



**WORLD***ecr*

**TRADE COMPLIANCE  
IN A TIME OF CRISIS**



# Circling the wagons: reactions to Covid-19 bolster regulatory exclusions

By Caroline E. Brown and Chandler S. Leonard

**A**s the Covid-19 pandemic raced from one country to another, governments moved quickly to seal their borders in an effort to slow its transgression and started closely watching who – and what – comes and goes. One thing has been made clear: borders matter.

Consequently, the inherent appetite for risk required for reliance on global supply chains is dwindling as Covid-19 exposes vulnerabilities in dependence on an uninterrupted flow of goods from around the world. Pivoting to new norms, companies are moving supply chains closer to home. While arguably the pandemic served as an accelerant to protectionist trends presaged by other geopolitical events, the advent of Covid-19 supplies a valid defence to an increasing exercise of regulations to protect national security. In the United States, regulatory reforms aiming to protect critical infrastructure and an expansion of export controls and sanctions are closing borders previously flung open to globalism, signaling that economic nationalism spurred by Covid-19 will have lasting effects on supply chains.

Recent reform has galvanised instruments that aim to protect critical infrastructure from ‘weaponisation of investment’. The passage of the Foreign Investment Risk Review Modernization Act (‘FIRREA’) broadened the scope of review of the Committee on Foreign Investment in the United States (‘CFIUS’). Other jurisdictions, like Australia, have followed suit, reforming their own foreign investment review mechanisms. Similarly, momentum is building to bolster a lesser-known review body. A recent executive order enhances Team Telecom, formally known as the ‘Committee on the Assessment of Foreign Participation in the United States Telecommunications Services Sector’, the multi-agency group that assesses national security implications of certain Federal Communications Commission licences, including subsea cables, satellites, and foreign telecommunication connections.

Though these review bodies stop short of prohibiting specific components, some industry sectors are furiously scrubbing their supply chains at the direction of executive orders designed to fill that gap. In May, another executive order declared a national emergency regarding threats to the US bulk-power system, broadly prohibiting

‘bulk-power system electric equipment’ transactions where the transaction involves property in which any foreign country or national has an interest. Depending on how it’s implemented, the order has the potential to significantly disrupt the supply chain for electrical equipment for US bulk-power systems, which include items used in electric generation projects and transmission systems. The order closely mirrors one issued almost a year prior directed at the

## The advent of Covid-19 supplies a valid defence to an increasing exercise of regulations to protect national security.

information communications technology and services (‘ICTS’) supply chain. Using very similar language, that order directed the Department of Commerce to promulgate regulations to prohibit transactions involving ICTS produced by ‘foreign adversaries’ that pose risks to US national security.

Many companies are also finding their supply chains compromised by export controls increasingly used to guard against perceived threats to national security. The Commerce Department’s Bureau of Industry and Security (‘BIS’) continues to add to its Entity List, a powerful tool that generally cuts off listed companies from US exports, reexports, or transfers of items subject to Export Administration Regulations (‘EAR’) absent a licence. BIS’s reach is demonstrated by its efforts to limit Huawei Technologies Co., Ltd.’s control of the semiconductor industry. Last year, BIS added Huawei and 114 of its affiliates to the Entity List. In May, BIS amended the Foreign-Produced Direct Product Rule to further restrict Huawei’s and

its non-US affiliates’ access to US technology or equipment used by semiconductor manufacturers outside the United States, leaving companies confronted with a choice between US-origin technology and equipment integral to advanced semiconductor manufacturing, or Huawei, the world’s largest supplier of telecom equipment.

Separately, expanded BIS end user controls and the continued use of sanctions as national security tools are increasing the due diligence companies must perform throughout their supply chain, even during the pandemic-induced economic downturn when companies are facing severe resource constraints. Indeed, the agencies that issue sanctions continue to expand their scope through secondary sanctions and by targeting unconventional entities, such as the International Criminal Court. Likewise, the agencies haven’t stopped their enforcement of these regulations, and there’s been an uptick in cases brought by the Justice Department in these areas.

Increasingly used in coordination with one another, this all-tools approach tightens controls on who and what crosses US borders, and is likely to continue to erect barriers to the ease with which goods, people, and services were ferried around the world before Covid-19. Due in part to an emotional response not seen in years to the pandemic, those that find themselves subject to these stringent measures might be more accepting of a new reality at which they may have balked before. As these mechanisms become even further entrenched, both US and non-US companies might recognise the increasing importance of due diligence as part of their overall business risk assessments and further evaluate the adequacy and depth of their compliance functions and their businesses’ ability to withstand increased scrutiny. ■



Caroline E. Brown is a Partner at Crowell & Moring. She previously worked at the US Department of Justice’s National Security Division and the US Department of the Treasury. Chandler S. Leonard is an Associate at the firm, and was formerly a case officer at the US Treasury Department’s Office of Foreign Assets Control and the US State Department’s Directorate of Defense Trade Controls. [www.crowell.com](http://www.crowell.com)