Global Counsel

Highlighting Commerce's new ICTS Rule – A Little-Known Process with Major Headwinds for Tech

Blog post by Senior Associate Michelle Ryang 14 April 2022

Last month, Chinese technology company Baidu (NASDAQ: BIDU) was added to the U.S. Securities and Exchange Commission's (SEC) provisional watchlist, the latest development in a longstanding clash between the U.S. and China around audit oversight of foreign companies. The purview of the SEC and other regulatory bodies such as the Committee on Foreign Investment in the United States (CFIUS) is commonly understood. But a much lesser-known, new rule from the Department of Commerce (Commerce), "Securing the Information and Communications Technology and Services Supply Chain" (ICTS Rule), has quietly opened up a second arena of investigation into foreign companies and potentially U.S. companies with commercial relationships abroad.

The ICTS Rule signals the Biden Administration's intent to significantly ramp up scrutiny of foreign commercial activity in a number of ways. First, it is highly notable that the rule itself is predicated on a Trump Executive Order (EO 13873), which President Biden not only allowed to stand, but doubled down upon by issuing an EO of his own (EO 14034), directing Commerce to refine the existing rule whilst revoking several other Trump EOs in the same breath.

Second, the rule differs from existing regimes such as CFIUS's in its broad reach – opening up **individual commercial activities**, rather than investments, for review. Its expansive definition of "Transaction" encompasses any activity "dealing in, or [using]" ICTS products or services, even as passive as "data transmission, software updates … or the platforming or data hosting of applications for consumer download." While a transaction must be deemed "under the influence" of foreign adversaries (specifically China, Russia, Iran, North Korea, Cuba, and Venezuela) to be reviewed, the rule's parameters cover a vast array of sectors. A single category, Critical Infrastructure, alone includes the use of ICTS by industries such as chemicals and agriculture, per Presidential Policy Directive 21.

Third, Commerce appears to be taking a more aggressive stance on the rule – the agency released a Notice of Proposed Rulemaking (NPRM) last fall, proposing a set of amendments claiming to narrow the scope of the rule. The NPRM's language, however, appears to **expand** the rule's parameters instead, particularly through its treatment of "connected software applications" ("apps") and additional risk criteria in Section 7.103(c).

For instance, Commerce posits changing the term "end-point devices" to "end-to-end technology". This is a small but impactful distinction, as "end-to-end" implies services are provided in a vacuum, without integration of other technology. As many products rely on a stack of technology or various hardware components to create, distribute, or enable usage of a final offering, this suggests the

entire supply chain for the XaaS could come under review, with some measure of fault up and down the stack including, presumably, cloud service providers, or mobile operating system owners.

In another example, the NPRM asks whether "ownership, control or management" would be understood by industry to mean "both continuous control … and sporadic control and management." As software is not typically static but requires updates and patches or other ongoing services which may be provided by a third party, "sporadic control" not only widens the ICTS Rule's domain but could have the opposite intended effect of securing ICTS, perhaps by disincentivizing ongoing security practices, or in the case of telecom providers, hampering operations by preventing the use of critical backhaul networks which can be shared or leased.

Commerce also ponders whether audits should be limited to "source code examination" or expand to "monitoring of logs or other data". Creating a precedent whereby companies offer up source code or provide access to data collected by the app to a third-party auditor may not only present a new host of data protection issues, but prompt reciprocal review requirements from other nations as a condition for operation, potentially compromising IP.

Though the rule appears to target primarily Chinese companies - its only officially confirmed use has been to subpoena five Chinese firms last spring and reportedly investigate two Chinese tech companies this year –, major U.S. players have obvious cause for concern given the outsized role, and complex nature, of American technology companies in the global marketplace.

Between the expansive language in the NPRM and utter silence from Commence on any kind of licensing or pre-clearance process that would provide certainty and reduce regulatory overhang (the contours of a process were floated under an ANPRM last spring but has seen no progress), it is clear that U.S. firms are being put on notice. It is also significant that Commerce is not leaning on existing, globally accepted standards that might reduce compliance burdens, including those originating even from Commerce itself, such as the National Institute of Standards and Technology's Secure Software Development and Cybersecurity frameworks.

Taken altogether the clear signal to the U.S., and indeed the wider Westerntech sector is that global decoupling is a key priority for this Administration. American technology companies would do well to review their supply chain and commercial relationships with foreign entities.