Appendix:
ICS 35.040
L80

National Standard of People's Republic of China

GB / T XXXX - XXXX

Information Security Technology-Guidelines for Data Cross-Border Transfer Security Assessment

(Draft)

Released by XXXX - XX - XX Implemented by XXXX - XX - XX

Released by General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China and Standardization Administration of the People's Republic of China

Table of Contents

Preface

This Standard is drafted according to the provisions of GB / T 1.1-2009.

This Standard is proposed and centralized by the National Information Security Standardization Technical Committee (SAC / TC260).

Drafting unit of this Standard:

Main drafters of this Standard:

Introduction

In recent years, with the rapid development of the Internet, data flows everywhere., economic and social value generated by the data flow has been highlighted and the security risks in this process also increase. national security, public interests and personal privacy have received serious threat, to prevent the risk of data leakage and misuse is arising increasingly and urgently.

This Standard specifies the data cross-border transfer security assessment process, assessment points assessment methods and other content, network operators conduct a security assessment of their personal information and important data cross-border transfer as this guideline. If they find safety problems and risks, measures shall be taken timely to prevent personal information cross-border transfer to prejudice the legitimate interests of personal information subject, to prevent important data cross-border store without the national safety assessment and approval of the appropriate authority to adversely affecting the national security.

Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment

1 Range

This Standard specified the work requirement, process flow, assessment content and determicountry results of personal information and important data cross-border transfer assessment.

This Standard applies to personal information and important data cross-border transfer security assessment carried out by the network operator, also applies to the competent and regulatory authorities to guide and monitor the personal information and important data cross-border transfer security assessments by the network operator.

Cyberspace administration and, competent and regulatory authorities in charge of personal information and important data cross-border transfer security assessment can refer to this Standard.

2 Normative References

The following documents for the application of this document is essential. For all the reference documents, only the dated edition is applicable to this document. For undated references, the latest edition (including any amendments) applies to this document.

GB / T 25069-2010 *Information Security Technology - Terms*

GB / T AAAA *Information Security Technology - Personal Information Security Specification*

3 Terms and Definitions

The following terms and definitions apply to this document.

3.1

Network Operator

Network operators referred in this Standard mean the owner, managers and service providers of the network. .

3.2

Data

Data referred in this Standard means the personal information and important data in the electronic form collected and generated during operators' operating within the territory of the People's Republic of China.

3.3

Personal Information

Various information in electronic form or other means capable of recording alone or in combicountry with other information to identify natural individuals identity or to reflect the activities of specific natural persons, include but not limited to, the natural person's name, date of birth, ID number, contact details, personal biometric information, address, account password, property status, location, behavior information, etc.

3.4

Sensitive Personal Information

Personal information, once the leak, illegally providing or abuses, might endanger the safety of persons and property, harm personal reputation and the physical and mental health, resulting in discriminatory treatment, etc.

3.5

Important Data

Data closely related to national security, economic development, and social and public interests, for detailed scope, reference to Appendix A.

3.6

Data Cross-border Transfer

One-time events or continuity activities of making collected and generated important data and personal information in electronic form, in the territory of the People's Republic of China, available to foreign institutions, organizations, individuals.

Note: Foreign data transfer via the People's Republic of China, without any change in circumstances or data processing does not belong to the data cross-border transfer.

3.7

Risk of Data Cross-borders Transfer

Exit and then transfer the data after the leak, damage, tampering, abuse and other possible risks to national security, public interests, the legitimate interests of individuals brought.

3.8

Provide

The network operator initiative to provide data to foreign institutions, organizations or individuals, or distribute the data in other ways, including its user function of product or service offered by network operators, and provide data to overseas institutions, organizations or individuals.

Note: Except that network operators who disclosed data in accordance with law.

3.9

Self-assessment

Network operator conduct data cross-border transfer security assessment in accordance with the national laws and regulations and relevant standards.

3.10

Data Desensitization

Network operators conduct deformation processing of sensitive data through data transformation rules, to reach protection of the privacy and sensitive data.

3.11

Data Protection Capability

Network operators' ability to ensure data security in storage, processing, transmission of data.

4 Evaluation Process

4.1 Start Self-Assessment

Network operators should start self-assessment in the following cases:

a) the product or service involves providing data to overseas institutions, organizations or individuals;

b) data cross-border transfer involved in the product or service, which has completed the security assessment, has greater change in the purpose, scope, type, quantity, etc., the data receiver changes or major security incidents occur.

4.2 Develop Data Cross-border Transfer Plan

Network operators should first develop data cross-border transfer plan, the contents of the plan include, but not limited to:

a) purpose, scope, type and scale of data cross-border transfer;

b) related information system;

c) transit countries and regions (if any);

d) basic situation of data receiver and the country or region where it locates;

e) safety control measures.

4.3 The legality and risk control of assessment of data cross-border transfer plan

First of all, evaluate the legality and legitimacy of data cross-border transfer; data cross-border activities without the legitimacy and legality are not allowed transferred border. On this basis, the risk control of data cross-border transfer plan can be evaluated, to effectively prevent leakage,, destruction, alteration, misuse and other risks of data cross-border transfer and retransfer. Specific procedure is shown as Figure 1.

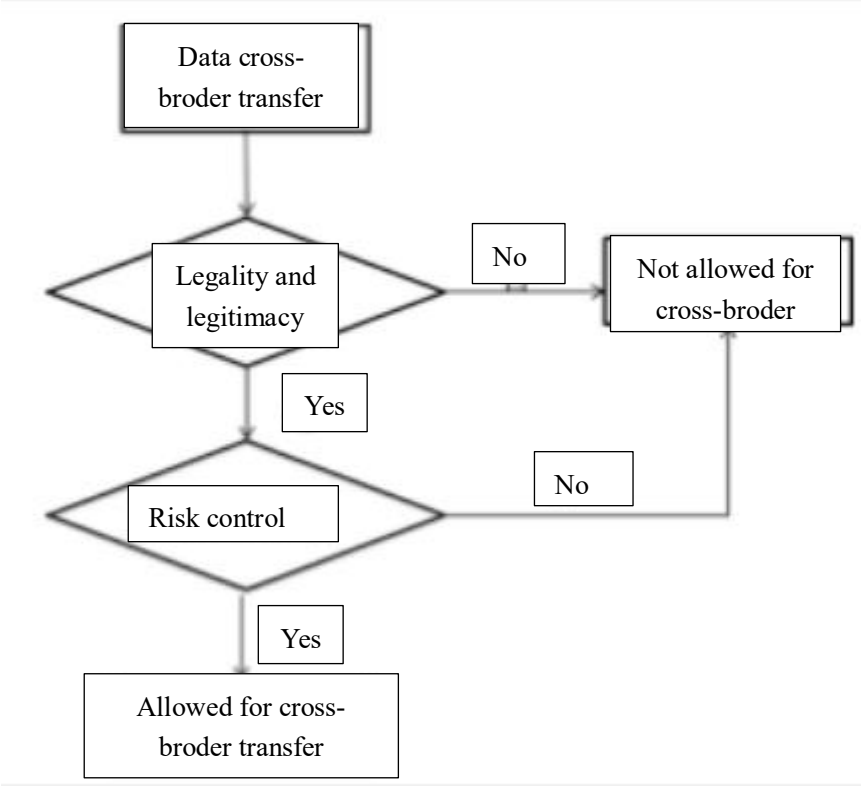

Figure 1 Data cross-border transfer safety assessment principles

4.4 Assessment points and Methods

Network operators are required to follow the assessment criteria in Chapter 5 for self-assessment, assessment methods refer to Appendix B; if after the assessment, the security risk is very high or high personal information and important data shall not transferred border.

4.5 Assessment Report

The network operator, after the completion of the assessment of data cross-border transfer plan, should form the assessment report, assessment report should be kept for at least five years.

4.6 Check and Amendment

If the data cross-border transfer plan does not meet the proper and legal requirements, or after assessment does not meet the requirements of risk control, network operators can correct the plan, or adopt relevant measures to reduce the risk of data cross-border transfer and re-conduct self-assessments.

Note: The measures can be used to reduce the data cross-border transfer security risks include, but not limited to: to streamline content, use technical measures to process the data to reduce sensitivity, enhance data sender security capabilities, limit processing activity of data receiver, replace with data receiver with higher protection level, select the data receiver in the religion with higher political and legal environment support capacity. After making adjustments, data cross-border transfer security assessment can be conducted again.

5 Evaluation Essentials

5.1 Legality and Legitimacy

Data cross-border transfer should also meet the requirements of legality and legitimacy:

a) Legality include:

1) not prohibited in laws and regulations;

2) in line with the treaties, agreements signed by Chinese government with other countries and regions;

3) authorized with consent of the personal information subject, except the emergency endangering the safety of life and property of citizens;

4) not belong to the prohibited scope of cyberspace administration, public security departments, security departments and other relevant departments for data cross-border transfer.

b) Legitimacy include:

1) network operators are required to engage in normal activities within the legal scope of business;

2) necessary to fulfill contractual obligations;

3) required by legal obligation;

4) needed for judicial assistance;

5) necessary to maintenance cyberspace sovereignty and national security, public interests, protect the legitimate interests of citizens in need.

5.2 Risk Control

5.2.1. Outline

Risk control of the data cross-border transfer plan should consider the properties of data transferred border and possibility of security incidents:

a) Data property:

1) personal information property, including the number, scope, type, sensitivity, technical handling, etc.;

2) important data property, including the number, scope, type and technical handling, etc..

b) Possibility of data cross-border transfer security incidents:

1) technical and management capabilities of the data sender;

2) security and protection measures taken by the data receiver;

3) political and legal environment where the country or region.

5.2.2. Personal Information Property Assessment Points

5.2.2.1 Type and Sensitivity

We should identify the information type contained in the personal information, and determines the number of sensitive personal information which are involved.

5.2.2.2 Quantity

The quantity of personal information subject and group characteristics of the main group involved should be evaluated, when the quantity of personal information subject involved in the data cross-border transfer reaches or exceeds certain magnitude or is involved in a particular group, personal information will be provided with derived value after data collection.

5.2.2.3 Range

Personal information cross-border transfer scope should be evaluated for compliance with the minimization principle:

a) personal information in cross-border transfer should be directly associated with the service function related to cross-border. That direct association means that no the information participation, no corresponding function can be achieved;

b) personal information frequency in cross-border transfer should be the minimum value required by service function related to cross-border;

c) the amount of personal information in cross-border transfer should be the minimum amount required by service function related to cross-border.

5.2.2.4 Technical Handling

The technical processing of personal information shall be assessed, including:

a) whether it use technical measures for the desensitization treatment of personal information;

b) whether desensitizing effect is valid and reliable, reaching a reasonable degree of irreversibility.

5.2.3 Important Data Property Assessment Points

5.2.3.1 Types

Important data types should be evaluated, which includes whether covering the data in areas of nuclear facilities, chemical and biological, defense industry, population health, the data of large-scale engineering activities, the marine

environment and sensitive geographic information, system vulnerabilities of critical information infrastructure, leaks or abuse situation of network security information such as security protection and other important data which will have a serious impact on national security and public interests.

5.2.3.2 Quantity

The quantity of important data in cross-border transfer and the social and economic values it contained should be assessed, the greater the number, the leak occurred, the time of disclosure or misuse, the greater the risk of national safety hazard and public interests in case of the leakage, disclosure or misuse.

5.2.3.3 Range

Important data scope should be consistent with the principle of minimum:

a) personal information in cross-border transfer should be directly associated with the service function related to cross-border. That direct association means that no the information participation, no corresponding function can be achieved;

b) personal information frequency in cross-border transfer should be the minimum value required by service function related to cross-border;

c) the amount of personal information in cross-border transfer should be the minimum amount required by service function related to cross-border.

5.2.3.4 Technical Handling

The technical processing of personal information shall be assessed, including:

a) whether it use technical measures for the desensitization treatment of personal information;

b) whether desensitizing effect is valid and reliable, reaching a reasonable degree of irreversibility.

5.2.4 Data cross-border transfer technology and management capabilities of the sender

5.2.4.1 Management System Support Capabilities

a) Safety management system:

1) provided with data security management system, including security policy, management systems, and cross-border transfer operation procedures;

2) security policy management file contains the overall objectives, the scope of important data, cross-border transfer principle, overall security framework of cross-border transfer, etc.;

3) the data cross-border transfer security management system should cover the number, scope, type and sensitivity and other content;

4) the personal information data should reflect the security operation flow of cross-border transfer, including the process and subsequent security;

5) the implementation of strict safe operating procedures of cross-border transfer for critical data, including the process and subsequent security.

b) Personnel management mechanisms:

1) designated full-time management staff within the organization should be appointed specially for cross-border transfer, and be ensured to fulfill their respective responsibilities, including but not limited to: audit,

compliance management, writing and submit of assessment report for data cross-border transfer, cooperating with the competent department in charge of supervision, inspection and dealing with disputes;

2) establishment of personnel training system, personnel training mechanism should be established within the organization to ensure the training of personnel to meet training requirements for data cross-border transfer.

c) Signing of a contract with the data receiver, and the content shall include:

1) establish a data security audit mechanisms, develop audit requirements, carry out the audit in accordance with auditing requirements;

2) cooperate with the network operator or personal information subject to investigate reasonably data cross-border transfer activities;

3) in addition to the law, without obtaining authorization network operators as well as knowledge of personal information subject and consent of the premise, data receiver shall not process, disclose and transfer the data;

4) take appropriate technical security measures to protect the confidentiality and integrity of data.

d) Audit mechanism:

1) audit data cross-border transfer protection policies and the effectiveness of procedures, processing, and security measures, and form the audit results. Audit results should be able to support the disposal of the incident, emergency response and subsequent investigation;

2) during the audit, security measures shall be taken to prevent unauthorized access, alteration or deletion.

e) Emergency plan:

1) when the data cross-border transfer may cause harm to the data subject rights, data cross-border transfer should be terminated immediately, and the emergency plan mechanism shall be immediately launched, with measures to protect the rights of the data subject;

2) the behavior, reason and emergency measures and other related information should immediately reported to the data regulatory agencies;

3) when emergency handling is judged unreasonable or unnecessary by data regulators, network operators should immediately make corrections as required.

f) Complaints and disposal strategies:

1) ensure that relevant data subject can through the mechanism appeal for behavior in data cross-border transfer;

2) designate independent person with appropriate permissions responsible for handling complaints of all of the data subject;

3) flow information, etc. of complaints handling mechanism for data cross-border transfer is required to be disclosed to the data subject.

g) Security event reporting mechanism:

1) reporting trigger condition, including data leak occurring, data lost, the data receiver’s breach of contract for data processing, as well as all every behavior that may endanger national security, harm the public interest, violate the law or infringes the rights of the data subject;

2) report content, including the time of emergency, the data type, size and content.

5.2.4.2 Technology Support Capabilities

a) The overall safety technology

1) establish and improve the data transfer protection measures;

2) adopt protective measures in security border and conduct regular security assessments and audits;

3) detect and repair existing security vulnerabilities;

4) possess account rights management technology, to prevent unauthorized access to data.

b) Data cross-border transfer log retention. data cross-border transfer log retention mechanism should be established in advance, the retained information should include, but not limited to: audit report, data cross-border transfer, logs and other data accessing logs..

5.2.5 Safety Protection Capability of Data Receiver

5.2.5.1 Subject Review

a) It should have legal qualifications, such as business license, organization code certificate, tax registration certificate;

b) Business scope should consistent with the content and type of the received data;

c) No major violations record, including large-scale personal information leakage and misuse of personal information in violation and other records;

d) For important data, background of data receiver shall be evaluated..

5.2.5.2 Management Support Capabilities

a) Institution building:

1) clear data security function framework should be established with definition of data security duties;

2) full-time team of data security compliance should be set, to identify security compliance requirements data the stage of receiving data;

3) data security functions work practices should be developed to clear collaboration between the various functional positions and clarify the running mechanism of the functions and posts. .

b) System process:

1) develop and implement top-level policy, strategy of data security management, based on business needs and compliance requirements;

2) establish the data safety management system in reception, storage, use, transfer, destruction, put forward safety management requirements in various stages, and establish a reasonable mechanism to ensure normalization of the developing, publishing, revision of system;

3) the prevention, early warning, emergency response, accountability mechanism of data security risks should be established;

4) data security management identification procedures should be established, to identify security support requirements of data and implement the relevant requirements in the existing data security controls.

c) Personnel ability:

1) personnel within the organization should have a good sense of data security;

2) personnel in data security positions should have professional data security capabilities;

3) overall staff responsible for receiving data should be able to understand and implement data security compliance requirements.

5.2.5.3 Technical Support Capabilities

a) Security technology capabilities:

1) be provided with prevention, detection and response capabilities for data security risks;

2) be provided with the ability to confidentiality, integrity, consistency, availability, traceability, authenticity of the received security data;

3) be provided with the overall data protection and security technical emergency support system;

4) be provided with the identity and rights management ability of data accessing;

5) be provided with the ability to identify and record data receiving source ;

6) be provided with the security management ability to data storage medium;

7) be provided with the ability to monitor and audit each stage of data reception, storage, use, transport, destruction, etc.

b) Information system:

1) information system planning, construction, deployment, and operation & maintenance of information systems should comply with the safety requirements of the country or region;

2) information system should have the ability to ensure data security, including identity and rights management, risk management, emergency management, back recovery, and log management.

c) Automated tools:

1) the automatic support ability to data security by using technology tools should be provided;

2) automation tools should be provided to monitor and audit the stages of data receiving, storage, use, transport and destruction;

3) the unified technical tools should be established for data backup and recovery;

4) technical tools should be provided to protect network security, detect and limit DDOS, network attacks, data reptiles and other abnormal behavior launched from inside or outside

5.2.6 Political and Legal Environment of country or Region where Data Receiver Locates

5.2.6.1 Personal Information

Only when it comes to personal information cross-border transfer, assessment of the political and legal environment country or region where the data receiver locates should include:

a) the country or region's current personal data protection laws, regulations, standards, difference obtained through comparison with the protection provided by the personal information the laws, regulations and standard in our China;

b) regional or global mechanisms for the personal information protection which the countries or regions join, as well

as the binding commitments they made;

c) implementation of mechanisms to protect personal information in the countries or regions, such as whether there is the legal personal information protection agency, the relevant judicial mechanism, industry self-regulation association and mechanisms, as well as the effectiveness of administrative and judicial relief channels for individuals.

5.2.6.2 Important Data

When it comes to important data cross-border transfer, assessment on the political and legal environment of the naiton or region where the data receiver locates include:

a) assessment content Standard 5.2.6.1;

b) the country or region's existing laws, regulations and standard situation in terms of data security;

c) the country or region's mechanisms to implement data security, such as the competent authority, the relevant judicial mechanism and industry self-regulation association and self-regulation mechanisms of network security or data security;

d) the country or regional government, including law enforcement, national defense, national security and other departments' right to obtain legal authority;

e) bilateral or multilateral agreements between the country or the region and other countries or regions in the relevant aspects of data flow and sharing, including bilateral and multilateral agreements of data flow and sharing in terms of law enforcement, regulatory and other aspects.

Appendix A

(Normative Directory)

Important Data Identification Guidelines

Important data in the guidelines refers to the data not involved in state secrets but closely related to national security, economic development and public interest (including raw data and derived data) collected and generated by Chinese government, enterprises and individuals in the territory, once with unauthorized disclosure, loss, misuse, alteration or destruction or after convergence, consolidation and analysis, the following consequences may be caused:

(a) endanger national security, national defense interests, and undermine the international relations;

(b) damage to state property, public interests and the legitimate interests of individuals;

(c) affect countries to prevent and combat economic and military espionage, political infiltration and organized crime;

(d) impact administrative agencies in the investigation and dealing with illegal activities and malfeasance or suspected illegal activities and malfeasance according to the law;

(e) interfere with government departments to carry out supervision, management, inspection, audit and other administrative activities according to law, hinder government departments to perform their duties;

(f) endanger national critical infrastructure and critical information infrastructure, security of government systems and information systems;

(g) impact or jeopardize the country's economic order and financial security;

(h) state secrets or sensitive information can be analyzed;

(i) affect or harm national politics, land, military, economic, cultural, social, technological, information, ecology, resources, nuclear facilities and other security matters.

According to relevant regulations defined above and industry (field) authorities, guidelines suggest a range of important data of various sectors (areas). Please the competent authorities in all sectors (areas), combining with reality, clear the industry (field) important data definitions, scope or judgment based; and update or replace relevant content in this guideline according to industry (field) developments. .

This guideline does not affect the implementation of China's obligations under the on *WTO Agreement* and other International Agreement.

A.1. Natural Gas

Competent authority: National Development and Reform Commission and National Energy Administration

Important data include, but not limited to:

a) the type of value, including information indicating the amount of resources and so on;

b) the type of production, including various production information;

c) the type of sales, including various sales information;

d) the type of construction amount, including various construction amount information;

e) the type of safety and environmental protection, including information of measurement management, energy

management, labor supplies, dangerous work area, quality control, etc.;

f) the type of reserve, including the information about the number of reserves, reserve facilities location coordinates.

A.2. Coal

Competent authority: National Development and Reform Commission and National Energy Administration

Important data include, but not limited to:

a) the basic situation of the industry, mainly including the number of enterprises, enterprise distribution, enterprise type, number of employees, employees distribution, etc.;

b) industry economic conditions, mainly including assets, liabilities, income, profits, major economic indicators, industry tension level of industry funding, etc.;

c) industry procurement, mainly including purchases of raw materials, purchase amount, purchase price and procurement cycle, etc.;

d) industry production, mainly including the output value of the industry, production inputs, labor productivity, capacity and capacity factors, etc.;

e) industry sales, mainly including market size, investment sales, the sales level per capita, the main product selling prices;

f) industry investment, mainly including the number of new projects in the industry, investment, sources of funding, etc.

A.3. Petrifaction

The competent authorities: National Energy Administration

Important data include, but not limited to:

a) main economic indicators and major policy measures in the annual and long-term development plan of the national petroleum and petrochemical industry;

b) annual import plan of important production materials in petrochemical industry and the undistributed amount of controlled foreign exchange.

A.4. Electric Power

Competent authority: National Development and Reform Commission and National Energy Administration

Important data include, but not limited to:

A.4.1 Power Plant Information

a) The amount of coal in thermal power plant, water consumption in hydraulic power plant and other information;

b) Data of generator set, including reliability index data and information of generator set, like thermal power and hydro power;

c) Switch data within the substation in the power plant, comprising substation name, switch type, reactance value, bus voltage, input time, exit time and other information.

A.4.2 Transmission and Distribution Information

a) Actual load, load prediction and other information;

b) Power transmission equipment reliability indicators, including voltage level, statistics of several hundred sets, failure rate, failure times, failure downtime, repair time, inspection rate, average inspection time and other information;

c) Information of transmission lines, including the line segment number, names of the side, side switch number, parallel number, side province name, scheduling weight, line length, conductor type, ground line type, safe current, control current, conductor arrangement, positive-sequence resistance, etc.;

d) Loss consumption, environmental information that impacts line status, etc.

A.4.3 Construction and Operation & Maintenance Information

a) Installed capacity, power generation, supply and other information;

b) Year-on-year and month-on-month increase information;

c) Each power system configuration information, including distribution automation systems, production management systems, outage management systems, advanced metering system, power quality monitoring system, and user energy efficiency management system, etc.;

d) Power running information of each system, including voltage, current, frequency, waveform, etc.;

e) Real-time monitoring of the power system state, electric power system inspection, power scheduling, etc.;

f) Statistical analysis of reliability, including availability factor, forced outage rate, available hours MTBF, failure rate, repair rate, etc.

A.4.4 Other Information

a) Each power system assets and supporting security system-related information;

b) Unpublished grid/power plant plans, etc;

c) Urban distribution pipeline and grid graphic information;

d) Geographic coordinate information of power network;

e) Additional information that can contribute to the attack power infrastructure invasion.

A.5. Communicate

Competent authority: Ministry of Industry and Information Technology

Important data include, but not limited to:

A.5.1 Construction and Planning Data

It mainly include important data of telecommunications networks, Internet networks and information systems generated in the planning and construction sectors, such as planning and building programs, disaster backup system design and construction program, device location, network topology, line routing, purchases lists of equipment asset, etc.

A.5.2 Operation & Maintenance Data

It mainly includes the importance data collected and generated in network and information system maintenance, such as equipment and software configuration information, IP address allocation information and the external network switching information, network traffic flow information, network and system running information, network and system operation

maintenance log, the system user profile information, etc.

A.5.3 Security and Protection Data

a) Network and information security management data, such as early warning and monitoring information of network security, systems and data access operations log, security audit record record, network security contingency plans, data related to monitoring and disposal of illegal and harmful information, user log of accessing the Internet, personal communication data such as user charging data and Internet records;

b) Emergency communication data, such as emergency communications system planning, construction, operation and other relevant information; emergency communications event grading and emergency plans, action programs of major events, security plan information, emergency communication equipment and material storage and deployment support team.

A.5.4 Radio Data

a) National critical industries such as transport, fisheries, marine systems, aviation, aerospace, military, radio and television industries involved in national sovereignty, safe radio frequency and station information;

b) The satellite communication information means information related to the communication by satellite, including earth station infrastructure of the satellite, disaster recovery of ground station of satellite, satellite communication user information;

c) The position of cellular mobile communication base station, infrastructure of cellular mobile communication base station, disaster recovery of cellular mobile communication base station, cellular mobile ability to send and receive information;

d) Radio monitoring information refers primarily to relevant information about carrying out the radio monitoring work, including geographic position of radio stations, antenna configuration, device capability and other monitoring information,, monitoring signal samples, frequency band scan data, frequency-time occupancy and other information of electromagnetic environment;

e) Except the above information included in the International Telecommunication Union (ITU) International MIFR (Master International Frequency Except the information in the Register, MIFR) and radio network data that state radio regulatory agencies is or required to make application to ITU.

A.5.5 Statistical Analysis Data

It mainly includes, based on network and information system running and the user network behavior, directly generated and collected important data and the data obtained after statistical analysis, such as industry and business operation, user network behavior analysis information, industry or business development forecast information.

A.5.6 Other Communication Data

a) Original data of critical infrastructure Internet threats;

b) Communication content, signaling and records;

c) The underlying core technology, the main performance parameters of core equipment, and overall defensive capabilities of network information security .

A.6. Digital information

Competent authority: Ministry of Industry and Information Technology

Important data include, but not limited to:

a) Industry operating data, mainly including: above scale-undisclosed number of electronic information enterprises, output value, sales revenue, profit and other basic information, the number of undisclosed new industrial projects under construction, project feasibility report, investment, investment funds and sources and the undisclosed electronic information products import and export trade situation;

b) Industry data, including: undisclosed industrial development planning, development priorities, and the recent national focus of the Ministry of R & D support projects;

c) Top 100 electronic information enterprises business data, mainly including: undisclosed business development corporate decision-making, investment and financing decision-making, and corporate output value, sales revenue, profit, R & D investment, the number of R & D personnel and other content;

d) Basic hardware model of electronic information products, important parameter, source code and object, technical solutions, experimental data, test reports, all technical information of important technology;

e) Sales and use information of electronic information equipment in national defense and military fields, the field of government and public services in critical areas or important industries, such as the list of buyers, the transaction price, number of transactions, procurement cycle, procurement, product model, applications, products destination, replacement frequency, etc.;

f) Electronic information products' operation, maintenance and repair information in critical areas or important industries, frequency and other equipment operating parameters, such as frequency of equipment failures, failure causes, solutions, service life, maintenance records;

g) Electronic information products in the course of acquisition storage, management and analysis of information involved in government secret, trade secrets and personal privacy in critical areas or important industries, including information on geographical topography, climate environment, satellite orbit, military deployment, information and personal privacy that enterprise, business unit decided not to public including personal identification information, property information, health information,etc.

A.7. Iron and Steel

Competent authority: Ministry of Industry and Information Technology

Important data include, but not limited to:

A.7.1 Strength, Potential and Competitive Information of Steel Industry

a) Production schedule, steel ratio, size, yield, production equipment & technology, procurement planning, logistics distribution, energy consumption and other information of the critical areas;

b) Information of major products batch of the enterprise into the petroleum, chemical and other key areas and emerging areas;

c) Information of frequency, varieties and tons for purchasing of major steel customers purchasing, etc.

A.7.2 Steel required by national defense and military and the national economic construction and development, excellent steel industry and other strength information

Advanced steel materials and products needed for national economic construction and development in metallurgy, energy, transportation, construction, bridges, machinery, electronics, etc.

A.7.3 National industrial development and control and dealing with the relevant information of the external

environment

a) Forecast and monitoring of dynamic information of steel market conditions;

b) Unpublished policy documents, layout arrangement, soldiers and civilians assign configuration, statistics and other relevant information in iron and steel industry.

A.8. Non-ferrous Metal

Competent authority: Ministry of Industry and Information Technology

Important data include, but not limited to:

A.8.1. The strength, potential and competitive information of non-ferrous metals industry

a) Production schedule, scale, output, equipment & technology level, procurement plans, distribution, consumption, sales destination, trade negotiations and other information;

b) Varieties, frequency, tons and other data for non-ferrous metals purchasing of major customers .

A.8.2 Information of non-ferrous metal required by national defense and military industry and national economic construction and development

The name, scientific research, exploration mining plan of non-ferrous metal products, production capacity, process technology route, all the technical information, business name, place of origin, production, capacity, reserves, consumption destination and statistics information.

A.8.3 National non-ferrous metals industry development and control and responding of the external environment, Forecast and dynamic monitoring information of non-ferrous metals market.

A.9. Equipment Manufacturing

Competent authority: Ministry of Industry and Information Technology

Important data include, but not limited to:

A.9.1 Investment Information

Safety and production equipment and key high-tech equipment, such as investment information required by military, aerospace equipment, etc.

A.9.2 Project activity information after important equipment factoring

Information about equipment of the national economy, national defense construction and other production activities for a long time or a wide range in important areas.

A.10. Chemical Industry

Competent authority: Ministry of Industry and Information Technology.

Important data include, but not limited to:

a) the country's main chemical products production capacity, the reserves and other statistics, import and export information of major chemical project;

b) chemical economic program, project, plan, and military chemical export-related information in important region;

c) road transport, sea transport, air transport and other information of toxic chemicals and explosive hazardous

chemicals;

d) production and storage unit of hazardous chemicals and its workplace communication, alarms, security protection and other information;

e) assessment report on safety conditions of chemical companies issued by agency;

f) new construction, renovation, expansion of production and storage of hazardous chemicals construction projects, and new construction, renovation, expansion of storage, loading and unloading of hazardous chemicals and port construction project information;

g) chemical plant plan, the distribution of chemical storage warehouse, storage yard area, capacity, annual usage, sources and other information;

h) production, stockpiling of toxic chemicals and the number and flow of explosive hazardous chemicals.

A.11. Defense Industry

The competent authorities: State Administration of Science, Technology and Industry for National Defense

Important data include, but not limited to:

a) name, quantity, sources, pathways, agents and other information of the purchased components, software, model materials, industrial equipment testing equipment;

b) internal name, location, construction planning, security planning, security level, security protection, plant map Information paper, the treasury volume, reserves and so on of military research and production units .

A.12. Other Industries

Competent authority: Ministry of Industry and Information Technology

Important data include, but not limited to:

a) emergency interim period to prepare for war and temporary announce, transport, store planning and implementation of military products in major regions of the country;

b) industrial research and development projects and programs in the world advanced level, with a significant impact on the national economy;

c) the core of the scientific research with international level and major economic benefits;

d) national oil and gas transport pipelines and coordinates of combat readiness oil depot;

e) distribution , statistics and relevant information of the country's oil inventories;

f) involving electricity production planning, planning and statistics for national defense production;

g) the key scientific and technological content of industrial technology development priorities and security-related tasks.

A.13. Geographic Information

Competent authority: Ministry of Land Resources (National Mapping Geographic Information Bureau, the State Oceanic Administration).

Important data include, but not limited to:

A.13.1 Important Goal of Geographic Information

a) Remote sensing marking important target security guards, facilities and critical information infrastructure of the country or region;

b) Virtual image location accuracy information with important security guards objective, national or regional facilities;

c) Better resolution and positional accuracy of remote sensing image using an image disclosure requirements;

d) Scale charts greater than 1: 50,000 (inclusive) and its digital results;

e) Scale topographic maps greater than 1: 50,000 (inclusive) and its digital results;

f) Released important geographic information without auditing, including borders, national coastline length; territory, territorial sea, contiguous zone, exclusive economic area; national seashore beach area, the number of reefs and area; important characteristic points of the national territory, topography, geomorphologic partition location; other important position, height, depth, area, length and other geographic information of natural and human geography mapping geographic entities of the State Council administrative department of the relevant departments of the military;

g) Geographic information analyzing data, including geographic distribution, recoverable reserves, design reserves, long-term reserves and other reserves information, especially in the case of mine closely related to national security energy of metals and other major non-metallic minerals.

A.13.2 Geographic Information with the Identification of the Following Content (except the opened to the public)

a) Special railway lines and train station, railway marshalling station, and special road;

b) Major national economic construction information related to geography publicly available without the approval of relevant departments of the country;

c) Undisclosed airport (including civilian, military and civilian jointly used airports) and organs, units of information;

d) Content disclosure prohibited in national laws and regulations and departmental rules .

A.13.3 Identification of the following target specific shape and properties (facilities for public services can label name) geographic information

a) Large-scale water conservancy facilities, power facilities, communications facilities, oil and gas facilities, important strategic material storage, meteorological stations, rain drop radar and hydrologic observation stations (net) and other issues involving the country's economic lifeline and civilian facilities with significant impact on people's production and life;

b) Prisons, detention centers, detention centers, forced isolation unit related to public safety;

c) Internal structure and properties of public transport capacity of the airport;

d) Internal structure and properties of ferry;

e) Other disclosures related to the shape and propertied in national laws and regulations, departmental rules.

A.13.4 Geographic Information Marked with the Following Attributes

a) Attributes of high voltage power lines, communication lines and pipes;

b) Disclosure of other relevant attributes prohibited in national laws and regulations and departmental rules;

c) Accurate data of reservoir capacity and transmission line voltage, etc., the form of bridges, ferries, and tunnel and the nature of the river bottom, and undisclosed detailed data of harbors, ports, coastal tide immersion zone;

d) High limit, limit width, clearance, load and slope attributes of important bridges, height and width attributes important tunnels, and highway road paving material properties;

e) Navigable rivers capability, attributes of water depth, velocity, substrate, dams reservoirs and the the constructional material properties and height of the dam.

A.13.5 Special Mapping Information

a) State gravity control point achievements, encryption gravity measurements results, airborne gravity survey results, marine gravity measurement results and various kinds of derived products of calculation results of average gravity anomalies and like results of less than 5 ' × 5 ';

b) Magnetic measurements of the military restricted area and waters magnetic survey data and its derivatives;

c) Digital elevation models and digital terrain model data better than 25 meters network..

A.13.6 Public Map Data

According to *Map Management Regulations* enacted in December 2015 (State Council Decree No. 664), the Internet map service units shall install the map data server in the territory of People's Republic of China, and of user's location related information collected, used and provided by the Internet services unit should be stored in the territory of People's Republic of China.

A.13.7 Beidou Satellite Navigation Information

a) Disaster recovery and data service capabilities of the Beidou satellite navigation system;

b) high-precision position data and services generated by the Beidou satellite navigation system;

c) User directories, property, equipment identification number (ID) and the short message service content data of the Beidou satellite navigation system.

A.14. Civilian Nuclear Facilities

Civilian nuclear facilities competent authority:
State Administration of Science. Technology and Industry for National Defense and National Energy Administration.

Civil nuclear safety supervision department: Department of Ecology and Environmental Protection (National Nuclear Safety Administration).

Important data include, but not limited to:

A.14.1 safety regulatory information of civil nuclear facility

a) The key design and running parameters involved in the activity approval for construction, loading, operation, decommissioning and other activities by the management department.

b) Unpublished original information of national radiation in environmental monitoring.

A.14.2 Civilian Nuclear Facilities Operating Information

a) Electronic data of key technologies in nuclear fuel production, processing, storage and reprocessing facilities, radioactive waste treatment facilities such as information of key equipment design drawings and manufacturing processes;

b) Production capacity of nuclear power plants (nuclear power plants, nuclear power plant, nuclear heating plant gas, etc.), annual procurement disposal amount of nuclear fuel and disposal Information, systems important business statistics of business information, the daily operation & maintenance management information (such as large events of abnormal operation in the running of major nuclear power plant, cold-refueling or maintenance);

c) Usage information of other reactors (research reactors, experimental reactors, critical facilities, etc.), annual procurement disposal amount of nuclear fuel and disposal information, important service data statistics of business information system, the daily operation & maintenance management information (such as cold-refueling or maintenance);

d) Annual processing capacity of nuclear fuel production, processing, storage and reprocessing facilities, the annual processing records, procurement of raw materials, product sales and other statistical information and other business-related information in business systems;

e) Annual processing capacity of radioactive waste treatment and disposal facilities, annual processing records, procurement of raw materials, product sales and other related statistics information in service system;

f) Communication network-related information established by the nuclear power plants, reactors, nuclear fuel processing mechanism and the like to meet the regulatory requirements, the reported refueled or access information;

g) Information formed in nuclear facility data acquisition system to monitor the working parameters of nuclear facilities.

A.14.3 Nuclear Facilities Information Industry Development

a) China's nuclear materials distribution of mineral resources, reserves and other information;

b) Information of civilian nuclear facilities of national development planning;

c) Test or test data in civil nuclear facility research.

Note: According to China's relevant laws and regulations and international conventions to attend, with the exception of the above information that has been disclosed.

A.15. Transportation

Competent authority: National Traffic Combat Readiness Office, Ministry of Transport, National Railway Administration, China Railway.

Important data include, but not limited to:

A.15.1 Data that contains and can validate and deduce the following information by convergence analysis

Information communication system deployment related to transportation and radio spectrum (except as provided in accordance with the open standard, national conventions, national laws and regulations).

A.15.2 Single point of attribute data in specific areas can be measured or disclosed, but the concentrated batches of data leakage may harm national security, military or security against terrorism

a) The key railway route map, station layout, track distribution, storage data and other information;

b) Geography, hydrology, technical information and unified aperture diameters of foreign transportation engineering construction process.

A.16. Post Express

Administrative department: State Post Bureau

Important data include, but not limited to:

a) information that can not be shared by signing a confidentiality agreement or specified in the confidential terms in the agreement with customers;

b) name, address, contact information and amount of the postal service process, etc.;

c) waybill data of postal companies and courier companies, such as name, specifications, quantity, weight, time of the acceptance of goods, recipient name and receiver's address, telephone, and real-time location, location track, vehicles and personnel information of delivering goods;

d) relevant information of the name and address of up-downstream user collected by post companies and express business, covering customer lists of individual customers, customer name or unit name, URL or address, telephone number, etc.;

e) real name identification information of the registered up-downstream users in express and acceptance service, etc.;

f) particular individual user data, such as name, address, ID number, contact information, etc. through big data analysis;

g) data that contributes to hacker attacking of postal industry, materials related to infrastructure, networks, systems, etc., including, but not limited to system architecture design documentation, infrastructure layout and construction documentation, network architecture design documents, IP address assignment document, main type of software and hardware, maintenance personnel information, manage user accounts and passwords.

A.17. Water Conservation

The competent authorities: Ministry of Water Resources

Important data include, but not limited to:

a) water information report code;

b) published water, drought information and prediction of the outcome that may cause major disaster without the approval of national flood control, drought relief and forecast headquarters;

c) operation and management information of large and major flood control reservoirs;

d) planning of large-scale water conservancy and hydropower, water control, inter-basin water transfer and other important projects, project proposals, feasibility studies, early design, construction, completion and acceptance reports, drawings and other information and systematic hydrological analysis results;

e) medium and long term plans of provincial river basin institution development,;

f) medium and long term water supply and demand in the seven major river basins and important area;

g) unpublished scientific and technological achievements, information involving foreign technical cooperation and cooperation in water conservancy projects;

h) information that reflect hard immigrant life of large, medium-sized reservoir and annual plan of special funds for reservoir resettlement;

i) hydrology, water quality yearbook, annual water regime, water and hydrogeological data compilation and communique (containing water, water resources, etc.);

j) run real-time hydrology and engineering running information of transport network;

k) official data of inter-provincial water disputes and illegal cases, and important cases about water and soil conservation;

l) statistical yearbook and compilation of water conservancy before publishing of water conservancy administrative departments;

m) hydrological data of rivers and lakes countrywide , statistical integration, hydrological analysis, etc..

A.18. Population Health

Competent departments: National Health and Family Planning Commission

Important data include, but not limited to:

a) personal privacy, patients and reporter information obtained in adverse reaction report of drugs and contraceptive;

b) acquired infectious disease patients and their families and close contacts in case of public health emergencies and surveillance of infectious diseases, and related diseases, epidemiological information;

c) and other diagnosis, treatment and health data such as personal electronic medical records and health records stored in medical institutions and health care management services agencies;

d) personal information of human organ donors, recipients and human organ transplant applicant in human organ transplant medical services;

e) personal information of sperm, egg donors and users as well as human assisted reproductive technology services applicant in human assisted reproductive technology services

f) personal privacy in family planning services;

g) genetic information of individuals and families;

h) vital registration information.

A.19. Financial

Competent authority: People's Bank of China

Important data include, but not limited to:

A.19.1 Information Security of Financial Institutions

a) New product development programs and related records and data generated in the process of R & D;

b) Technical solution, circuit design, computer software, source code and object code, database, recording of research and development, technical reports, test reports, test data, test results, drawings and other technical documentation;

c) Product sales information, market research information, marketing plans, financial information, business research analysis and other business information;

d) Customer lists, customer identification information, customer transaction records and other customer information;

e) Internal security system, operational details, test key of banking, programming and special markings, code, command password;

f) ,Information that would damage security and interests of financial institutions upon disclosure.

A.19.2 Financial Information of Natural Persons, Legal Persons and other Organizations

a) Personal property information, including personal income, real property, vehicle condition, the amount of tax, deposit amount of provident fund payment, etc;

b) Account information, including information on bank settlement accounts and payment accounts. The main elements are: account name, account number, account type, account opening time, account opening institution, binding of account information, verification of account information (including customer identification verification information from external sources), sensitive media information of account mapping (such as bank card expiration date, verification code, track information, etc.), account balances, account and other transactions;

c) Personal credit information, including credit card repayments, the loan repayment as well as other information of individuals formed in economic activity to reflect its credit standing;

d) Financial transaction information of natural persons, legal persons and other organizations, including transaction information of natural person, legal person and other organizations acquired in the business of financial institutions in fields of banking, securities, insurance finance, trading and clearing and non-bank payment;

e) Identity information, including personally identifiable information and unit identification information, in which personal identifiable information includes personal names, gender, nationality, ethnic group, identity card number, expiration date, occupation, contact information, marital status, family status, domicile or work unit address and photos. Unit identity information includes company name, unified social credit code, type, legal representative (person in charge) name and ID number, place of business, contact information, etc.;

f) Derived information, including personal spending habits, willingness to invest, etc. that can reflect certain situation of specific person formed in the processing and analysis of original information;

g) Information of other natural persons, legal persons and organizations obtained during the establishment of business relationship with the natural, legal person and organizational information.

A.19.3 Work secrets not involved in state secrets, generated in the work of Central Banks, Financial Regulators and Foreign Exchange Management Department

A.20. Credit

Competent authority: People's Bank of China

Important data includes the following:

a) Entry into force of the court judgment, ruling or mediation and implementation of information;

b) Tax arrears information;

c) Information of unpaid labor and social security insurance;

d) Administrative fees, government funds arrears information;

e) Utility arrears information;

f) Credit card repayments and the loan repayment;

g) Information generated due to finance credit relationship between enterprises, individuals and market players other than the financial institutions, including commercial credit, private lending and utilities arrears information.

A.21. Food and Drug

Regulators: China Food and Drug Administration

Important data include, but not limited to:

a) drug test data related to national security strategy submitted in the drug approval process, for example, animal models test data of pharmacology, toxicology, stability, pharmacokinetics, clinical trial data in humans, as well as data of drug manufacturing processes, production facilities of empirical data;

b) Class II and III medical device clinical trial data/report;

c) food safety traceability identification information, including product name, the implementation of standards, drug traceable identification information, including traceability coding, product name, performance standards, ingredients, production technology, and labeling;

d) major food and drug safety (emergency) information, including event time, location, current status, degree of harm, early disposal, trends, events progress, follow up actions, details of the investigation and cause analysis;

e) bulk processed food (including rice, wheat flour) sampling monitoring information.

A.22. Statistics

Competent authority: National Bureau of Statistics

Important data include, but not limited to:

A.22.1 Population

a) Census information (including name, gender, age, ethnicity, household registration status, level of education, industry, migration flow, social security, marriage, birth, death, housing and so on);

b) Information that can recognize or infer the single identity in the census.

A.22.2 Economy

a) Initial number of the country's gross domestic product (GDP) account;

b) National-scale industrial output value and increase value and the main financial indicators;

c) Energy consumption and lower rate of the gross domestic product per unit (GDP);

d) GDP energy consumption, reduce rate, fixed asset investment and retail sales of all provinces, autonomous regions and municipalities directly under the central government;

e) Grain and cotton production of provinces, autonomous regions and municipalities directly under the central government;

f) National grain and cotton production;

g) Industrial producer price index and its main sub-index, the purchase price index and its major sub-index of provinces, autonomous regions, municipalities directly under the central government;

h) Producer price index and the main sub-index, the purchase price index and the main sub-index of the national industrial producer;

i) Major industrial products of the nation and province, autonomous regions and municipalities directly under the central government;

j) Investment in real estate development, sales, marketing area, total construction output, value added of the nation and province, autonomous region and municipalities directly under the central government;

1. k) Total output value of agriculture, forestry, animal husbandry & fishery agricultural production price index, retail price index, fixed asset investment price index and the main sub-index of the nation and province autonomous regions and municipalities directly under the central government;

l) Total consumption of coal and other energy and its growth rate of the nation and province, province autonomous regions and municipalities directly under the central government;

m) Cash income per capita, income per capita, disposable income per capita and live consumption expenditure per capita of rural residents in the nation,and province, province autonomous regions and municipalities directly under the central government;

n) Disposable income per capita and live consumption expenditure per capita of urban residents in the nation, and province, province autonomous regions and municipalities directly under the central government;

o) Disposable income per capita and consumption expenditure per capita of residents in the nation, and province, province autonomous regions and municipalities directly under the central government;

p) Other key statistics and statistical analysis materials closely related to national security and economic interests;

q) Other key statistics and statistical analysis materials closely related to the social order and economic order of the country or a larger area (a province or several provinces).

A.23. Meteorology

Competent authority: China Meteorological Administration

Important data include, but not limited to:

a) original data of meteorological satellite of our country;

b) meteorological observation data of special meteorological station for the state or military secret mission;

c) special meteorological data for combat, military exercises and training, defense research laboratory;

d) atmospheric monitoring data for high-tech or special scientific experiment research;

e) critical meteorological data specialized in statistical integration and analysis for the state or military secret mission;

f) various foreign meteorological data obtained by way of non-international exchange;

g) ground meteorology, high-altitude meteorology, meteorology radiation, atmospheric composition, weather radar, weather satellite data and corresponding not participated in the international exchange and the unpublished numerical forecast products of our country;

h) special, specialized meteorological data, including marine meteorology, space weather, history climate proxy data, meteorological disaster data, aeronautical meteorology data, scientific study test data and corresponding meta data.

A.24. Environmental Protection

Administrative department: Ministry of Ecology and Environment

Important data include, but not limited to:

a) unpublished important pollution sources monitoring data, harm degree and severe pollution accident for long time of series various sectors (areas) environmental pollution ;

b) unpublished water-supply source quality materials for long time of series large and medium-sized cities, and water

quality monitoring and monitoring system information of major rivers and lakes

c) unpublished air quality monitoring data and appropriate monitoring system information for long time of series cities;

d) unpublished national soil pollution monitoring or survey data.

A.25. Broadcasting

Competent authority: State Administration of Press, Publication, Radio, Film and Television

Important data include, but not limited to:

a) safe broadcast, operation & maintenance, emergency support, command control and other information materials of radio and television;

b) related data generated by the system of radio and television monitoring and supervision;

c) business-related system network topology security, operation & maintenance information and the coverage plan that should not be disclosed, media resources files and other information generated by radio and television;

d) wireless and satellite transmission coverage network system configuration of radio and television, broadcast parameters, station location information and other important data;

e) national broadcast satellite user information.

A.26. Marine Environment

Competent authority: State Oceanic Administration

Important data include, but not limited to:

a) observations and statistical data reorganization of submarine topography, marine hydrology, marine meteorology, physical oceanography and acoustic environments such as field observations and statistical data reorganization;

b) measured data and related outcomes of temperature-salinity, sound of water, sediment, tides, currents within the territorial sea;

c) unpublished marine environment monitoring data.

A.27. E-commerce

Competent authority: Ministry of Commerce.

Important data include, but not limited to:

a) personal registration information in e-commerce platform, including name, gender, age, address, marital status, education, occupation, income, account and contact information;

b) enterprise registration information in the e-commerce platform, including business name, address, license number, scope of business, account, contact side type and the like;

c) e-commerce transactions and related personal spending habits and preferences and business data;

d) e-commerce transactions and related personal spending habits and preferences and business data;

e) credit history and credit rating information on e-commerce parties to the transaction;

f) business data of e-commerce platform enterprise;

g) e-commerce related services, including payment and financing information, logistics information;

h) statistical analysis report of the national or regional economic performance, the development of the industry involved in the people's livelihood, etc. formed in the above data processing.

A.28. Other

Important data involves many scopes, this guideline lists only some sectors (areas) part range of important data or content, other important data may be determined and identified according to the following rules:

a) data grasped by enterprises and institutions to reflect the overall situation of certain industry (fields), which is closely related to the national security and public interest;

b) overall running data of enterprises and institutions can reflect occurrence of systemic risk in certain sectors (areas) and once the integrity, confidentiality and availability is damaged, the stable operation of these units can significantly be affected;

c) data that can reflect natural, economic and social characteristics which can not be changed, or remained stable for a long time, such as geographic location, geomorphology, mining location, ethnic genetic characteristics;

d) data that featured with identification, association and connection function in the various data collection, such as geographic location, ID number, phone No., and legal codes;

e) data that industry competent department relied on major planning, planning, decision-making or transferred from the enterprises and institutions industry (field);

f) data collected and generated by the executive authorities and law enforcement agencies in the performance of their duties law enforcement, which could affect national security, public interests or carry a lot of individual privacy information;

g) A single or a small amount of information does not affect national security or public interests, but once covering a larger range or time, data cross-border transfer will harm or affect some information collection;

h) a single or a small amount of information does not affect national security or public interests, once involving some important areas or periods, data cross-border transfer will harm or affect some information collection;

i) system design, security plans and strategic plan of critical information infrastructure, and its units or equipment selection, configuration, software and other attribute information and vulnerability information; and other elements related to national security, including cryptography, including, apparatus, equipment, system or plan, design capability and defect information;

j) cultural safety-related information about the ideology, public opinion and so on;

Competent authorities of the industry (field), according to industry (field) development, assessment practices, to determine whether there are other important data and there is need to update the guidelines.

Appendix B

(Normative Directory)

Personal information and important data cross-border transfer security risk assessment method

B.1 impact Level of the Personal Information Assessment on Individual Rights

B.1.1 Personal Information Types and Sensitivity

Because of the difference of the personal information sensitivity and the purpose of processing after the data cross-border transfer, impact on individual rights may be different, in case of sensitive personal information leakage, damage, tamper or abuse,after cross-border transfer, the impact on the legal rights of individuals are usually higher than the non-sensitive personal information.

B.1.2 Number of Personal Information

The greater the number of personal information, or the greater the number of personal information concerning specific groups, when security incidents occur, the impact on individual rights will increase, and even affect national security and public interests.

B.1.3 Range of Personal Information

When personal information beyond the minimum set of data cross-border transfer purpose, it will cause additional impact on individual rights.

B.1.4 Handling of Personal Information Technology

Network operators can while meeting business requirements, take desensitization technical treatment, like deidentification for personal information, and deal with the de-identification of personal information can once again verify whether the personal information subject can be identified after the deidentification treatment, to ensure reach a reasonable irreversible degree and personal information after processing technology can effectively reduce data cross-border transfer security risks.

B.1.5 Personal Interests impact LevelDetermination

When assessing the impact level of individual rights, first of all, we need to analyze the key elements, the sensitivity of the personal information, make preliminary judgement of impact level; secondly, depending on the number, range of personal information, technical processing, the data frequency and other data features and other elements of personal information to further amended to make it more accurate.

For analsis and computing, impact level of personal interests can be judged by semi-quantitative determination, wherein the determining method is as the following table

Table B.1 Individual Rights impact Level Determination Table

Key elements	Impact level	Correction factors		
Sensitivity		Quantity	Range	Technical handling
Mainly sensitive personal information	3	If data cross-border transfer is involved in personal information	If the personal information in cross-border transfer beyond the minimum elements set meeting the purpose of cross-border	If using technical measures for personal information in cross-border transfer to carry out the deidentification process can effectively
containing a small amount of sensitive personal information	2			

Personal information only, with no sensitive personal information	1	within a year covering the population of greater than 50 people, increase the impact level of 1.	transfer, increase impact level of 1	identify individual, increase impact level of 1.

B.2 Assessment of the impact level of important data cross-border transfer for national security, public interests

B.2.1 Important Data Types

After important data cross-border transfer, if leakage, damage, tampering or abuse occurs, it would harm national security and public interests.

B.2.2 Important Data Amount

For social and economic value of the important data, the greater the number of the value, in case of leaks, damage, tampering or abuse, the greater the harm to national security and public interests.

B.2.3 Range of Important Data

If important data beyond the minimum set related to the cross-border transfer purpose, it will cause additional impact on national security and public interests.

B.2.4 Technical Handling of Important Data

Before important data cross-border transfer, network operators shall take technical measures such as desensitization treatment, and the effect of desensitization process will be validated to ensure that a reasonable degree of irreversible effects. Important data with desensitization can moderately reduce security risks of data cross-border transfer.

B.2.5 impact Level Determination of National Security and Public Interests

When evaluating the impact level of national security and public interests, first of all, it is necessary to identify content of key elements and critical data, as well as its impact level; secondly, the impact level shall be further amended in accordance with the elements such as the amount of important data, important data range and technical processing, to make it more accurate.

In order to facilitate the analysis and calculation, impact level determination of national security and public interests can adopts semi-quantitative way, in which the determining method is as the table below:

Table B.2 impact Level Determination Table of National Security and Public Interests

Key elements / Important data category	impacts grade	Correction factors		
		Quantity	Range	Technical handling
Identified important data	4	If important data in cross-border transfer more than 1,000GB, increase the impact level of 1.	If the personal information in cross-border transfer beyond the minimum elements set meeting the purpose of cross-border transfer, increase impact level of 1	If using technical measures of desensitization treatment for important data can achieve a reasonable degree of irreversible effects, increase impact level of 1.

B.3 Possibility Level Assessment of Security Incidents

B.3.1 Assessment for Sender's Security and Support Capacity Level

Based on the sender's implementation of the technical support and management support requirements, the support capabilities level can be divided in high, medium and low levels.

Table B.3 Sender Security and Support Capabilities Assignment

Category	Support capacity level	Specific description
Technical support capabilities	High	The sender uses the overall security technology such as the data transfer protection, border protection and others, and establish the data cross-border transfer retention log mechanism, which can effectively protect data security, in case of facing threat, the damage can be ignored.
	Medium	The sender uses the security technology such as the data transfer protection and border protection with low grade defects, or the data cross-border transfer retention log mechanism is defective, in case of facing threat, the common damage can be caused.
	Low	The sender uses the security technology such as the data transfer protection and border protection with higher grade defects, or the data cross-border transfer retention log mechanism is not established, which can not effectively protect data security, in case of facing threat, the complete damage can be caused.
Management support capabilities	High	Sender has complete management system, emergency response mechanisms, audit mechanisms, complaints and disposal policy, security event reporting mechanism, management mechanism, to effectively protect data security, in case of facing threat in use, the damage can be ignored.
	Medium	The sender has complete management systems, emergency response mechanisms, audit mechanism and other management mechanism, and management needs to be improved, in case of facing threat, the common damage can be caused.
	Low	The sender does not have effective management system, emergency response mechanisms, audit mechanism and other management mechanism, with a serious lack of management tools, the possibility of data leakage is great , in case of facing threat, the complete damage can be caused.

B.3.2 Assessment of Receiver's Security and Support Capability

Based on the receiver's implementation of the technical support and management support requirements, the support capabilities level can be divided in high, medium and low levels.

Table B.4 Receiver Security Capabilities Assignment

Category	Support capability level	Specific description
Technical support capabilities	High	Data receiver has more advanced security technology capabilities, while the information system of receiving data comply with safety class and protection requirements of the country or region where it is located, and has the automated tools for support of data security, which can effectively protect the data, in case of facing threat in use, the damage can be ignored.
	Medium	Data receiver has a certain security technology capabilities, while the information system of receiving data basically comply with safety class and protection requirements of the country or region where it is located, and has lacks in the automated support for data security, in case of facing threat in use, the common damage can be caused.
	Low	Data receiver has weaker security technology capabilities, while the information system of receiving data Fail to comply with safety class and protection requirements of the country or region where it is located, and has no automated tools for support of data security, which can not effectively protect the data, in case of facing threat in use, the complete damage can be caused.
Management support capabilities	High	Data receiver has the sound organization construction, complete manufacturing and preparation process, good staff capacity, in case of facing threat in use, the damage can be ignored.
	Medium	Data receiver has the basic organization construction, normative manufacturing and preparation process, common staff capacity, in case of facing threat in use, the complete damage can be caused.
	Low	Data receiver has the weak organization construction, defective manufacturing and preparation process, poor staff capacity, in case of facing threat in use, the complete damage can be caused.
Subject review	High	Data receiver has complete enterprise qualification, clear background relations, and content and type of data is consistent with business scope, and there is no offense records.
	Medium	Data receiver has basically complete enterprise qualification, relatively clear background relations, and content and type is basically consistent with business scope, and there is no major offense records.
	Low	Data receiver has no qualified enterprise qualification, content and type is different from the business scope, and there is major offense records.

B.3.3 Assessment of the Political and Legal Environment Where the Receiver is Located

B.3.3.1 Assessment of the Political and Legal Environment Where the Individual Information Receiver is Located

Assessment of the political and legal environment where the individual information receiver is located means the assessment of current protection laws, regulations, standards situation for personal information ,in the country and region, the country's joining regional or global mechanisms for personal information protection and binding commitments and implementation of the personal information protection mechanism. Based on levels of all aspects, the support capability is divided into high, medium and low levels.

Table B.5 Political and Legal Environment Assignment of the Country / Region Where the Personal Information Receiver is Located

Category	Support capabilities grade	Specific description
Political and legal environment and legal assignment of the country/region where receiver is located	High	Laws and regulations and standards of the personal information protection have become more mature and systematic, which protects the individuals rights in terms of personal information, along with a complete, effective, multilevel relief channels.
	Medium	Laws and regulations and standards of the personal information protection are basically complete, which protects part individuals rights in terms of personal information, along with relative administrative and judicial relief channels.
	Low	Laws and regulations and standards of the personal information protection are poor and not complete, individuals can protect rights through judicial relief channels.

B.3.3.2 Assessment of the recipient country where important political and legal environment data

Political and legal environment assess the country of important data receiver means to assess existing laws and regulations and standard of the country or region where the important data receiver is located, implementation of data security mechanism, data transfer for law enforcement, national defense, national security in bilateral or multilateral agreements by the national or regional government and other departments, and ,the bilateral or multilateral agreements on relevant data flow and sharing between other countries or regions. Based on the level of all aspects, the support capabilities will be grading as high, medium, low levels.

Table B.6 Political and Legal Environment Assignment of the Country / Region Where the Important Data Receiver is Located

Category	Support capabilities level	Specific description
Political and legal environment and legal assignment of the country/region where receiver is located	High	Legal standard of network security and data security is complete, the competent regulatory authorities or has strong oversight and enforcement capacity, multilevel, multifaceted effective and accountable oversight mechanisms can be used after data security incident occur. The data transfer authority of government is subject to constraints of the law, open and transparent, in the past there is no related negative reports.
	Medium	Legal standard of network security and data security is basically complete, the competent regulatory authorities or has strong oversight and enforcement capacity, and security incident is mainly depending on the administrative supervision. Multilevel, multifaceted effective and accountable oversight mechanisms is formed preliminarily. The data transfer authority of government is subject to the procedure, in the past there is no related negative reports.
	Low	Legal standard of network security and data security is poor and weak, the competent regulatory authorities lack oversight and enforcement capacity, there is no effective accountability after security incidents, and the government's right to access data is basically unrestricted.

B.3.4 Security Incidents Possibility Level Determination

The possibility of security incidents is related to the sender’s security capabilities, the receiver’s security capabilities and legal environment of the country or region concerned, according to the analysis and evaluation of these elements, in order to facilitate the analysis and calculation, the security incidents possibility level determination refer to the following table:

Table B.7 Security Event Possibility Level Determination Table

Confidence level	Determine conditions
3	Any one of the sender's technical support capabilities, management support capabilities, the receiver's subject review, technical support, management support capabilities, political and legal environment is assigned to "Low".
2	There are sender's technical support capabilities, management support capabilities, the receiver's subject review, technical support, management support capabilities, political and legal environment assigned to "High" and "Medium".
1	The sender's technical support capabilities, management support capabilities, the receiver's subject review, technical support, management support capabilities, political and legal environment are all assigned to "High".

B.4 Comprehensive Security Risk Assessment

Comprehensive security risk assessment is a comprehensive evaluation based on national security, public interests and individual rights and interests of both impact aspects of security incidents, analyzing the overall level of cross-border transfer activity security risk, security risk level is divided into high, high, low levels, for the determination of risk level, please refer to the following table.

Table B.8 Security Risk Level Determination Reference Table

	Security incidents possibility level		
Influence level	1	2	3
≥ 5	High	Very high	Very high
4	Medium	High	High
3	Low	Medium	High
2	Low	Medium	Medium
1	Low	Low	Medium

References

[1] ISO / IEC 27000-2013 Information Security Management System Overview and Terminology

[2] ISO / IEC 27001-2013 Information Security Management System Requirements

[3] ISO / IEC 27002-2013 Code of practice for information security management

[4] ISO / IEC 27003-2013 Implementation Guidelines of Information Security Management System

[5] GB / T 22239-2008 Information Security Technology Essential Requirements of Information System Security Level Protection

[6] GB / T 25070-2010 Information Security Technology Technical Requirements of Information Systems Level Security and Protection Design

[7] NIST Special Publication 800-53 Security and Privacy Control of Federal Information Systems and Organizations