Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Navigating Geopolitics In US-China Investments

By **Charles Comey and Jim Ryan** (October 22, 2018, 1:55 PM EDT)

Charles Comey

Jim Ryan

As 2018 moves into its last quarter, the White House continues to foster uncertainty in global markets while China responds tit for tat on trade sanctions and keeps a wary eye on capital flight risk by maintaining close scrutiny over outbound investment flows.

Notwithstanding protectionist trends on both sides of the Pacific (China's rhetoric about "continued opening" notwithstanding) and ongoing cybersecurity issues, we continue to see high levels of interest from Chinese and other foreign investors looking to invest in U.S. companies and from U.S. companies seeking to explore expansion opportunities in China and elsewhere overseas. To succeed in the current environment, companies need to be aware of the latest developments affecting China-related investments and operations, in particular: (1) in China, tightened enforcement of regulations on Chinese outbound investment and new Chinese cybersecurity and data regulations, and (2) in the U.S., the most important reform to the Committee on Foreign Investment in the United States since 2007, just-issued interim pilot rules thereunder, and soon-to-follow related export control regulations from the U.S. Department of Commerce.

China

In March 2018, the People's Republic of China National Development and Reform Commission, or NDRC, amended its outbound direct investment regulations to more stringently regulate outbound investments viewed as problematic by the state while streamlining procedures for transactions that are deemed to further China's transition to a modern diversified economy. The new rules replace the former "road pass" system (which required submission of a project report before a bidder could join an auction process and was, in effect, a presigning approval) with a filing requirement prior to closing for transactions involving $300 million or more, and preclosing approval for "sensitive" deals (i.e. in the real estate, hospitality, entertainment and sports franchise sectors).

U.S. companies entertaining Chinese investment or acquisition proposals should consider whether their deals are subject to NDRC filing/review or other regulatory approvals, and plan their timing of closing to take account of applicable approvals and related delays. In our experience, even "valid" outbound investments in leading-edge technology and health care business can take weeks to obtain PRC regulatory approval. Indeed, given trade tensions, many, if not most, U.S.-bound Chinese state-owned

investments requiring the conversion of RMB into U.S. dollars are simply not being approved in practice.

Another recent regulatory challenge for U.S. companies in China has been the Cyber Security Law, or CSL, which came into effect in June 2017. The CSL regulates data localization, requires government security audits, and restricts cross-border transfers of data. A number of key definitions and provisions in the CSL are vaguely drafted to maximize administrative discretion and can present challenges for foreign companies seeking to implement compliant IT systems, particularly with respect to the sharing, storage and transmission of data generated in China. As but one example, “operators of critical information infrastructure” are required to store personal information and important business data onshore in China, and provide undefined “technical support” (in practice, including facilitating access to user accounts) to PRC security authorities and pass national security reviews. Further regulations issued in September give PRC police enhanced authority to monitor and supervise cyber compliance of “internet service providers” and “entities connected to the internet.” U.S. technology growth companies need to keep cyber risk and compliance top of mind when entering the PRC market.

U.S.

Meanwhile in the U.S., CFIUS has moved from being a little-understood (often termed “secretive” in the mainstream press for no clear reason) to being a regular feature in national business news headlines. In the current climate, CFIUS’ role has expanded to address not only blockbuster M&A tech deals but also private equity/venture capital-style investments and smaller M&A deals, where foreign parties may acquire control (which CFIUS defines very broadly) of companies in sensitive sectors.

In August, the president signed into law the Foreign Investment Risk Review Modernization Act of 2018. In one of a number of important changes brought by FIRRMA, CFIUS will have (once implementing regulations are issued) jurisdiction over any foreign investment in U.S. businesses involving critical infrastructure, critical technologies, or the collection or possession of sensitive data, which means that parties to small and otherwise “passive” investments in these spaces are no longer exempt from CFIUS jurisdiction and must evaluate whether to notify CFIUS voluntarily. In a further recent development, the U.S. Treasury Department (as the CFIUS chair) this month issued pilot program regulations under FIRRMA that expand CFIUS’ jurisdiction to cover certain foreign investments in “critical technologies” and subjected 27 enumerated industry sectors to coverage under the pilot program. While mostly focused on familiar defense- and tech-related manufacturing sectors (defense components, semiconductors, semiconductor manufacturing equipment, battery manufacturing and optics manufacturing), the "list of 27" includes nanotechnology and biotechnology research and development.

Firms looking abroad for investors or buyers should plan for the possibility of a CFIUS notification (or, for transactions covered by the pilot program regulations, a more streamlined five-page declaration). In the process, companies should assess their approach to cyber/data security and handling personally identifiable information of U.S. citizens, the potential of transferring sensitive intellectual property to the foreign acquirer, the Chinese government’s support of the transaction (which can be important to getting the deal done on the Chinese side but which CFIUS views negatively), the perceived impact of the transaction on the "integrity" of U.S. domestic commercial and government/military supply chains, and whether their technology falls within an area of heightened scrutiny, such as semiconductors, artificial intelligence, robotics, autonomous vehicles, navigation, robotics, 3D printing and cybersecurity.

In addition to the expanded jurisdiction and increased scrutiny of CFIUS after FIRRMA, a new export control rule-making process is poised to place restrictions on outbound technology transfers (noting that even access to the technology in the U.S. by a foreign national can trigger a deemed export) by U.S.

businesses developing “emerging and foundational technologies.” The definition of “emerging and foundational technologies” awaits determination by an interagency process. Nevertheless, many expect the list of technologies to be similar to CFIUS’ areas of focus. The secretary of commerce is ultimately responsible for determining what controls and export licensing requirements will be placed on these technologies, but FIRMMA requires an export license prior to exporting to arms-embargoed countries (including China). Since many transaction structures pair an inbound investment to the U.S. with an outbound license or joint venture offshore, parties should carefully consider their research and development and expansion plans and factor in timing considerations resulting from potential export license requirements.

It’s good news that Presidents Donald Trump and Xi Jinping may meet for trade talks during the G20 meetings in Buenos Aires next month. However Xi’s “Strong China Dream” and Trump’s “America First” policies play out, forward-looking entrepreneurs and investors can continue to achieve their business goals through thoughtful planning to navigate opportunities and avoid pitfalls in an increasingly complex cross-border environment.

Charles C. Comey is a partner and Jim Ryan is an associate at Morrison & Foerster LLP.