Westlaw Today
powered by Reuters

China faces existing and expanded US restrictions on trade, investment and technology

By Brian J. Egan, Esq., Steve Kwok, Esq., Jessie K. Liu, Esq. and Daniel Michael, Esq., Skadden, Arps, Slate, Meagher & Flom LLP*

JANUARY 31, 2022

Takeaways

- Chinese investments requiring CFIUS review have declined as the U.S. scrutinizes those transactions aggressively, and rules governing interactions with "Chinese military-industrial complex companies" have been revamped.
- Import restrictions on products made in the Xinjiang region have been deployed by the U.S. government.
- Despite several high-profile case dismissals and a trial loss, the DOJ's China Initiative, aimed at thwarting economic espionage and trade secret theft, continues.
- Multinational companies that have dealings in China or with its citizens will need to comply with two new Chinese data protection laws.

National security regulation

China remains one of the U.S. government's top priorities for national security regulation. The Biden administration has retained or even augmented key aspects of the Trump administration's national security approach to China, while making modest adjustments to some of the more controversial or legally vulnerable regulations:

- The Committee on Foreign Investment in the United States (CFIUS) maintained an aggressive approach to reviewing transactions involving investors from China or third-country investors with significant connections to China. This has resulted in a notable drop in Chinese investments requiring a CFIUS review, from an average of 57 cases per year in the 2016-18 time period to 28 in 2019 and 22 in 2020. We anticipate that the data will reveal a comparable drop in China-related CFIUS cases in 2021.
- The U.S. government has deployed sanctions and new legislation to pressure U.S. companies to avoid products from the Xinjiang region of China, in response to U.S. government concerns about the use of forced labor for products from Xinjiang. On December 23, 2021, President Biden signed into law the Uyghur Forced Labor Prevention Act, which Congress had passed with broad bipartisan support. The act effectively prohibits imports of goods made wholly or in part in Xinjiang, relying on a strong presumption that forced labor is used for all products coming from the region.
- In a modification of Trump administration policy, in June 2021 President Biden revoked an executive order that would have restricted the use of eight popular Chinese apps in the U.S. In its place, the Commerce Department was instructed to monitor and take appropriate action against any "connected software applications" — defined as software "used on an end-point computing device ... [with] the ability to collect, process, or transmit data via the internet" — that may pose risks to U.S. national security. We expect Commerce to issue further guidance on this issue in 2022, and we anticipate a rigorous regulatory and enforcement regime.
- In June 2021, the Biden administration revamped the sanctions framework for "Communist Chinese Military Companies" (now called "Chinese Military-Industrial Complex Companies" or CMICs) by clarifying listing criteria, revoking some of the more controversial sanctions on particular companies and shifting primary responsibility for administering the list from the Department of Defense to the Treasury Department's Office of Foreign Assets Control (OFAC). In December, OFAC added additional companies to the CMIC list.

Import restrictions on products made in the Xinjiang region have been deployed by the U.S. government.

We anticipate a similar approach in 2022, with the administration continuing a relatively aggressive but more nuanced approach to national security regulation.

Securities regulation

On December 2, 2021, the Securities and Exchange Commission (SEC) adopted final amendments[1] implementing the disclosure and submission requirements of the Holding Foreign Companies

Accountable Act (HFCAA). The legislation directs the SEC to delist registrants if, for three consecutive years, the Public Company Accounting Oversight Board (PCAOB) is unable to inspect the auditor of the registrant's financial statements.

We expect continued focus on the Chinese government's perceived involvement in intellectual property misappropriation, economic espionage and cyberattacks.

On December 16, 2021, the PCAOB sent the SEC a report with its determinations that it was unable to inspect or investigate completely PCAOB-registered public accounting firms headquartered in China and Hong Kong because of positions taken by government authorities in those jurisdictions. Access to the audit work papers of firms headquartered in China and Hong Kong likely will continue to be a significant issue in 2022.

DOJ China Initiative

Originally announced in November 2018 as a Department of Justice (DOJ) effort to counter Chinese trade secret theft and economic espionage, the China Initiative faced significant criticism last year.

After the DOJ dropped several cases, and a judge acquitted University of Tennessee professor Anming Hu on wire fraud and false statement charges based on allegations that he hid his affiliation with a Chinese university while receiving funding from the U.S. National Aeronautics and Space Administration, some observers questioned whether prosecutors had overreached.

Critics also raised concerns that the China Initiative could contribute to negative stereotypes of Asians and Asian Americans.

The DOJ has not disavowed the China Initiative, however, and on December 21, 2021, a federal jury in Massachusetts convicted Harvard professor Charles Lieber of false statements and tax offenses stemming from the concealment of his affiliation with the Wuhan University of Technology and his participation in China's Thousand Talents Program.

Although the DOJ may be more cautious in bringing false statement-type cases given its losses in other cases last year, we expect continued focus on the Chinese government's perceived involvement in intellectual property misappropriation, economic espionage and cyberattacks.

New Chinese legislation

In addition to American laws and regulations applying to Chinese companies and trade, two new Chinese laws came into force in late 2021 that are likely to have an impact on many multinational companies operating in, or with operations touching, the country: the Data Security Law (DSL) and the Personal Information Protection Law (PIPL).

The DSL applies to all data activities in China, as well as extraterritorially if they are deemed to impair the country's national security and public interest. It sets up a framework to classify data collected and stored in China based on its potential impact on Chinese national security and regulates its storage and transfer depending on the type of data.

Specifically, the DSL clarifies and expands data localization and transfer requirements for certain categories of data and certain types of data handlers, and it expands the scope of regulation to cover both the initial collectors and downstream intermediaries.

Two new Chinese laws came into force in late 2021 that are likely to have an impact on many multinational companies operating in, or with operations touching, the country.

The PIPL generally applies to all types of data activities involving the personal information of subjects in China, as well as activities outside the country aimed at providing products or services to individuals in China or analyzing their behavior.

The PIPL imposes the following key obligations on data handlers:

- obtain consents;
- localize and delete data when certain conditions are met;
- ensure that any foreign recipient of the data has protection measures in place that are no less stringent than those imposed by the PIPL in cross-border data transfers; and
- conduct regular self-audits to assess information security risks and implement corresponding policies and safeguards.

Given these laws' broad coverage and expansive compliance obligations, companies doing business in China should reassess their information technology systems and seek advice before exporting data overseas.

Notes

[1] https://bit.ly/35ChpdP

About the authors




(L-R) **Brian J. Egan**, a national security partner in **Skadden, Arps, Slate, Meagher & Flom LLP**'s Washington, D.C., office, advises clients on foreign investments in the U.S., export controls, economic sanctions, cross-border disputes and data privacy matters. **Steve Kwok**, a litigation partner in the firm's Hong Kong office, represents clients with internal investigations, U.S. regulatory enforcement matters, and trial and appellate litigation. **Jessie K. Liu**, a litigation partner in the firm's Washington, D.C., office, focuses on government and internal investigations, audit committee representations, the False Claims Act and crisis management counseling. **Daniel Michael**, a government enforcement and white-collar crime partner in the firm's New York office, advises corporations, boards and individuals on criminal and civil enforcement matters. This article was originally published Jan. 19, 2022, on the firm's website. Republished with permission.

This article was published on Westlaw Today on January 31, 2022.