursuant to the present Law and applicable laws and administrative regulations.

3. **Competent authorities of local people's governments at county level or above** shall take the responsibilities for cybersecurity protection and regulation in accordance with the relevant regulations of the State.



PI Protection under the CSL

Overview of Legislations on PI Protection

Before the CSL is promulgated, provisions of PI protection were scattered in several laws and rules. According to incomplete statistics, there are about 40 laws, 30 regulations, and almost 200 rules concerning PI protection.

Overview of major laws on PI before the promulgation of CSL

1. 2012 Decision on Strengthening Network Information Protection published by the Standing Committee of the National People's Congress
Including "electronic information that can be used to identify a citizen and involves a citizen's privacy" into scope of protection.

2. 2013 Provisions on Protecting PI of Telecommunications and Internet Users published by Ministry of Industry and Information Technology
Setting forth rules for collection and usage of PI by telecommunications business operators and internet services providers

3. Administrative Regulations on Credit Investigation Industry published by the State Council on January 21, 2013
Regulating collection, usage, storage, and processing of information related to credit business.

4. The 9th Amendment of Criminal Law published by the Standing Committee of the National People's Congress
Defining activities that "sell or provide PI of citizens to others in violation of relevant national provisions" as crime

5. 2016 E-Commerce Law (Draft) published by the Standing Committee of the National People's Congress
Setting forth regulation on PI protection involved in internet transaction.

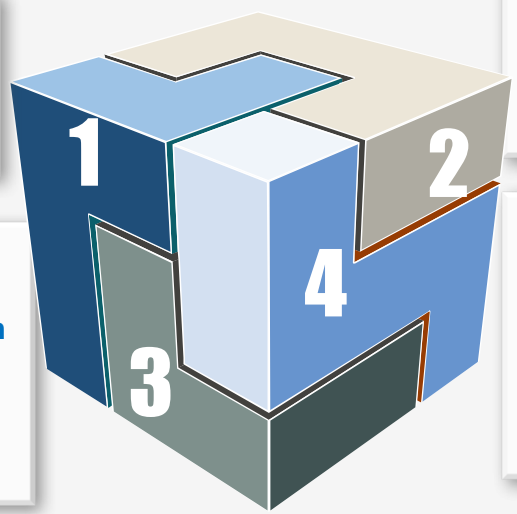
Breakthrough of PI Protection by the CSL

- The CSL lists the **basic principles and requirements for PI protection** that is tantamount to a small version of PI protection law, which allows follow-up relevant detailed rules and regulations and standards to have host law.

- The CSL also lists requirements for providers of network products and services, especially pointing to issues of some enterprises such as stopping services arbitrarily, threatening users based on monopolistic advantages, or collecting user information randomly.

1. For the first time, it establishes **the general definition of "PI"** in Law to ensure the fundamental system of PI protection

2. For the first time, it legally stipulates **storage place for certain PI** for protection the national information security
   - CII
   - PI and important data



3. For the first time, it **provides explicitly exceptions to prohibition on providing PI to others**
   - PI after processing, cannot identify a particular individual

4. For the first time, it **legally establishes administrative responsibility** when violating rules of PI protection
   - Unit responsibility and personal responsibility
   - The fines can amount up to one million RMB

The Scope of Personal Information ("PI")

- The definition of PI in current laws and regulations in force emphasizes its **Identifiable Character** → Personal Identifiable Information ("PII")

- **The CSL**

PI refers to various information which is recorded in electronic or any other form and used alone or in combination with other information to **recognize the identity of a natural person**, including but not limited to name, date of birth, ID number, personal biological identification information, address and telephone number of the natural person. (Art. 76)

- **Interpretation of Several Issues regarding Application of Law to Criminal Cases of Infringement of Citizen's PI Handled by the Supreme People's Court and the Supreme People's Procuratorate**

PI includes "name, identity document number, correspondence and contact information, address, account password, property status and **movement track**". (Art. 1)

- **Information Security Techniques – Draft PI Security Specification**

PI is any information that is recorded, electronically or otherwise, can be used solely or in combination with other information to **identify** the identity of a natural person or **can reflect activities of a natural person**. (Both identifiable character and correlation character)

Note: * The Scope of PI stipulated in other regulations governing specific industries, e.g. telecommunication, finance and etc.
** PI Security Specification is under further revision by relevant national authorities.

Discussion: vs. **"Personal Data"** under EU GDPR?

Basic Principles of PI Collection and Using

- **Article 111 of the General Provisions of the Civil Law**
  - Any organizations or individuals who need to obtain PI of others shall obtain the information in accordance with law and shall **ensure the information security**;
  - It is not allowed to illegally **collect, use, process or transmit** the PI of others;
  - It is illegal to **buy, sell, supply or make public** the PI of others.

Discussion:
Similar with EU GDPR? **Article 5 Principles relating to processing of personal data**

- **Article 41 of the CSL**

In the course of **collecting or using** PI, network operators shall:

- Abide by the **"lawful, justified and necessary"** principle;
- **Make public the rules** for collection and use;
- **Expressly notify** the data subject of **the purpose, methods and scope** of such collection and use;
- **Obtain the consent** of the data subject;
- **Not** collect PI that is not related to the services provided;
- **Comply with** laws and administrative regulations and **agreement with users**;
- **Process** the stored PI in accordance with laws and administrative regulations and **agreement with users**.

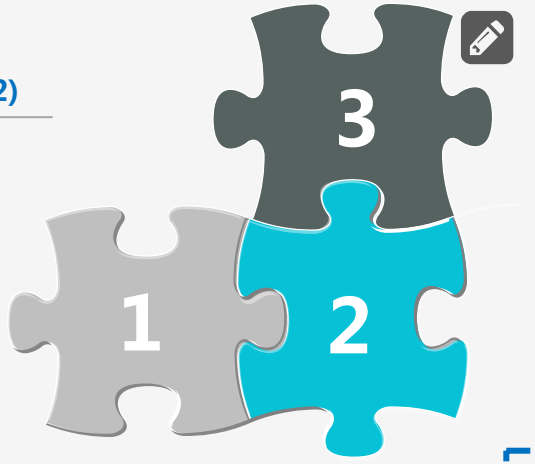
Extended PI Rights under the CSL

Based on rules of PI protection established, the CSL expands scope of PI rights from several perspectives and provides more comprehensive protection.

Extend citizen's right to be informed (Article 22 and Article 42)

Network operator or network service provider should inform customers promptly if:

- (1) there is disclosure, damage or loss of, or possible disclosure, damage or loss of such information; or
- (2) any risk such as security defect or bug of their network product or service is found.



Establish the right to delete leaked information (Article 43)

- Each individual is entitled to require a network operator to delete his or her personal information if he or she founds that the network operator's collection and use of such information violate (1) the laws, administrative regulations, or (2) the agreement by and between such operator and him or her.

Establish the right to correct errors in information (Article 43)

- Each individual is entitled to require a network operator to make corrections if he or she founds errors in such information collected and stored by such operator.

Discussion: MORE under EU GDPR, e.g.?

- Right of Access;
- Right to Erasure
- Right to Data Portability

Also **MORE** in Chinese **recommended national standard**:

- Draft PI Security Specification

Legal Liabilities for PI Infringement

➢**Administrative liabilities**

According to the CSL, infringement upon any right in PI may be subject to warning, confiscation of illegal earnings, suspension of related business, winding up for rectification, close of website, and revocation of business license.

To be specific:

- The supervisor directly in charge and other directly liable persons are subject to a fine up to RMB 100,000.
- Network operator is subject to a fine up to RMB 1million.

Compared with previous rules, the CSL distinctly **increases the fines** imposed on illegal activities.

Compared with the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection, the CSL **adds fines imposed on directly liable persons,** and **explicitly lists several penalties** when infringement of PI is severe, i.e. suspension of related business, winding up for rectification, close of website, and revocation of business license.

Legal Liabilities for PI Infringement

- **Civil liabilities——*Article 74(1) of the Cybersecurity Law : In case of violation of the present Law and any harm caused to others, the civil liability shall be borne pursuant to the laws.***

- **General Rules of the Civil Law**

Article 111 Natural persons' PI shall be protected by law. Any organizations and individuals who need to obtain PI of others shall obtain the information according to law and shall ensure the information safety. It is not allowed to illegally collect, use, process or transfer the PI of others. It is illegal to buy and sell, supply or release the PI of others.

- **Tort Law——Protects privacy right of natural person as one of civil rights.**

Article 2 Persons who infringe civil rights and interests shall bear tort liability pursuant to this Law.

- **Relevant clauses in other laws and regulations**

Law on Protection of Rights and Interests of Consumers

Article 50 A business operator which infringes upon consumers' dignity, personal liberty or lawfully protected PI of consumers shall stop infringement, reinstate reputation, eliminate impact, apologize and compensate losses.

Legal Liabilities for PI Infringement

- **Criminal liabilities ——*Article 74(2) of the CSL Any violations of the present Law which constitutes… crimes shall be subject to investigations on criminal liabilities.***

- Criminal Law, the 7th Amendment to Criminal Law, the 9th Amendment to Criminal Law
- Interpretation of Several Issues regarding Application of Law to Criminal Cases of Infringement of Citizen's PI Handled by the Supreme People's Court and the Supreme People's Procuratorate
- The Interpretation sets different conviction standards depending on type, quantity, and subject of information, and provides calculation rules of information numbers. Details are as follows:

Type of information	Information content	Conviction standard	
		General condition	Professional
Sensitive information	Whereabouts information, communication content, credit information, property information	50 pieces/illegal gains of RMB 5000	25 pieces/illegal gains of RMB 2500
Important information	Accommodation information, communication records, health and physiological information, transaction information and other personal information that may affect personal and property safety	500 pieces/illegal gains of RMB 5000	250 pieces/illegal gains of RMB 2500
Other information	Personal information other than above two types	5000 pieces/illegal gains of RMB 5000	2500 pieces/illegal gains of RMB 2500

Compliance Issues in Data Storage and Transmission

Data Storage Within China

➢ Within the Territory of the PRC

- **Article 37 of the CSL**：CII operators shall store PI and important data collected and generated during its operation in the PRC within the territory of the PRC.
- For the above purpose, "the PRC" **does not include** Hong Kong, Macau and Taiwan.

➢ The Standard of "to be Stored within the Territory of the PRC"

- All **copies of the data** shall be stored within China.
- The **physical equipment** containing the data, such as data center and cloud processors, shall be located within China.

➢Suggestions

- Be well prepared for responding to this requirement, from technical methods to physical equipment;
- Closely keep track of the associated regulations and rules promulgated in future.

Cross-Border Data Transmission - Outbound (1)

- **Overall legal basis**
- Comprehensive regulation
  - The CSL

    The PI and important data generated or collected by a CII operator during its operation **within the territory of the PRC** shall be stored **within the PRC**. Where such information and data have to be provided abroad **for business purpose**, **security assessment** shall be conducted pursuant to the measures developed by the CAC together with competent departments of the State Council; unless provided for in other laws and administrative regulations, such laws and administrative regulations shall prevail.

  - The Law on Guarding State Secrets
  - Information Security Technology – Guidelines of PI Protection in relation to Pubic or Commercial Information System
  - Opinions for the development of Information Technology and Protection of Information Security
- Regulation by industry


Cross-Border Data Transmission - Outbound (2)

➢ **Cross-border Data Transmission under the CSL**

- CAC published the Measures for the Security Assessment of PI and Important Data to be Transmitted Abroad (seeking public comments) (hereinafter referred to as "*Draft Assessment Measure*") on 11 April 2017
- The National Standardization Technical Committee for Information Security published *the Guidelines for Data Cross-Border Transfer Security Assessment (Draft)* (hereinafter referred to as "*Draft Assessment Guideline*") to seek public comments for the second time on 30 August 2017.
- **Parties under regulation:**

☐ **Network operators** (Art. 2 of the Draft Assessment Measures)

☐ **CII operators** (Art. 37 of the CSL)

- Requirement of local storage
- Different requirements on data export
- Storage of assessment result and data export log for at lease 2 years
- Provision of grace period

Cross-Border Data Transmission - Outbound (3)

- **Restrictions on data export initiated by network operators**

  - Prohibition on data export
  - Data export after self assessment and filing the assessment result to industrial competent authorities
  - Data export after self assessment

- **Threshold** for filing the assessment result to industrial competent authorities
  - the data contains PI of over 500,000 individuals **in one year;** or
  - Important data related to **sensitive industries**; or
  - May affect national security, economic development, social and public interests

When data export is necessary for business purpose, **CII operator** should conduct self-assessment and seek approval from industrial competent authority before the data export .

Discussion: vs. EU GDPR?
Article 45 Transfer on the basis of an adequacy decision
Article 46 Transfer subject to appropriate safeguard
Article 47 Binding Corporate Rules

- **Obligation of conducting security assessment annually/Re-assessment**

Cross-Border Data Transmission - Outbound (4)

➢**Liability**

Article 66 of the CSL

- A CII operator which stores or exports network data in violation of the CSL shall be:
  - Ordered to make rectifications; Warned;
  - Confiscation of illegal earnings;
  - Imposed a fine between RMB 50,000 and RMB 500,000 ;
  - Suspension of related business, winding up for rectification, shutdown of website, and revocation of business license;
- **The supervisor directly in charge and other directly liable persons** shall be subject to a fine between RMB 10,000 and RMB 100,000

Article 14 of the Draft Assessment Measures

- Violations to these Measures shall be penalized in accordance with relevant laws and regulations.

Cross-Border Data Transmission - Outbound (5)

➢ **The Draft Assessment Guideline**

- published by the National Standardization Technical Committee for Information Security and General Administration of Quality Supervision, Inspection and Quarantine of the People’s Republic of China
- the National Standard mentioned in the Assessment Measures (two appendixes) : **Refine and Supplement** the date export assessment under the framework of the Assessment Measures
- Recommend National Standards (GB/T): **Not mandatory**, but reflecting the regulatory attitude to a certain extent and providing more practical guidelines for data export security assessment
- **Scope of Application**

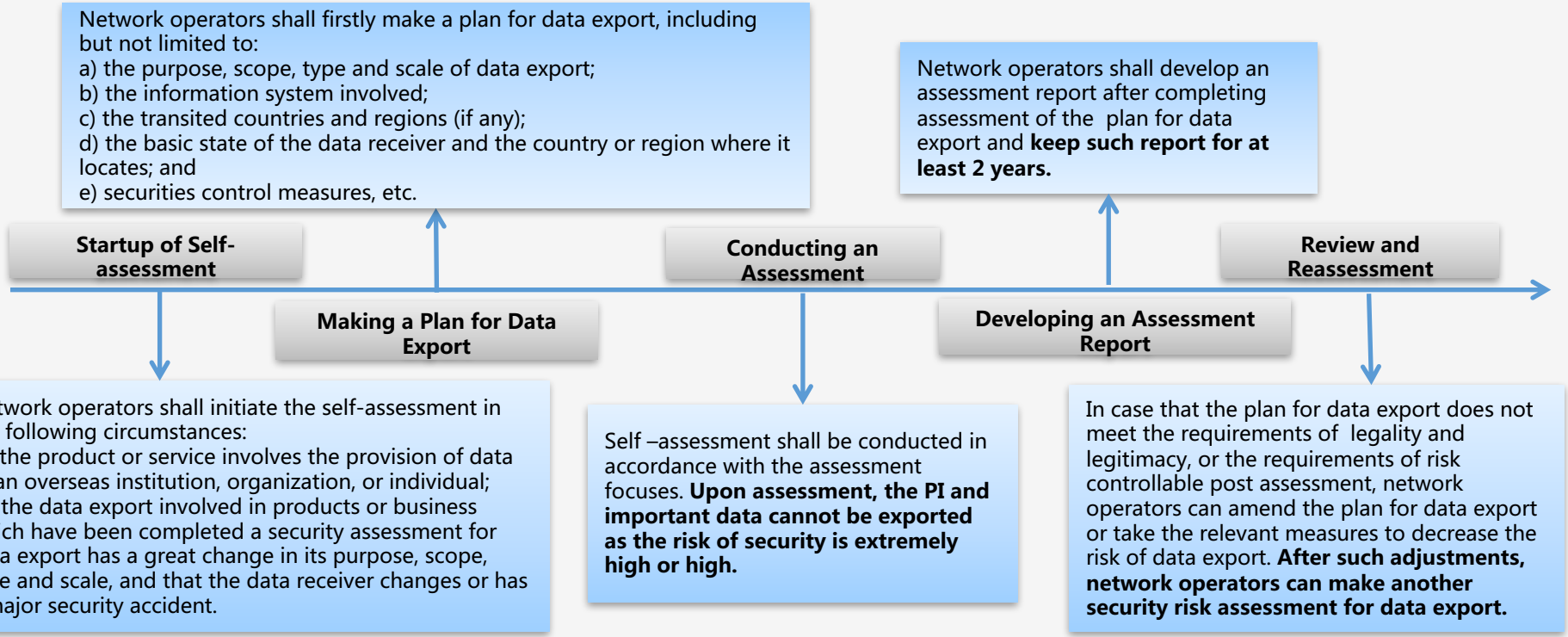
☐ Self-assessment by network operators

☐ Guidance and supervision by industrial authorities and regulators on network operators' self-assessment

☐ Assessment conducted by the cyberspace administration, industrial authorities and regulators in light of their duties (for reference)

Cross-Border Data Transmission - Outbound (6)

- **Assessment Processes**




Thanks
susan.ning@cn.kwm.com