

# Legal Commentary

August 17, 2023

## The New U.S. Executive Order Compounds Compliance Dilemmas

**Authors: TieCheng YANG | Angus XIE | Virginia QIAO | Huayi CHEN<sup>1</sup>**

On 9 August 2023, U.S. President Joe Biden signed the *Executive Order on Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern* (the “**Executive Order**”), to regulate U.S. persons engaged in transactions or investment activities in China (including mainland China, Hong Kong and Macau) that involve certain technologies and products.

The U.S. Department of the Treasury (the “**Department of Treasury**”) issued on the same day an *Advance Notice of Proposed Rulemaking* (the “**ANPRM**”) to seek public comments in formulating the regulations to implement the Executive Order and to clarify its scope.

The Executive Order and the ANPRM present a tiered regulatory scheme of “notifiable transactions” and “prohibited transactions” U.S. persons are required to undertake notification obligations for “notifiable transactions” and prohibited from engaging in “prohibited transactions”. In connection with “notifiable transactions”, investors should provide relevant information about the transaction to the Department of Treasury that may be shared with other U.S. government agencies.

Reportedly, in recent months, the U.S. Congress has initiated a series of investigations into U.S. firms which may involve several asset managers, investment companies, etc. The investigations are intended to determine whether the U.S. firms are funding or facilitating investments in certain Chinese companies blacklisted by the U.S. government due to national security or other concerns. The detailed scope or status of such investigations has not yet been disclosed to the public, but during such investigations these U.S. firms are very likely to be required by Congress to disclose investment details or corporate profiles of the invested Chinese companies in order to cooperate with the investigations.

In this legal commentary, we focus our analysis on the reporting of PRC enterprise information to the Department of Treasury under the “notifiable transactions” regime. We analyze the circumstances under which information may be provided, the content of such information and potential compliance risks under PRC law that may arise from such reporting.

---

<sup>1</sup> Team member Zhu Lin and Intern Peixi (Regina) Gong have contributed to this article.

## Circumstances for Reporting of Information

Viewing the Executive Order and the ANPRM, there are three scenarios which may involve the reporting of information to the Department of Treasury.

### I. ***Regular Reporting for “Notifiable Transactions”***

For certain transactions in the semiconductors and microelectronics, quantum information technologies, and artificial intelligence (AI) sectors which involve sensitive technologies and products that are critical to the military, intelligence, surveillance, or cyber-enabled capabilities of a country of concern, U.S. persons are required to provide notification to the Department of Treasury and provide information related to the covered transaction. These transactions are referred to as “notifiable transactions”. According to the ANPRM, notifiable transactions currently include those in the AI systems, semiconductor and microelectronics and quantum information technology sectors.

### II. ***Information Reporting Requested by the Department of Treasury when Carrying out Ex Officio Duties***

According to Section 10 of the Executive Order, the Secretary of Treasury is authorized to take certain actions to carry out the purposes of the Executive Order, which may include, among other things, to “investigate and make requests for information relative to notifiable or prohibited transactions from parties to such transactions or other relevant persons.” Therefore, in addition to regular reporting for “notifiable transactions” in the above item (i), the Department of Treasury may also, ex officio, require from the parties to such transactions or other relevant parties to provide information related to other transactions as well as other information related to such transactions.

### III. ***Additional Information Required Regarding Transactions after Issuance of the Executive Order***

As described in Subsection D of the ANPRM, reporting related to covered transactions and notification obligations for such transactions do not have *ex post facto* effect, and it is expected that transactions and the fulfillment of uncalled, binding capital commitments with cancellation consequences made prior to the Executive Order will not be canceled. Notwithstanding the above, the Department of Treasury may after the effective date of the relevant detailed rules, request information about transactions that were completed or agreed to after the issuance of the Executive Order (i.e., after 9 August 2023).

## Scope of Information Required

According to Subsection K of the ANPRM, with respect to a “notifiable transaction”, U.S. persons may need to furnish the following information to the Department of Treasury in the form of notification:

- ***Basic information of each party to the transaction:*** including the identity, nationality or place of incorporation, name, address, business identifiers, key personnel and beneficial ownership;
- ***Information related to the transaction:*** including the relevant or expected date of the transaction, nature of the transaction (including how it will be effectuated, the value and a brief statement of business

rationale), the transaction documents, other agreements or arrangements, arrangements or rights afforded to the U.S. persons, description of due diligence, information about previous transactions made by the U.S. person into the covered foreign person that is the subject of the notification, as well as planned or contemplated future investments into such covered foreign person; and

- *Additional detailed information about the covered foreign person*: including products, technology, the reason for being the covered foreign person, services, research and development, business plans, and commercial and governmental relationships with a country of concern (e.g., China).

Of note is that such information may include personal information of PRC individuals, and sensitive data concerning research and development, products, technologies and business plans. In addition to the foregoing, there is a possibility that the information requested during the review may potentially exceed the scope above as the Secretary of Treasury may have *ex officio* power to investigate transactions and make requests for information from the parties to the transaction or other persons related to such transactions.

## Potential Compliance Risks related to Information Reporting

Although the restrictions imposed by the Executive Order target U.S. persons, as covered companies are located in China, the reporting of information to the Department of Treasury may inevitably lead to cross-border transfers of data. A U.S. person may also request its affiliated entities and employees located in China to cooperate in the reporting of relevant information. Accordingly, the reporting of information to the Department of Treasury, depending on the level of details of the information provided (such as the nature, quantity or type of information provided), may be governed by relevant PRC laws and regulations, posing potential compliance risks under PRC law. Specifically, these risks may include the following:

### I. *Risks Related to Network Security, Data Security and Personal Information Protection*

Transfers to Department of Treasury of certain data, especially important data and personal information, may run afoul of certain PRC laws on data security and personal information protection.

Specifically, Article 36 of the *Data Security Law of the People's Republic of China* (the “**PRC Data Security Law**”, 《中华人民共和国数据安全法》) provides that any organizations or individuals within the territory of the PRC shall not provide to any foreign judicial bodies and law enforcement bodies with any data stored within the territory of the PRC without the approval of the competent authority of the PRC; and Article 41 of the *Personal Information Protection Law of the People's Republic of China* (the “**PIPL**”, 《中华人民共和国个人信息保护法》) provides that, without the approval of competent authorities, personal information processors shall not provide any personal information stored within the territory of the PRC to a foreign judicial or law enforcement body. In addition, Article 31 of the PRC Data Security Law and Article 38 of the PIPL provide, respectively, that the transfer of important data and personal information to overseas parties shall be subject to the regulatory rules of cyberspace administration. Therefore, prior approval may be required, where data or personal information is stored within the territory of the PRC to be provided to the Department of Treasury. Failure to do so could constitute a violation of the PRC Data Security Law and the PIPL.

## II. *National Security Risks*

The Department of Treasury may also require information to be provided regarding commercial and governmental relations between the covered entities and the country of concern, such information may include state secrets or intelligence which are not permitted to be disclosed to foreign parties. Article 111 of the *Criminal Law of the People's Republic of China* (the "**PRC Criminal Law**", 《中华人民共和国刑法》) provides legal liabilities for the crime of stealing, spying, buying or illegally providing state secrets or intelligence to foreign parties. The *Counter-Espionage Law of the People's Republic of China* (《中华人民共和国反间谍法》) also includes the "illegal provision of state secrets, intelligence, and other documents, data, materials or items relating to national security or interests" within the scope of its regulation. The PRC government has been relatively active recently in national security and counter-espionage enforcement activities and the provision of such information to the Department of Treasury could potentially be seen as triggering national security risks.

## III. *Trade Secret Infringement Risks*

Trade secrets refer to business information such as technical and operating information which is unknown to the public, has commercial value, and for which rights holders have adopted corresponding measures to ensure its confidentiality. According to Article 9 of the *PRC Anti-Unfair Competition Law of the People's Republic of China* (《中华人民共和国反不正当竞争法》), a business operator shall not disclose, use or allow others to use the trade secrets under its possession in breach of its confidentiality obligation or the requirements of rights holders on keeping such trade secrets confidential. Article 219 of the PRC Criminal Law also criminalizes serious instances of trade secret infringement and the stealing, spying, buying or illegally providing of trade secrets to foreign parties. The products, services, research and development, business plans and other information of the covered companies required by the Department of Treasury could constitute trade secrets. Therefore, providing such information may have the risk of infringing trade secrets.

## IV. *Anti-Foreign Sanction Risks*

Article 12 of the *Anti-Foreign Sanctions Law of the People's Republic of China* (the "**PRC Anti-Foreign Sanctions Law**", 《中华人民共和国反外国制裁法》) provides, "no organization or individual shall implement or assist in the implementation of the discriminatory restrictive measures taken by any foreign countries against any Chinese citizens or organizations". If the Executive Order is deemed as a discriminatory restrictive measure against the citizens and organizations of the PRC, the reporting of relevant information to the Department of Treasury may be deemed as assistance with the implementation of the discriminatory restrictive measure taken by the United States against the citizens and organizations of the PRC, thereby violating the PRC Anti-Foreign Sanctions Law.

## **Compliance Dilemmas Compounded**

According to the Executive Order and the ANPRM, investments by U.S. persons in certain Chinese companies may require a notification to the Department of Treasury providing extensive information regarding related transactions, which may contain personal information of PRC individuals or sensitive data of PRC companies. As a result, there is a risk of violating relevant PRC laws and regulations when

providing such information, including but not limited to the risks of cybersecurity, data security and personal information protection, national security, trade secret infringement and anti-foreign sanction provisions.

It is worth noting that, currently, although the reporting of information to foreign government authorities is also involved in the normal administrative review procedures such as foreign anti-trust notification and foreign investment security review, the regulatory controls are generally more prudent and do not impose a substantial burden on PRC companies. However, both the PRC Ministry of Foreign Affairs and the PRC Ministry of Commerce have expressed grave concern over the apparent targeting of the Executive Order and the sensitivity of the industries involved and said they will reserve the right to take appropriate actions. Therefore, it remains to be seen whether PRC regulatory authorities will adopt a stricter attitude towards information reporting under the new system. U.S. firms that have PRC investment exposures are worse off in terms of complying with restrictions and prohibitions from the US and countermeasures from China.

## Market Observations and Compliance Suggestions

The Executive Order has triggered a lot of discussion and controversy in the market, especially among subsidiaries or branches of U.S. entities in China.

### I. Branches of U.S. entities

Branches of U.S. entities domiciled within China will potentially face conflicting regulations in different jurisdictions.

- U.S. law: The scope of “U.S. persons” as defined in the Executive Order includes “foreign branches” of entities organized under the laws of the United States or any jurisdiction within the United States. U.S. firms’ branches in China are thus subject to the Executive Order; and
- PRC law: Firstly, for such branches domiciled within China, the Anti-Foreign Sanctions Law requires them not to implement or assist in implementing “discriminatory restrictive measures” taken by any foreign country against Chinese citizens or organizations. Secondly, they are likely to be regarded as “organizations within the territory of China” so that they need to carry out countermeasures according to the Anti-Foreign Sanctions Law. This further aggravates the above-mentioned dilemma in practice.

### II. Subsidiaries of U.S. entities

Subsidiaries of U.S. entities domiciled in China are not explicitly covered under “U.S. persons” subject to the Executive Order. Nevertheless, as legal entities incorporated in PRC, they are still subject to regulation and supervision of PRC data protection laws and must pay attention to the data compliance issues discussed above.

However, although not directly regulated by the Executive Order, subsidiaries of U.S. entities may be required by their parent companies in the United States to cooperate with the offshore requests raised by the Department of Treasury for assisting in certain data collection, transfer or other processing activities, which pose additional compliance challenges for intra-group operations.

How the compliance dilemmas will be solved still needs to be clarified by implementing rules and specific

enforcement cases. Although there may not be an available answer at this stage, more and more U.S. clients have included sanctions-related clauses in their business contacts and taken a prudent approach to avoid “one-sided / biased statements” that emphasize compliance with one country’s sanctions compliance requirements only, which may serve as evidence for implementing “discriminatory measures” under another jurisdiction.

Please note that the content in this article related to offshore jurisdictions is prepared by us by generally referring to laws and regulations, cases, documents, articles and reports publicly available in offshore jurisdictions, as well as based on our practical experience. The section on offshore laws or regulations is intended to be an introductory overview to the topic and is for reference only. It does not imply that we are qualified to review or express opinions on the laws or regulations of the offshore jurisdictions. This article does not constitute legal advice or a formal opinion or memorandum.

We hope the above is helpful. Please feel free to contact us if you have any questions or comments.

## ***Important Announcement***

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

### **TieCheng YANG**

Tel: +86 10 8516 4286

Email: [tiecheng.yang@hankunlaw.com](mailto:tiecheng.yang@hankunlaw.com)

### **Angus XIE**

Tel: +86 10 8524 5866

Email: [angus.xie@hankunlaw.com](mailto:angus.xie@hankunlaw.com)