大成 DENTONS

Practice/Industry sector:Energy/ Environment and Natural Resources

Grow | Protect | Operate | Finance

Sort date: 2022.02.14

In recent years, a majority of industries are evolving themselves to be more digitalization and intellectualization. Under this trend, the energy and chemical industry is, without doubt, becoming more inseparable from data, which has been involved deeply through the whole life cycle of energy and chemical products. Being the fundamental industry and pillar of national economic development, data compliance of the energy and chemical industry is of great importance to all.

In general, energy and chemical enterprises, in addition to meeting general data compliance requirements, also need to consider from the following two perspectives: (1) data processor perspective; and (2) data grading and classification perspective, to see whether there are any special requirements. Energy and chemical enterprises generally tend to be large in size, high in value, and of great significance to the national economy, the people's livelihood, and national security. In this sense, energy and chemical enterprises could easily fall into the category of critical information infrastructure operators ("CIIO") when acting as the data processors, and the data processed by energy and chemical enterprises are likely to be classified as important data or key data.

From our past experience of serving clients in the energy and chemical industry, our team hereby shares with you a series of articles (three in total) on how to meet data compliance requirements in the daily operation of energy and chemical enterprises. This article begins with an analysis of CIIOs' obligations in data compliance, from the perspective of data processors.

1. What kind of energy and chemical enterprises will be identified as CIIOs?

1.1 Definition of Critical Information Infrastructure ("CII")

According to the Cyber Security Law of the People's Republic of China ("Cyber Security Law") and the Regulations on the Protection of the Security of Critical Information Infrastructure ("Regulations"), on the one hand, the CII has obvious industrial characteristics and is mainly located in key sectors such as "energy, transportation, and finance"; On the other hand, the destruction of the CII could be disastrous. In case of disfunction or data leakage of CII, there is a great chance that such an incident would seriously endanger national security and affect public interests.

1.2 Definition of CIIO

Once we made clear the definition of CII, the meaning of CIIO becomes quite obvious. In short, a CIIO refers to the owner and manager of the CII, as well as the subjects responsible for establishing and improving the data security protection system and accepting the strong data supervision in the field of CII.

1.3 Steps to Identify the CII

At present, whether infrastructure is qualified as the CII is still not crystal clear and pending for further instruction and regulation issued by the competent authorities and supervisory authorities of the industry (collectively referred to as "Competent Authorities"). Nonetheless, energy and chemical enterprises may, in accordance with the Operation Guidelines for the National Cyber security Inspection ("Operation Guidelines") and the following steps, preliminarily judge by themselves whether they are likely to be deemed as CIIOs.

a. Step 1: Identifying Key Business

Energy and chemical enterprises may, by making reference to the Judgment Form for Basic Business of Key Information ("Judgment Form") provided in the Operational Guidelines, preliminarily judge whether their main business falls within the scope of key business areas. We have selected and listed the key businesses in the Judgment Form which possibly relating to energy and chemical industries as follows:

Industry		Key Business
Energy	Electricity	• Production of electric power (including thermal power, hydropower, nuclear power, etc.) • Power transmission • Power distribution
	Petroleum and petrochemical	• Oil and gas recovery • Refining Processing • Oil-gas transportation • Hydrocarbon storage
	Coal	• Coal Mining • Coal chemical industry
Industrial Manufacturing (Manufacture of Raw Materials, Equipment, Consumer Goods, Electronics)		• Enterprise Operation Management • Intelligent manufacturing system (industrial internet, internet of things, intelligent equipment, etc.) • Control of Production, Processing and Storage of Hazardous Chemicals (Chemical, Nuclear, etc.) • Management and Control of High-risk Industrial Facilities Operation

b. Step 2: Identifying information systems or industrial control systems that support the key business

Energy and chemical enterprises may, according to the key business identified in the previous step, sort out the information systems or industrial control systems supporting their key business operation or related to their key business one by one, and form a list that may be identified as CII.

c. Step 3: Identifying CII

Energy and chemical enterprises may conduct preliminary self-judgment based on the list of CII generated by Step 2 and by reference to the standards listed in Appendix I.

2. What is special about the compliance obligations of CIIOs?

In addition to the obligations that general network operators must perform, CIIOs are required to assume the following obligations and responsibilities:

2.1 "Three Synchronizations"

Both the *Cybersecurity Law* and the Regulations stipulate the "Three Synchronizations" system, which requires CIIOs to plan, construct and use network and data security protection measures synchronously with the main project of the CII, and minimize potential network and data security risks by technical means. Therefore, CIIOs shall implement data and cyber security protection in all phases of the construction of the main project of the CII.

2.2 Stricter Security Protection Obligations

a. Building up Internal System

CIIOs shall establish and improve their internal cyber security protection system and accountability system, set up a dedicated security management department which should be staffed with the person in charge of the dedicated security management department and other relevant personnel.

The dedicated security management department shall be responsible for the security protection of the CII of the entity and shall perform the following main functions, including but not limited to: (1) establishing and improving cyber security management, evaluation and assessment systems, and drafting plans for the security protection plan for the CII; (2) organizing and promoting the construction of cyber security protection capabilities, and conducting cyber security monitoring, detection and risk assessment; (3) formulating its own emergency plans in accordance with the national and industrial cyber security incident emergency plans, and conducting regular emergency drills and disposing of cyber security incidents; (4) organizing cyber security education and training; and (5) reporting cyber security incidents and important matters.

b. Personnel Education and Background Check

CIIOs shall conduct cyber security related education, technical training and skill assessment for their employees on a regular basis. The person in charge of the dedicated security management department and the personnel in key positions shall also be subject to security background check.

c. Emergency Response and Disaster Recovery Backup

On the one hand, CIIOs shall conduct disaster recovery backup for important systems and databases to prevent the permanent loss or destruction of data in the event of cyber security incidents. On the other hand, CIIOs shall formulate their own emergency plans and conduct regular emergency drills to reduce the losses and risks caused by cyber security incidents.

d. Timely Reporting

CIIOs shall report the following matters in a timely manner: (1) If the CII undergoes significant changes that may affect the determination results, the CIIO shall report the relevant information to the Competent Authorities in a timely manner; (2) The CIIO shall conduct by itself or entrust a cyber security service agency to conduct at least one cyber security test and risk assessment for CII every year, timely rectify any security problem found, and timely submit the same as required by the Competent Authorities; (3) In the event of a major cyber security incident in the CII or a major cyber security threat, the CIIO shall report to the Competent Authorities and the public security organ in accordance with the relevant provisions; and (4) In the event of merger, division or dissolution of the CIIO, the CIIO shall report the incident to the Competent Authorities in a timely manner, and dispose of the CII as required by the Competent Authorities to ensure its security.

e. Network Products and Services Purchased

CIIOs shall give priority to the procurement of safe and reliable network products and services. If the network products and services purchased may affect national security, the CIIO shall pass a security review in accordance with national cyber security provisions. Meanwhile, when purchasing network products and services, CIIOs shall enter into security confidentiality agreements with the suppliers of network products or services to specify the technical support and security confidentiality obligations of the suppliers and supervise the performance of the obligations and responsibilities of the suppliers.

f. Domestic Storage and Cross-border Transmission of Data

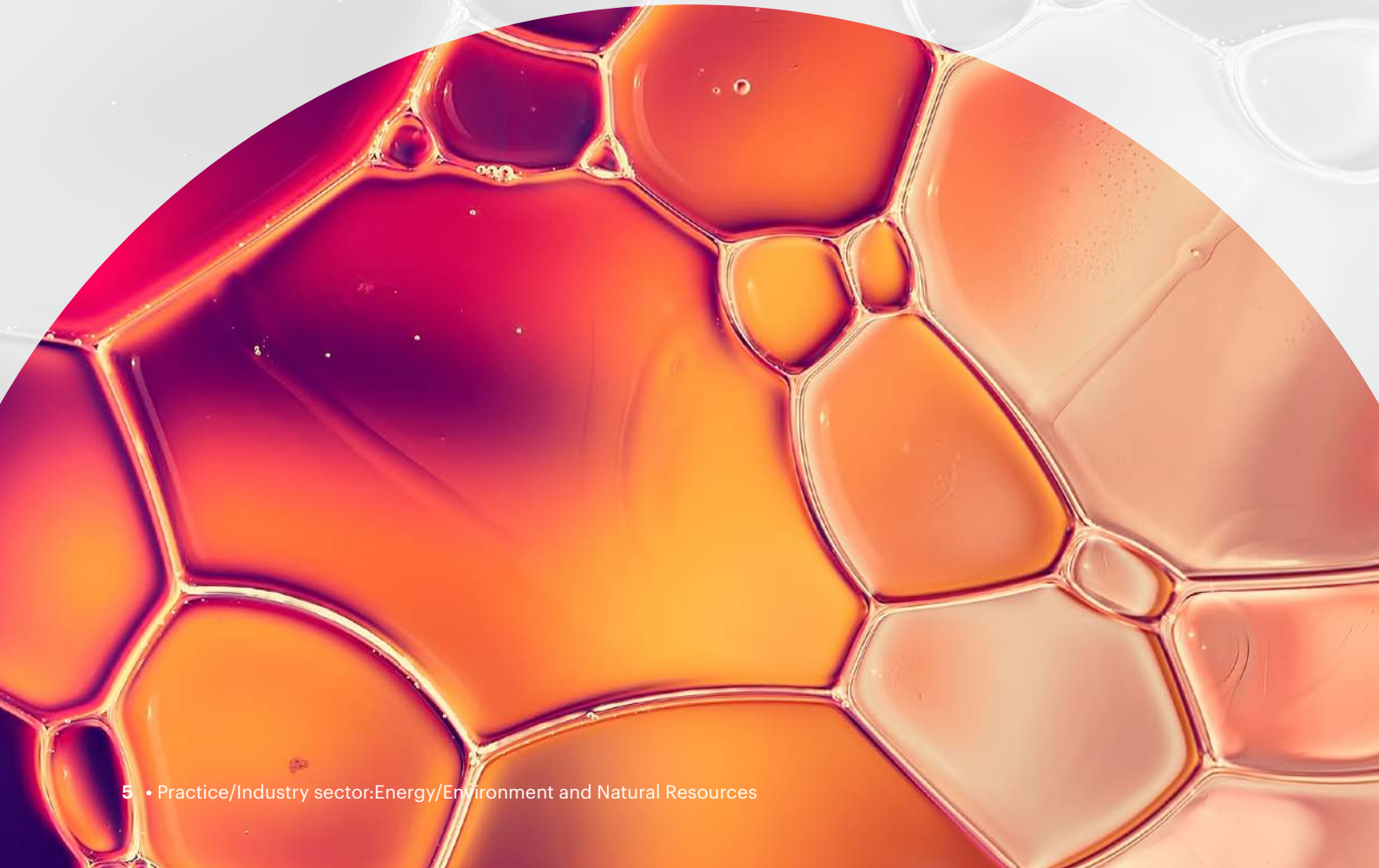
Cybersecurity Law clearly stipulates that the personal information and important data collected or generated by CIIOs during their operation within the territory of the People's Republic of China shall be stored within the territory of the People's Republic of China, so as to safeguard national cyber security. If it is necessary for CIIOs to provide such data to overseas parties for business purposes, the data shall be subject to security assessment by the relevant regulatory authorities before being allowed to be transmitted abroad.

3. Legal Consequences of Failure of CIIOs to Fulfill Their Obligations

Both the *Cybersecurity Law* and the Regulations provide a "dual-track" punishment measure. That is, when a CIIO fails to fulfill its statutory obligations or responsibilities, both the CIIO and the directly responsible executives will face legal consequences of punishment. We summarize the relevant legal consequences in the table below:

Responsible Party	Circumstances of Violation	Legal Consequences
CIIO Direct Responsible Executives	• Failing to implement the "three-synchronization" system; • Failing to set up a dedicated security management organization and appoint a responsible person, and conduct background review on such responsible person and personnel in key positions; • Failing to provide regular cybersecurity education, technical training and skill assessment for its employees; • Failing to make disaster recovery backups for important systems and databases; • Failing to formulate cybersecurity contingency plans and conduct regular drills for such plans; • Failing to make decisions related to cybersecurity and informatization with personnel from dedicated security management organizations; • Failing to enter into security confidentiality agreements with providers when purchasing network products and services; • Failing to conduct inspection and assessment of cybersecurity and potential risks at least once a year; Failing to make timely rectification for identified security problems; or Failing to report relevant information as required by the Competent Authorities; • Failing to report to the Competent Authorities in a timely manner when a major change to the CII may affect the determination results; and • Failing to report to the Competent Authorities in a timely manner when a merger, division or dissolution occurs, or failing to dispose of the CII as required by the Competent Authorities.	• The relevant authorities will, ex officio, order the offender to make rectification and issue a warning; • If the offender refuses to make rectification or such consequences as endangering cybersecurity are caused, a fine of not less than RMB100,000 but not more than RMB 1 million shall be imposed, and a fine of not less than RMB10,000 but not more than RMB100,000 shall be imposed on the directly responsible executives.

Responsible Party	Circumstances of Violation	Legal Consequences
CIIO Direct Responsible Executives	Failing to report to the Competent Authorities or public security authorities in accordance with relevant provisions when a major cybersecurity incident occurs, or a major cybersecurity threat is identified	The Competent Authorities or public security authorities will, ex officio, order the offender to make rectification and issue a warning; If the offender refuses to make rectification or such consequences as endangering cybersecurity are caused, a fine of not less than RMB100,000 but not more than RMB 1 million shall be imposed, and a fine of not less than RMB10,000 but not more than RMB100,000 shall be imposed on the directly responsible executives.
CIIO Direct responsible person in charge and other direct responsible persons	Failing to conduct security review in accordance with national cybersecurity provisions when purchasing network products and services that may affect national security;	The national cyberspace administration and other relevant authorities will, ex officio, order the offender to make rectification and impose a fine of not less than one time but not more than ten times the purchase amount, and a fine of not less than RMB10,000 but not more than RMB100,000 shall be imposed on the directly responsible executives and other directly liable persons.
CIIO Direct responsible person in charge and other direct responsible persons	Storing network data overseas or providing network data overseas in violation of the Cybersecurity Law;	The relevant authorities will order the offender to make rectification and issue a warning, confiscate illegal gains, and impose a fine of not less than RMB 50,000 but not more than RMB 500,000, and may order suspension of relevant business, winding up for rectification, shutdown of website, and revocation of relevant business permit or business license; and A fine of not less than RMB 10,000 but not more than RMB 100,000 shall be imposed on the directly responsible executives and other directly liable persons.



To sum up, when considering data compliance, energy and chemical enterprises may first determine whether they are CIIOs from the perspective of data processors, so as to determine whether they need to perform additional compliance obligations applicable to CIIOs. Meanwhile, energy and chemical enterprises must also perform data compliance obligations from the perspective of data grading and classification. The second and third articles in this series will further explore the data compliance obligations of energy and chemical enterprises from the perspective of data grading and classification. See you in our next article.

Annex I: CII reference standards:

类别 Category	标准 Standards
生产业务类 Production business category	a) Public service business systems of government agencies above prefectural and municipal level, or urban management systems related to medical treatment, security, fire control, emergency command, production scheduling, traffic command, etc. b) Data centers with a size of more than 1,500 standard racks. c In the event of a security incident, one of the following effects may be caused: • Affecting the work and life of more than 30% of the population in a single prefecture-level administrative area; • Affecting 100,000 people's access to water, electricity, gas, oil, heating or transportation; • Incurring more than 5 deaths or serious injuries of more than 50 people; • Directly causing economic losses of more than 50 million yuan; • Causing information leakage of more than 1 million individuals; • Causing the leakage of sensitive information of a large number of institutions and enterprises; • Causing the leakage of geography, population, resources and other national basic data; • Seriously impairing social and economic order, or endangering national security. d) Others should be identified as CII.
平台类 Platform class	a) More than 10 million registered users, or more than 1 million active users (logging in at least once a day). b) More than 10 million yuan of daily orders or transactions. c) In the event of a cybersecurity incident, one of the following effects may be caused: • More than 10 million yuan of direct economic losses; • Directly affecting the work and life of more than 10 million people; • Causing the leakage of information of more than 1 million individuals; • Causing the leakage of sensitive information of a large number of institutions and enterprises; • Causing the leakage of geography, population, resources and other national basic data; • Seriously impairing social and economic order, or endangering national security. d) Others should be identified as CII.
网站类 Website class	a) Websites of Party and government agencies above the county level (inclusive). b) Key news websites. c) Websites with more than 1 million daily visitors. • In the event of a cybersecurity incident, one of the following effects may be caused: • Affecting the work and life of more than 1 million people; • Affecting the work and life of more than 30% of the population in a single prefecture-level administrative area; • Causing the leakage of personal information of more than 1 million individuals; • Causing the leakage of sensitive information of a large number of institutions and enterprises; • Causing the leakage of geography, population, resources and other national basic data; • Seriously impairing government image, social order, or endangering national security. d) Others should be identified as CII.