Decoupling From China: Part 2 — Security Requirements

By **Jamie Gorelick, Stephen Preston and Matthew Ferraro**

Jamie Gorelick

Stephen Preston

Matthew Ferraro

The COVID-19 pandemic and the serious supply chain vulnerabilities it exposed have led to a seismic shift in U.S. policy and regulation, from stepped-up measures to protect U.S. technology, intellectual property and data from theft or acquisition by China to a new national imperative to end U.S. dependence on China for strategically important materials, components and products.

In this three-part article, we provide a comprehensive discussion of the security-driven, China-focused policy and regulatory developments affecting private sector businesses, with particular attention to recent changes addressing U.S. supply chain concerns. We discuss key U.S. policy and regulatory developments and the consequences for private sector businesses, focusing on potential opportunities, as well as regulatory and enforcement risks.

Part one focuses on legislation and federal funding to promote onshoring and Committee on Foreign Investment in the United States review of foreign direct investment to impede offshoring.

Part two focuses on security requirements to protect supply chains, U.S. export controls to protect technologies and consequences for international trade.

Part three focuses on oversight and enforcement, and the impact of the 2020 U.S. presidential election.

Security Requirements to Protect Supply Chains

Several recent actions have illustrated that U.S. companies increasingly need to choose between U.S. government sales and reliance on Chinese supply chains. Although some of these actions do not expressly identify China as the target, government contractors' ties to China lie barely below the surface.

Recent U.S. moves against China-dependent supply chains extend beyond federal contracting to commercial businesses operating, providing components for or servicing critical infrastructure — notably including the ban on federal funding in the U.S. telecommunications system for components by Huawei Technologies Co. Ltd. and ZTE Corp.

U.S. Department of Defense-mandated cybersecurity and data protection requirements for systems handling sensitive unclassified information are flowed down to commercial businesses in DOD supply chains.

The persistent and increasing friction in the U.S.-China relationship has exacerbated long-simmering concerns about the security of both incoming Chinese products and technologies used in U.S. supply chains and outbound transfers of products and technologies exported to China.

Supply chain risks include concerns that an adversary may sabotage or otherwise subvert the design or functioning of a system. Technology transfer risks include concerns that Chinese recipients may leverage U.S. technologies to undermine American advantages in defense and national security or convey those technologies to other U.S. adversaries.

Federal Contracting

Several recent actions have illustrated that U.S. companies increasingly need to choose between U.S. government sales and reliance on Chinese supply chains.[1]

Security Added as a Pillar of Contract Policy

In 2018, the DOD launched its Deliver Uncompromised program, part of the government's effort to establish security as the fourth fundamental pillar of defense acquisition decision-making, alongside cost, schedule and performance, thus including security considerations in source selection and performance evaluation.

New Supply Chain Risk Management Obligations

The National Defense Authorization Act for fiscal year 2019 and subsequent implementing regulations made supply chain risk management a permanent expectation of government contractors, required contractors to investigate their own supply chains to minimize and mitigate any perceived security risks, and empowered contracting agencies to impose new oversight tools leveraging both public and nonpublic information to assess contractors' supply chain risks.

Chinese Telecom and Video Ban

Section 889 of the fiscal year 2019 NDAA imposed unprecedented supply chain safeguards targeting five specific Chinese telecommunications and video surveillance technology suppliers: Huawei, ZTE, Hytera Communications Corp., Hangzhou Hikvision Digital Technology Co. and Dahua Technology Co. Ltd. Implemented in three parts over 2019 and 2020, these new rules effectively prohibit federal agencies from awarding contracts or renewing contracts with companies that use equipment or services from those Chinese companies.

Disclosure of Foreign Access to Contractor Software

Section 1655 of the fiscal year 2019 NDAA addresses foreign influence over software code licensed to the DOD, by mandating new rules requiring contractors to disclose (1) whether their noncommercial software code has been subject to review by a foreign government; (2) whether their source code has been subject to review by a foreign government or foreign person; and (3) whether the contractor has sought or received an export license for their information technology products containing custom-developed code.[2]

Ban on Defense Acquisitions from China-Controlled Entities

In June 2020, the Department of Defense issued an updated list of entities from which the federal government is prohibited from acquiring military articles and services to include Huawei and Hangzhou Hikvision, which were designated by virtue of being owned by, controlled by or affiliated with China's government, military or defense industry.

Critical Infrastructure

Recent U.S. moves against China-dependent supply chains are not limited to federal contractors and subcontractors.

Information and communications infrastructure transaction review

Under a May 2019 executive order titled "Securing the Information and Communications Technology and Services Supply Chain," the U.S. Department of Commerce is developing a system that, if implemented, would empower the department to identify, assess, and potentially prohibit or otherwise address information and communications technology, and services transactions, that are determined to present an undue risk to U.S. national security, U.S. persons, critical infrastructure or the digital economy in the U.S.

FCC Ban on Huawei and ZTE

Reflecting the primacy of the telecommunications sector in the U.S.-China drive for dominance, an order finalized by the Federal Communications Commission on June 30 declared that Huawei and ZTE, China's largest telecom companies, present unacceptable security risks to the U.S. telecommunications system.

Cementing the companies' prohibition from the build-out of 5G technologies in the U.S., this action prohibited funds from the FCC's $8.3 billion-per-year Universal Service Fund from being used to purchase equipment or services from Huawei or ZTE. This prohibition affects all users of Universal Service Fund money.

Bulk-Power Supply Infrastructure Safeguards

Similar supply chain risk measures have been imposed in the energy sector. Pursuant to a May 2020 executive order, the Federal Energy Regulatory Commission is studying how best to prohibit the network of interconnected energy transmission utilities from acquiring, importing, transferring or installing bulk-power supply electric equipment from sources associated with foreign adversaries of the U.S., focusing specifically on China and Russia.

Cybersecurity and Data Protection

Long-standing DOD and federal government concerns regarding cybersecurity and data protection have received increased attention as alarm has grown over China's efforts to penetrate U.S. networks in order to obtain sensitive defense and national security information or steal commercially valuable information.

For example, in September, the DOD released an interim rule for its Cybersecurity Maturity Model Certification process, which will require contractors to prove they are keeping up with key cybersecurity standards, including federal contract information and controlled unclassified information. The CMMC framework is designed to provide the DOD with assurance that the contractor can adequately protect controlled unclassified information at a level commensurate with the perceived risk.

The interim rule establishes a flow-down requirement to "ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments."[3]

Similarly, the DOD has led the government's efforts by requiring contractors to implement enhanced data security controls and incident reporting requirements. Following a multiyear

effort by the DOD to define the scope of information requiring protection and the necessary controls to protect this information, most DOD contractors and subcontractors are now required, under the DOD Federal Acquisition Regulations Supplement contract clauses and the National Industrial Security Program Operating Manual, to implement data security controls protecting unclassified and classified contract information, respectively, and to report data security incidents.

Finally, when government contractors rely on cloud service providers to meet federal requirements, they must establish that they have cloud services configured in compliance with National Institute of Standards and Technology Special Publication 800-171, a regulation that governs controlled unclassified information in nonfederal information systems and organizations.

U.S. Export Controls to Protect Technologies

Recent amendments to the export control regulations have added or enhanced numerous restrictions aimed at China or Chinese entities — including listing Huawei and dozens of other Chinese companies and governmental organizations on the Department of Commerce's entity list and extending export licensing requirements for certain items to any Chinese person or entity "whose actions or functions are intended to support military end-uses," even if there is no nexus between that support and the items being exported.

U.S. export control regulations provide one of the government's principal levers for curtailing U.S.-China technological exchange. Recent amendments to the export control regulations have focused especially on restrictions aimed at China or Chinese entities.

Emerging and Foundational Export Controls

The Export Control Reform Act initiated a regulatory process for imposing new export control licensing requirements for emerging and foundational technologies that historically have not been subject to restrictions based on design or performance considerations. This regulatory mechanism was implemented to provide new tools for denying Chinese access to important U.S. technologies that are either too new or too ubiquitous for the traditional multilateral export control regime.

Although the U.S. has not yet imposed unilateral controls under this authority, in a rule issued in June, the U.S. secured new multilateral controls for certain emerging technologies mostly relating to precursor chemicals with chemical weapons applications. Separately, in January, the Commerce Department exercised a rarely used authority to impose a temporary unilateral control on certain geospatial imaging software that was not previously controlled.

Several measures have expressly targeted China and Chinese entities.

Huawei Entity List Export Ban

Most prominently, Huawei and many affiliated companies were added to the entity list in May 2019, effectively banning Huawei's access to any items or technologies subject to U.S. regulatory authority. A subsequent act of Congress imposed conditions on any future effort to remove these restrictions. Then, in May, the Commerce Department expanded the Huawei ban so that it now covers certain foreign-produced items when there is knowledge that such items would be furnished to a designated entity on the entity list.

Entity List and Human Rights Actions

The Commerce Department has taken other actions to curtail exports to China through entity list prohibitions, particularly related to Chinese government human rights abuses targeting Uighurs in the Xinjiang Uighur Autonomous Region.

On July 1, several U.S. agencies jointly issued an advisory cautioning that U.S. companies would face reputational, economic and legal risks for continued involvement with entities that engage in human rights abuses in Xinjiang. The legal risks might include liability under various federal or state human trafficking and forced labor laws.

Chinese Military End-Users

Effective June 29, the Commerce Department expanded export licensing requirements for China to include military end-users, in addition to preexisting restrictions applicable to military end-uses for certain designated items and technologies spread across eight of the 10 export classification categories.

This seemingly technical amendment had sweeping impact because the military end-users subject to these new controls include any Chinese person or entity "whose actions or functions are intended to support military end-uses," even if that support is unrelated to the particular items being exported. Thus, exporters must now exercise heightened diligence with respect to a wide range of Chinese end-users, any one of which could be a military end-user.

Repeal of Civil End-Use Authorizations

In addition, effective June 29, another rule aimed principally at China repealed the civil end-use license exception that previously authorized certain exports to China, provided they would be used for strictly civilian purposes. This revision reflected the U.S. government's conclusion that "many countries seek to align civil and defense technology development for many reasons — to achieve greater efficiency, innovation, and growth," making it impracticable to "determine whether the end-use and end-users of items proposed for export, reexport or transfer (in-country) will not be or are not intended for military uses or military end-users."

Tightened Controls for Exports to Hong Kong

Following China's imposition of a stringent new security law that undermined the autonomy of Hong Kong, the Commerce Department quickly tightened export controls to Hong Kong, effective June 30. Now exports to Hong Kong will be treated the same as exports to China and subject to heightened scrutiny for potential illegal diversion to Chinese or other unauthorized end-users or end-uses.

Consequences for International Trade

This section probes two sets of implications of decoupling and onshoring policies: (1) implications related to China and (2) implications for global trade if the U.S. and third-party countries adopt these policies with respect to one another, not just China.

China Outlook

As an initial matter, government-led efforts to induce companies to shift supply chains away

from China will face substantial headwinds. The size and growth potential of the China market are powerful draws for foreign companies. Also, companies have invested significantly in developing their existing supply chains, including in China, and it is expensive and logistically difficult to reestablish them once they have been shortened or dismantled.

China may use tools to directly challenge decoupling and onshoring policies, as well as companies from countries that adopt them. China may pursue challenges at the World Trade Organization, as discussed in more detail below. More likely, China will employ a combination of carrots — e.g., subsidies and other incentives — and sticks — trade- or nontrade-related retaliation — to induce foreign companies to continue doing business in China.

In addition, China will likely respond to these efforts by accelerating some of the same policies that led these countries to pursue decoupling and onshoring in the first place. For example, barring effective international opposition, China can be expected to continue investing massive resources into subsidies for domestic technology and efforts to obtain foreign technology by any means necessary.

China will likely contend that it has no choice as avenues to obtaining advanced technology through other means recede. In addition, having taken affirmative steps in the decoupling process, China's trading partners will no longer be able to use the threat of it to deter China from pursuing this path.

These types of Chinese responses will present significant challenges for U.S. companies. With respect to the China market, some U.S. companies may exit, but they may relocate to lower-cost countries — e.g., Vietnam, Indonesia, Mexico — instead of the U.S.

Indeed, some Trump administration policies are likely to fuel such decisions: For example, the tariffs that the Trump administration has imposed on China under Section 301 of the Trade Act of 1974 are incentivizing some U.S. companies to outsource U.S. production, as these tariffs have increased costs for U.S. manufacturers that depend on Chinese parts.

Global Outlook

If countries apply these types of policies in their relations with one another — for example, if countries onshore their supply chains regardless of whether they currently run through China or friendlier trading partners — the onshoring trend will have an even greater impact on the global trading system. In the period since World War II, the movement of goods and services across borders has created enormous wealth and brought millions of people out of poverty.

Global trade has been made possible, in part, by widely accepted international trade rules in the General Agreement on Tariffs and Trade and additional agreements that entered into force in the 1990s with the creation of the WTO. Decoupling and onshoring policies cut in the opposite direction, limiting global trade.

In some cases, decoupling and onshoring policies are likely to violate the WTO agreement and other international rules. These policies are emerging, however, at a time when the WTO's dispute resolution mechanism is stalled due in large part to U.S. concerns about the WTO appellate body. Thus, WTO members are currently unable to use WTO dispute settlement procedures to obtain final decisions on the consistency of challenged measures with WTO rules.

In this environment, companies need to look to alternative means to protect their trade interests. For example, under Section 301 of the Trade Act, companies can petition the Office of the U.S. Trade Representative to initiate investigations into unfair foreign trade practices. If the USTR finds that the practices are inconsistent with Section 301, it can authorize a wide range of remedies, including tariffs. The European Union is currently considering whether to adopt a similar tool.

Aside from such unilateral mechanisms, companies should ensure they are familiar with the vast network of bilateral, regional and supraregional free trade agreements that may protect their trade interests, such as the recently negotiated U.S.-Mexico-Canada Agreement.

Other free trade agreements are currently under negotiation. Companies should ensure that their trade interests are reflected in these negotiations, as bilateral and regional negotiations are likely to supplant multilateral negotiations at the WTO for the foreseeable future.

Jamie Gorelick and Stephen Preston are partners, and Matthew Ferraro is counsel, at WilmerHale.

WilmerHale partner Jason C. Chipman, counsel Rachel Dober, partner Jeremy D. Dresner, partner Barry J. Hurewitz, senior public policy adviser Rob Lehman, special counsel Lauren Mandell and partner David J. Ross contributed to this article.

[1] Although some of these actions do not expressly identify China as the target, government contractors' ties to China are the clear concern.

[2] Likewise, producers of software with significant Chinese or other foreign influence might see their U.S. government business dry up. In July 2018, the undersecretary of defense for acquisition and sustainment confirmed the existence of a nonpublic "Do Not Buy" list of software products, believed to be primarily of Russian or Chinese origin, that do not meet national security standards.

[3] Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 Fed. Reg. 61505 (Sept. 29, 2020), https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of.