US Decoupling From China and the Onshoring of Critical Supply Chains:

Implications for Private Sector Businesses

September 21, 2020

*By **Jamie Gorelick** and **Stephen Preston***

With Jason C. Chipman, Rachel Dober, Jeremy D. Dresner, Matthew F. Ferraro, Barry J. Hurewitz, Rob Lehman, Lauren Mandell and David J. Ross

With the onset of the COVID-19 pandemic and the serious supply chain vulnerabilities it has exposed, we are seeing a seismic shift in US policy and regulation, from stepped-up measures to protect US technology, intellectual property and data from theft or acquisition by China to a new national imperative to end US dependence on China for strategically important materials, components and products. In this paper, 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 US supply chain concerns.

Introduction and Summary

In our January 2019 paper, "Regulatory Efforts to Protect US Innovation From China,"[1] we described a broad and sustained campaign of the US government to block China's access to advanced US technologies and counter its efforts to compromise sensitive government information and defense systems. In the past year and a half, that campaign has grown so much in scope and intensity that it has become a distinct phenomenon: a determined, widescale and bipartisan movement to revisit the globalization of supply chains integral to the free trade regime that has prevailed, with the support of both US political parties, for decades, seeking to reverse in significant respects the integration of the American and Chinese economies.

Beyond increasingly robust efforts to protect existing US advantages in technology, the government is now trying to regain what the United States has lost to China—critical production capability—and

[1] Jamie Gorelick and Stephen Preston, *Regulatory Efforts to Protect US Innovation From China: Implications for Private Sector Businesses*, WILMERHALE CLIENT ALERT (Jan. 10, 2019), https://www.wilmerhale.com/en/insights/client-alerts/20190110-regulatory-efforts-to-protect-us-innovation-from-china-implications-for-private-sector-businesses.

otherwise ensure that the country will have or can get what it needs in the future without relying on China-controlled supply chains. The intended result has been described as an economic "decoupling" from China and the "onshoring" of industries to eliminate vulnerability to single points of failure and provide reliable domestic (or at least friendly) sources of supply.[2]

The effects of this decoupling from China and onshoring of supply chains will reach a wide range of economic sectors, from telecommunications, pharmaceuticals and medical devices to microprocessors, rare earth minerals and permanent magnets. While these efforts are motivated largely by concerns about China as an economic rival and potential military adversary, they are not necessarily limited to China, as the United States may compete with allied or other countries where national interests require onshoring domestic production (e.g., of vaccines and ventilators) and, at the same time, may look to allies and friends as reliable sources of supply where diversifying away from China is deemed sufficient. Finally, this is not a short-lived phenomenon. Like protecting advanced technologies, reversing supply chain dependence on China has been embraced by both political parties and, with differences in emphasis and rhetoric, may be expected to continue apace whatever the outcome of the upcoming election.

In this paper, we discuss key US policy and regulatory developments and the consequences for private sector businesses, focusing on potential opportunities, as well as regulatory and enforcement risks. The discussion proceeds in seven parts, as highlighted below:

1. *Legislation and Federal Funding to Promote Onshoring*

   The CARES Act and authority under the Defense Production Act delegated to the US International Development Finance Corporation present opportunities for businesses to obtain federal funding for the purpose of building/rebuilding industrial base capabilities/supply chains in the United States.

   Additional opportunities may be presented by provisions addressing US dependence on foreign manufacturing in the next National Defense Authorization Act (for FY 2021) and in proposed follow-on COVID-19 relief legislation—some industry specific (e.g., medical supplies, semiconductors, rare earth minerals).

2. *CFIUS Review of Foreign Direct Investment to Impede Offshoring*

   Through reform legislation enacted in 2018, Congress greatly expanded the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS). Member agencies are, in turn, dramatically increasing the number of personnel devoted to reviewing transactions notified to CFIUS and investigating deals of national security interest that the parties did not notify.

   Nearly all corporate transactions with foreign acquirors or investors now merit some level of CFIUS risk analysis to determine whether a deal triggers a mandatory filing or presents a risk of CFIUS attention. And China deals, especially those involving the health sector, advanced

[2] "Onshoring" is used broadly to refer to the movement back to the United States of production capability that has been relocated overseas (also known as "reshoring") or otherwise building domestic production capability that has atrophied in the United States and/or developed abroad.

technology or information about US persons, are increasingly likely to be reviewed by CFIUS before or after closing.

3. *Security Requirements to Protect Supply Chains*

Several recent actions have illustrated that US companies increasingly need to choose between US 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 US 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 for Huawei and ZTE components in the US telecommunications system.

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.

4. *US 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 US 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.*

5. *Consequences for International Trade*

Government-led efforts to induce companies to shift supply chains away from China will face substantial headwinds because the potential size and growth of the China market are powerful draws for foreign companies.

China may use tools to directly challenge decoupling and onshoring policies and companies from countries that adopt them. There may be challenges at the World Trade Organization (WTO). More likely, China will employ a combination of carrots (e.g., subsidies and other incentives) and sticks (trade- or non-trade-related retaliation) to induce foreign companies to stay.

6. *Oversight and Enforcement*

The availability of federal funding for COVID-19 relief and the US industrial base may present opportunities (as noted in the part 1 summary above), but those opportunities will come with substantial risk of external scrutiny. Companies doing business in China and offshore can expect questions about how they have used any such funds.

Ensuing investigations by executive agencies likely will be rooted in the False Claims Act and the Foreign Agents Registration Act. Moreover, continued congressional investigations focused on Chinese trade, particularly in the tech sector, are likely.

7. *Impact of the 2020 US Presidential Election*

Whether President Trump or former Vice President Biden wins the 2020 election, the next administration will likely treat China as a strategic adversary and will look to reduce US supply chain dependence on China and rebuild domestic production capability for critical goods. Of course, there are significant differences between the candidates.

In the coming months, and if he is reelected, President Trump is likely to more aggressively pressure China to comply with its commitments in the US-China Phase 1 trade agreement, especially China's commitment to purchase US agricultural products. We should expect no moderation in the messaging, as indicated by, for example, Trump's expressed interest in "a complete decoupling from China" and his secretary of state's call for confrontation in place of engagement.

Vice President Biden is likely to focus on "bringing home" more US manufacturing. In his recently released "Plan to Rebuild U.S. Supply Chains," he outlined "fundamental reforms [to] shift production of a range of critical products back to U.S. soil, creating new jobs and protecting U.S. supply chains against national security threats." In addition to medical supplies and equipment, Biden emphasized the need for greater domestic resiliency for energy and grid technologies, semiconductors and key electronics, telecommunications infrastructure, and key raw materials.

In a second term of the Trump Administration, we would anticipate continued aversion to US participation in multilateral organizations and sometimes fraught relations with friendly governments. In contrast, a Biden Administration could be expected to take a multilateral approach to China, working with allies to address supply chain vulnerabilities and, possibly, pursuing a regional trade agreement based on the former Trans-Pacific Partnership.

Discussion

I. Legislation and Federal Funding to Promote Onshoring

In recent years, both Congress and the Trump Administration have acted to promote the onshoring of US manufacturing, particularly as related to such industries as pharmaceuticals, semiconductors, aluminum and steel. The COVID-19 pandemic has accelerated these onshoring efforts, particularly given China's dominance of certain medical-supply markets. For example, Congress has included provisions intended to discourage outsourcing in its COVID-19-relief efforts, and the Trump Administration has used the Defense Production Act (DPA) to encourage domestic production and support domestic supply chains for resources needed to combat the pandemic. Congress has also included proposals to promote onshoring in pending legislation, such as the National Defense Authorization Act for Fiscal Year 2021 (FY21 NDAA) and the next round of COVID-19 relief. Although

congressional Republicans and Democrats differ on some of the specifics, as a general matter, there is wide bipartisan support for these types of initiatives.

In March 2020, Congress passed and the president signed into law the Coronavirus Aid, Relief, and Economic Security (CARES) Act, a $2.2 trillion economic stimulus bill to address the economic impact of the COVID-19 pandemic. The law represented the largest economic stimulus package in American history,[3] and it included explicit efforts to prevent the offshoring of American economic activity. Specifically, in Title IV of the CARES Act, Congress authorized the Treasury Department to implement a program to provide direct loans to midsize businesses negatively impacted by the pandemic; however, the CARES Act requires Treasury to condition the loans on certifications that loan recipients will not outsource or offshore US jobs.

In May 2020, the president took a more overt step to promote onshoring by issuing an executive order (EO) delegating authority under the DPA to the US International Development Finance Corporation (DFC) to support domestic industrial base capabilities needed to respond to COVID-19. The EO provided authority to the DFC to make loans that would "create, maintain, protect, expand, or restore *domestic industrial base capabilities*" supporting "the national response and recovery to the COVID-19 outbreak" or "the resiliency of any relevant *domestic supply chains*."[4] The CEO of the DFC has characterized this new authority as a "tool" the DFC would use "to re-shore critical industries in our country, advancing our national security and the security of allies all over the world."[5] Indeed, on July 28, 2020, the DFC announced a possible $765 million loan to Eastman Kodak to build capacity to produce up to 25% of the active ingredients used in US generic drugs.[6] And in August 2020, President Trump signed an EO requiring the federal government to purchase certain "essential" drugs from US manufacturers rather than from overseas companies, particularly in China.[7]

In July 2020, the House and Senate passed their respective versions of the FY21 NDAA, and both bills include provisions to promote onshoring. For example, the Senate bill would afford new authority to the Department of Commerce to provide grants to "covered entities" to construct, expand or modernize facilities related to semiconductor manufacturing and research and development. The House bill includes a similar provision. While the two bills must be reconciled in conference, the conferees are expected to retain the semiconductor provisions in the final bill. Other FY21 NDAA provisions aim to reduce reliance on China for "critical minerals" and "rare earth elements" by

---

[3] Sarah D. Wire, *Senate Passes $2-Trillion Economic Stimulus Package*, LOS ANGELES TIMES (March 25, 2020), https://www.latimes.com/politics/story/2020-03-25/vote-senate-on-2-trillion-economic-stimulus-package-coronavirus.

[4] *Executive Order on Delegating Authority Under the DPA to the CEO of the US International Development Finance Corporation to Respond to the COVID-19 Outbreak*, THE WHITE HOUSE (May 14, 2020), https://www.whitehouse.gov/presidential-actions/eo-delegating-authority-dpa-ceo-u-s-international-development-finance-corporation-respond-covid-19-outbreak.

[5] *Boehler Statement on Defense Production Act*, US INTERNATIONAL DEVELOPMENT FINANCE CORPORATION (May 14, 2020), https://www.dfc.gov/media/press-releases/boehler-statement-defense-production-act.

[6] *DFC to Sign Letter of Interest for Investment in Kodak's Expansion Into Pharmaceuticals*, US INTERNATIONAL DEVELOPMENT FINANCE CORPORATION (July 28, 2020), https://www.dfc.gov/media/press-releases/dfc-sign-letter-interest-investment-kodaks-expansion-pharmaceuticals.

[7] *Executive Order on Ensuring Essential Medicines, Medical Countermeasures, and Critical Inputs Are Made in the United States*, THE WHITE HOUSE (August 6, 2020), https://www.whitehouse.gov/presidential-actions/executive-order-ensuring-essential-medicines-medical-countermeasures-critical-inputs-made-united-states.

strengthening domestic production and supply chains for these important materials and establishing the goal to "[e]nsure, by 2030, secure sources of supply for strategic minerals."

Congress is also considering the inclusion of onshoring provisions in the next round of coronavirus relief. For example, the Health and Economic Recovery Omnibus Emergency Solutions (HEROES) Act, which the House passed in May and would cost an estimated $3.5 trillion, would direct the National Academies of Sciences, Engineering, and Medicine to establish a committee of experts to analyze the impact of the United States' dependence on the foreign manufacture of critical drugs and devices "on patient access and care" and to recommend strategies to end that dependence. The bill would also direct the government to award contracts "to expand and enhance manufacturing capacity of vaccines and vaccine candidates" to combat COVID-19, and it would direct the establishment and maintenance of domestic reserves of critical medical supplies. The Senate did not include similar provisions in its competing bill, so it remains to be seen whether the House provisions will ultimately become law. However, as of this writing, the Senate bill does include the text of the United States Manufacturing Availability of Domestic Equipment (US MADE) Act of 2020, a bipartisan bill that aims to decrease US dependence on countries like China for personal protective equipment (PPE).

Finally, Congress has adopted other laws that promote the onshoring of foreign supply chains. For example, the Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act, which Congress enacted in 2018, established the Federal Acquisition Security Council to develop a strategic plan to address supply chain risks posed by the acquisition of certain information technology and telecommunications equipment. The Secure and Trusted Communications Networks Act, which Congress enacted in March 2020, requires the Federal Communications Commission (FCC) to publish a list of communications equipment or service providers determined to pose a national security risk, prohibits the use of federal funds to purchase communications equipment or services from those providers, and calls for the removal of existing equipment from those providers.

II. CFIUS Review of Foreign Direct Investment to Impede Offshoring

Regulatory scrutiny of foreign investment in the United States has been steadily growing for several years, and that trend is unlikely to change in the near term, regardless of what happens in the November elections. With enactment of the Foreign Investment Risk Review Modernization Act in 2018, Congress expanded the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS, or the Committee). At the same time, CFIUS agencies are dramatically increasing the number of personnel devoted to reviewing transactions and investigating deals that fall within CFIUS's jurisdiction.

Just a few years ago, Treasury had fewer than 30 people devoted to CFIUS reviews. Today, there are more than 100, and Treasury's CFIUS staff count is likely to approach 200 next year. Other CFIUS agencies are following suit and likewise growing their ranks. The recent growth of CFIUS authorities and resources reflects a bipartisan belief that some foreign investment represents a threat to US strategic dominance of key technologies. This perceived threat is particularly acute relative to China. As the Department of Defense (DoD) wrote:

> China is investing in the critical future technologies that will be foundational for future innovations both for commercial and military applications: artificial intelligence, robotics, autonomous vehicles, augmented and virtual reality, financial technology and gene editing. The line demarcating products designed for commercial vs. military purposes is blurring with these new technologies.[8]

It is hard to exaggerate the degree to which many in the defense community in Washington assess that Chinese advancements in critical technology represent a zero-sum calculus for the United States (e.g., either the United States wins the race for 5G or artificial intelligence (AI), or augmented reality, or China wins). One country's technological victory is the other country's defeat. In this environment, it is no surprise that Chinese investment in the United States is particularly fraught. Deals that are not notified to CFIUS may prompt attention from it, and deals submitted to CFIUS are likely to encounter substantial problems as part of the review process.

Although it's possible that a new administration will lower the temperature on US-China relations, easing regulatory scrutiny of foreign investment, the practical reality is that former Vice President Joe Biden has shown no interest in curtailing the foreign investment review processes. For example, the Biden campaign identifies supply chain security as a serious threat to the United States:

> Just like the United States itself, no U.S. ally should be dependent on critical supplies from countries like China and Russia. That means developing new approaches on supply chain security—both individually and collectively—and updating trade rules to ensure we have strong understandings with our allies on how to best ensure supply chain security for all of us.[9]

For a long time, CFIUS authority to review deals was relatively straightforward: the Committee had the power to review transactions where a foreign person acquired "control" of a US business. But today, CFIUS effectively has three separate jurisdictional regimes: a *voluntary regime* that captures a substantial amount of foreign investment in the United States; a *mandatory regime* that requires foreign investment in certain advanced technology companies to be notified to CFIUS in advance; and a new *real estate regime* that gives CFIUS special authority to review the foreign acquisition of lease or ownership interests in property in close proximity to over 100 specially identified federal installations.

For the voluntary CFIUS regime, the Committee has the power to review (a) any "control transaction" to determine the effect of a foreign person having "control" of a US business on the national security of the United States or (b) any "covered investment," which is any direct or indirect investment by a foreign person in a Technology, Infrastructure, or Data (TID) US Business that does not result in control of the US business but affords the foreign person with (i) access to material nonpublic technical information, personal data or critical infrastructure information; (ii) membership or observer rights on the board of the US business; or (iii) any other involvement in the operation of the US business (other than with respect to voting shares).

CFIUS has broad authority to initiate an investigation of any covered transaction over which it has jurisdiction that has not been notified to CFIUS and that may raise national security issues. In

[8] Defense Innovation Unit Experimental (DIUx), *China's Technology Transfer Strategy* (2018).
[9] *The Biden Plan to Rebuild US Supply Chains and Ensure the US Does Not Face Future Shortages of Critical Equipment*, https://joebiden.com/supplychains.

particular, if parties do not file with CFIUS, and the Committee concludes that it may have jurisdiction, the Committee retains the ability to examine the transaction after closing and to potentially impose mitigation measures for any national security concerns (or in rare cases, order divestment of businesses if the transaction is sensitive).

The mandatory regime is different. Transaction parties must formally notify CFIUS *before* closing of two types of transactions. (Failure to notify a deal covered by these rules can result in a fine of up to the value of the transaction.) First, a mandatory notification to CFIUS is required for certain transactions involving US businesses that produce, design, test, manufacture, fabricate or develop critical technology. Second, parties must notify CFIUS of any covered control transaction or covered investment that results in a foreign government having a "substantial interest" in certain companies associated with advanced technology, critical infrastructure or large amounts of sensitive personal data.

Together, the voluntary and mandatory regimes give CFIUS powerful tools to review a broad spectrum of foreign investment activities that may pose potential threats to the United States. For example, the COVID-19 pandemic has revealed perceived supply chain vulnerabilities associated with life sciences, pharmaceuticals and related biotechnology development. Both the United States and other jurisdictions are working aggressively to use foreign investment review authorities to protect medical supplies. The European Commission has publicly identified health sector companies as meriting special foreign direct investment reviews:

> [T]oday more than ever, the EU's [European Union's] openness to foreign investment needs to be balanced by appropriate screening tools. In the context of the COVID-19 emergency, there could be an increased risk of attempts to acquire healthcare capacities (for example, for the production[] of medical or protective equipment) or related industries such as research establishments (for instance, developing vaccines) via foreign direct investment. Vigilance is required to ensure that any such FDI [foreign direct investment] does not have a harmful impact on the EU's capacity to cover the health needs of its citizens.[10]

CFIUS is already following a similar course.[11] *The Wall Street Journal* recently reported that CFIUS is forcing a review of a past Chinese investment in a pharmaceutical company "after learning the firm was in talks to participate in a Pentagon project to develop injection devices for a coronavirus vaccine, according to people familiar with the matter."[12]

These new authorities for CFIUS to review deals—and to require notification before closing—speak to the growing complexity around transactions involving foreign investors. Nearly all corporate acquisition and investment transactions now merit some level of CFIUS risk analysis to determine whether a deal triggers a mandatory filing or presents a risk of CFIUS attention. And China deals,

---

[10] European Commission, *Guidance to the Member States Concerning Foreign Direct Investment and Free Movement of Capital From Third Countries, and the Protection of Europe's Strategic Assets, Ahead of the Application of Regulation (EU) 2019/452*, https://trade.ec.europa.eu/doclib/docs/2020/march/tradoc_158676.pdf (emphasis omitted).

[11] Himamauli Das, *Five CFIUS Enhanced Enforcement Trends During COVID-19*, BLOOMBERG INSIGHTS (May 19, 2020), https://news.bloomberglaw.com/white-collar-and-criminal-law/insight-five-cfius-enhanced-enforcement-trends-during-covid-19.

[12] Kate O'Keefe, *US National Security Panel Examining Chinese Investors' Purchase of Pharma Firm*, WALL STREET JOURNAL (July 10, 2020), https://www.wsj.com/articles/u-s-national-security-panel-examining-chinese-investors-purchase-of-pharma-firm-11594406334.

especially those involving the health sector, advanced technology or US-person information, are increasingly likely to be reviewed by CFIUS before or after deal closing.

III. Security Requirements to Protect Supply Chains

The persistent and increasing friction in the US-China relationship has exacerbated long-simmering concerns about the security of both incoming Chinese products and technologies used in US supply chains and outbound transfers of products and technologies exported to China. Supply chain risks include concerns that an adversary may sabotage, maliciously introduce unwanted functions into or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation or maintenance of a system. Technology transfer risks include concerns that Chinese recipients may leverage US technologies to undermine American advantages in defense and national security or convey those technologies to other US adversaries, such as Iran.

A. Federal Contracting

Several recent actions have illustrated that US companies increasingly need to choose between US 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. For example:

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. Section 881 of the National Defense Authorization Act for Fiscal Year 2019 (FY19 NDAA) 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 FY19 NDAA imposed unprecedented supply chain safeguards targeting five specific Chinese telecommunications and video surveillance technology suppliers: Huawei, ZTE, Hytera Communications, Hangzhou Hikvision and Dahua. Implemented in three parts over 2019 and 2020, these new rules (1) prohibit government agencies from acquiring the targeted equipment and services directly or as a substantial or essential component or critical technology of any system; (2) prohibit contract awards, extensions or renewals to any prime contractor that uses the targeted equipment or services as a substantial or essential component or critical technology of any system, whether or not such use has any relation to the entity's federal government work; and (3) prohibit recipients of federal government grants and loans from using those funds to acquire the targeted equipment or services. The sweeping "use" prohibition is accompanied by stringent conditions on

any agency waivers, including a full disclosure of the contractor's reliance on the targeted equipment and services and a comprehensive plan for phasing them out.

Disclosure of foreign access to contractor software. Section 1655 of the FY19 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.

Blacklisting of software presenting a security risk. Producers of software with significant Chinese or other foreign influence might see their US 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.

Ban on defense acquisitions from China-controlled entities. Some new measures targeting Chinese supply chains have leveraged existing legal authorities. For example, a 1999 law prohibited the federal government from directly or indirectly acquiring military articles and services from companies designated as "Communist Chinese military companies." In June 2020, the Department of Defense issued an updated list of entities, including Huawei and Hangzhou Hikvision, designated by virtue of being owned by, controlled by or affiliated with China's government, military or defense industry.

B. Critical Infrastructure

Recent US 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 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 critical infrastructure or the digital economy in the United States, or an unacceptable risk to US national security or the safety of US persons. The contemplated system described in November 2019 would allow the department to require mitigation, prohibition or an unwinding of such transactions, and it would not provide a CFIUS-like pre-clearance process.

FCC ban on Huawei and ZTE. Reflecting the primacy of the telecommunications sector in the US-China battle for dominance, an order finalized by the Federal Communications Commission on June 30, 2020, declared that Huawei and ZTE, China's largest telecom companies, present unacceptable security risks to the US telecommunications system. Cementing the companies' prohibition from the build-out of 5G technologies in the United States, this action prohibited funds

from the FCC's $8.3 billion-per-year Universal Service Fund (USF) from being used to purchase equipment or services from Huawei or ZTE. This prohibition affects all users of USF money, including schools, libraries, rural healthcare facilities, certain low-income consumers, and designated wireless and wireline telecommunications carriers. The FCC action prompted the UK government to adopt a similar ban in July 2020.

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 United States, focusing specifically on China and Russia. This new regulatory framework, which could be replicated in other industries, may also prescribe criteria for the "pre-qualification" of equipment and vendors, identify suppliers that present unacceptable risks, and establish an interagency coordinating body to secure government electricity supplies.

C. 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 US networks in order to obtain sensitive defense and national security information or steal commercially valuable information.

For example, in 2019 and 2020, DoD developed the Cybersecurity Maturity Model Certification (CMMC) process to certify that contractors have the controls in place to protect sensitive data. Such data includes federal contract information and controlled unclassified information (CUI).

The CMMC framework is designed to provide DoD with assurance that the contractor can adequately protect CUI at a level commensurate with the perceived risk. It combines various cybersecurity practices and processes and maps them to maturity levels, ranging from basic cyber hygiene (Level 1) to highly advanced practices (Level 5). The CMMC requires third-party certification to verify implementation. In order to be certified, contractors will be required to coordinate directly with accredited third-party commercial certification organizations and request the appropriate certification. DoD is creating a CMMC accreditation body that will provide oversight for CMMC accreditations and assessments, including managing and providing all associated processes. DoD guidance has made clear that the CMMC requirement will be a sweeping flow down to "all companies conducting business" with the DoD, including to those contractors and subcontractors that do not handle CUI. But it remains uncertain exactly how DoD guidance will apply CMMC to subcontractors.

Similarly, 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 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 DoD Federal

Acquisition Regulations Supplement (DFARS) contract clauses and the National Industrial Security Program Operating Manual (NISPOM), to implement data security controls protecting unclassified and classified contract information, respectively, and to report data security incidents. Recent implementation of the DFARS requirements has proven particularly challenging to the private sector, given the scope of mandatory requirements relating to authentication, logging, incident reporting and other specific security controls.

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 NIST 800-171, a regulation that governs CUI in nonfederal information systems and organizations.

IV. US Export Controls to Protect Technologies

US export control regulations provide one of the government's principal levers for curtailing US-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 of 2019 initiated a regulatory process for imposing new export control licensing requirements for "emerging" and "foundational" technologies that have not historically 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 US technologies that are either too new or too ubiquitous for the traditional multilateral export control regime. Although the United States has not yet imposed unilateral controls under this authority, in a rule issued in June 2020, the United States secured new multilateral controls for certain emerging technologies mostly relating to precursor chemicals with chemical weapons applications. Separately, in January 2020, 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. For example:

Huawei Entity List (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 US regulatory authority. A subsequent act of Congress imposed conditions on any future effort to remove these restrictions. Then, in May 2020, 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. As a result, if Huawei or its HiSilicon chipmaking arm produces or develops, for example, an integrated circuit design utilizing certain US-regulated electronics, computing, or telecommunications technologies or software, the resulting foreign-produced integrated circuit design is subject to the ban. This expanded prohibition also covers foreign-made items that are the direct products of a production facility that is itself a direct product of certain US-origin electronics, computing, or telecommunications technologies or software.

Entity List and human rights actions. The Commerce Department has taken other actions to curtail exports to China through Entity List prohibitions. For example, in October 2019 and June and July 2020, over 70 additional Chinese entities and governmental organizations were added to the Entity List, over half of which were designated upon being implicated in human rights violations and abuses against Uighur communities and other ethnic minorities in the Xinjiang Uighur Autonomous Region. Escalating the US campaign against Chinese activities in Xinjiang, on July 1, 2020, several US agencies jointly issued an advisory cautioning that US 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. In a further action on July 9, 2020, Treasury imposed sanctions on a Chinese government public security agency and four current or former Chinese government officials for their roles in Xinjiang.

Chinese military end users. Effective June 29, 2020, 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, 2020, 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 US 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, 2020. Hong Kong has traditionally been afforded more favorable treatment than China under US export regulations, but Hong Kong's loss of autonomy from Beijing ended that practice, so that 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.

V. Consequences for International Trade

In the years preceding the 2008 financial crisis, there was significant growth in international trade and a deepening of global supply chains, in part connected to China's entry into the World Trade Organization (WTO) in 2001. Since the financial crisis, however, this process has slowed for several

reasons, including China's increasing reliance on domestic rather than foreign demand, the movement of Chinese goods up the global value chain, and rising protectionism worldwide. Sustained, but modest, trade expansion in certain regions, including Central and Eastern Europe and Southeast Asia, has been offset by stagnating trade in North America and other regions.[13]

This is the international trade context in which the United States and other countries are pursuing policies to promote domestic technology and reorient supply chains away from China (i.e., decoupling and onshoring policies). These policies are motivated by current events—including the COVID-19 crisis and growing concern in many countries about China's trade and technology practices—but they will amplify, not diverge from, recent trends.

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 United States and third-party countries adopt these policies with respect to one another, not just China.

A. 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 will always draw foreign companies. Also, companies have invested significantly in developing their existing supply chains, including in China, and it is expensive and logistically difficult to re-establish them once they have been shortened or dismantled. Recent events in Japan are instructive. In April, just as the Japanese government was announcing plans to pay Japanese companies to leave China, 22% of Japanese companies surveyed by the Japan External Trade Organization said they planned to expand their China business, up 7% from the previous month.

China may also use tools to directly challenge decoupling and onshoring policies, as well as companies from countries that adopt them. China may pursue challenges at the WTO, 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 non-trade-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.

[13] *See* Tamim Bayoumi, Jelle Barkema and Diego A. Cerdeir, *The Inflexible Structure of Global Supply Chains* 14-15 (IMF Working Paper No. WP/19/193, September 2019), https://www.imf.org/en/Publications/WP/Issues/2019/09/13/The-Inflexible-Structure-of-Global-Supply-Chains-48562.

These types of Chinese responses will present significant challenges for US companies. With respect to the China market, some US companies may exit, but they may relocate to lower-cost countries (e.g., Vietnam, Indonesia, Mexico) instead of the United States. 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 US companies to *outsource* US production, as these tariffs have increased costs for US manufacturers that depend on Chinese parts.

B. 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, as we have seen to some extent with PPE—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 (GATT) 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 US 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 of 1974, companies can petition the Office of the US Trade Representative (USTR) to initiate investigations into unfair foreign trade practices. If USTR finds that the practices are inconsistent with Section 301, it can authorize a wide range of remedies, including tariffs. The EU 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 supra-regional free trade agreements that may protect their trade interests, such as the recently negotiated United States-Mexico-Canada Agreement. Other free trade agreements are currently under negotiation. (For example, the United States is currently negotiating agreements with the United Kingdom and Kenya.) 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.

VI. Oversight and Enforcement

In recent years, a range of US oversight and enforcement authorities have been reviewing Chinese trade issues. Since the COVID-19 pandemic, both US political parties have emphasized concerns about supply chain vulnerability and US dependence on China. We can expect oversight and

enforcement leaders to assess potential inquiries through this lens. While recipients of federal funding can always expect scrutiny, the global impact of COVID-19 has made all Chinese operations ripe for investigation. New investigations have emerged, and we expect this trend to continue.

Companies doing business in China and offshore can expect scrutiny of how they may have used any CARES Act or other COVID-19-relief funds, given the recent focus on onshoring. Ensuing investigations by executive agencies likely will be rooted in the False Claims Act (FCA) and the Foreign Agents Registration Act (FARA). Moreover, continued congressional investigations focused on Chinese trade, particularly in the tech and health sectors, are likely on the horizon.

A. CARES Act and Other COVID-19 Relief

As discussed in Section I, the CARES Act makes available trillions of dollars in federal loans, grants and other financial assistance to a wide range of industries that have been affected by the COVID-19 pandemic. Emergency infusions of government funding into the economy are typically followed by significant investigations, both by oversight entities created specifically for this purpose and by the standard constellation of law enforcement organizations, government agencies and congressional committees. These watchdogs have launched inquiries into alleged fraud, waste and abuse associated with CARES Act funds. So far, the primary focus has been on fraudulent Paycheck Protection Program (PPP) applications (e.g., on behalf of fake companies); price gouging (e.g., high cost of eggs); worker protections (e.g., proper PPE and social distancing requirements for farm workers); and fraudulent sales of supplies (e.g., sham COVID-19 tests).

Also as discussed above, President Trump issued an EO delegating DPA lending and contracting authority to the CEO of the DFC to boost "domestic production of strategic resources needed to respond to the COVID-19 outbreak, or to strengthen any relevant domestic supply chains."[14] In addition, as of this writing, Congress is considering legislation to provide further COVID-19 relief. Recipients of federal funding from the DFC or under such follow-on legislation can expect the same level of scrutiny that beneficiaries of the CARES Act are getting.

B. Executive Agency Enforcement: FCA and FARA

Enforcement context. The Trump Administration has taken a strong stance toward China in both its policy and enforcement actions. In 2018, the Department of Justice's (DOJ) National Security Division launched the China Initiative to target economic espionage, trade secret theft and hacking. In February 2020, the DOJ indicted Huawei and other defendants, including two US subsidiaries and Huawei's chief financial officer. The charges included conspiracy to steal trade secrets, racketeering conspiracy and violations of sanctions on Iran.

[14] *Executive Order on Delegating Authority Under the DPA to the CEO of the US International Development Finance Corporation to Respond to the COVID-19 Outbreak*, THE WHITE HOUSE (May 14, 2020), https://www.whitehouse.gov/presidential-actions/eo-delegating-authority-dpa-ceo-u-s-international-development-finance-corporation-respond-covid-19-outbreak.

False Claims Act. The DOJ has promised vigorous enforcement of the CARES Act and stated that "the False Claims Act is one of the most effective weapons in our arsenal."[15] The FCA requires companies and individuals seeking federal funds to be truthful and accurate in representations they make about their eligibility for those funds. It imposes treble damages and civil penalties, and it offers rewards for insiders who file claims on behalf of the government. FCA cases may arise based on certifications associated with the receipt of funds under CARES Act programs such as the PPP.

The PPP provides forgivable loans to eligible small businesses that spend the money on employee payroll and other enumerated expenses. To participate in the PPP, borrowers and lenders must make multiple certifications to the US Small Business Administration. For example, borrowers must certify in good faith at the time of loan origination that, among other things (1) the loan request is "necessary" to "support ongoing operations" in light of current economic conditions and (2) "funds will be used to retain workers and maintain payroll or make mortgage payments, lease payments, and utility payments."

A PPP participant may run afoul of the FCA based on knowingly false certifications of compliance with the PPP's eligibility rules, notwithstanding widespread industry confusion over the scope and meaning of these rules.[16] In the context of China decoupling, companies that accepted PPP funds may face enforcement issues if they use these funds—which are fungible—to benefit China in ways that are inconsistent with their certifications. Greater scrutiny of a broad range of corporate business activities—including Chinese-focused activities—can spin off from initial questions about the propriety or legality of large corporations, or their subsidiaries, obtaining CARES Act or other COVID-19-relief funds.

Foreign Agents Registration Act. FARA requires disclosure of lobbying on behalf of foreign governments. A core goal of DOJ's China Initiative is to apply FARA "to unregistered agents seeking to advance China's political agenda," and DOJ regularly pursues such charges.[17] On July 24, 2020, DOJ entered a guilty plea of a Singaporean who established a fake consulting company and used online career networking sites to solicit US government employees to write paid reports disclosing confidential information. The defendant then provided this information to the Chinese government.[18]

---

[15] *Principal Deputy Assistant Attorney General Ethan P. Davis Delivers Remarks on the False Claims Act at the US Chamber of Commerce's Institute for Legal Reform*, THE US DEPARTMENT OF JUSTICE (June 26, 2020), https://www.justice.gov/civil/speech/principal-deputy-assistant-attorney-general-ethan-p-davis-delivers-remarks-false-claims.

[16] *See, e.g.*, Anne Sraders, *The New PPP Loan Forgiveness Application is Causing Lots of Confusion. Here's What to Know So Far*, FORTUNE (May 20, 2020), https://fortune.com/2020/05/20/sba-ppp-loan-forgiveness-application-confusion; Paul Davidson, *Coronavirus PPP Loans Leave Small Firms Confused, Wary and Rushing to Secure Cash to Survive*, USA TODAY (Apr. 13, 2020), https://www.usatoday.com/story/money/usaandmain/2020/04/13/coronavirus-small-businesses-scramblesecure-federal-ppp-loans/5133984002.

[17] *Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018*, THE US DEPARTMENT OF JUSTICE, https://www.justice.gov/opa/information-about-department-justice-s-china-initiative-and-compilation-china-related.

[18] *Singaporean National Pleads Guilty to Acting in the United States as an Illegal Agent of Chinese Intelligence*, THE US DEPARTMENT OF JUSTICE (July 24, 2020), https://www.justice.gov/usao-dc/pr/singaporean-national-pleads-guilty-acting-united-states-illegal-agent-chinese.

Attorney General William Barr has highlighted the legal risks American tech companies face when doing business in China. In a July 16, 2020, speech, Barr raised concerns that American companies prioritized their relationships with the Chinese Communist Party over their relationships with the US government. Barr suggested that American companies are being pushed to support Chinese policy and Chinese-friendly candidates. He delivered a warning shot to them by promising FARA enforcement.[19] The maximum penalty for a FARA violation is 10 years' imprisonment.

C. Congressional Inquiries: National Security Threats and US Exports to China

Congress is also focused on the relationship between China and US technology companies. For example, the Senate Judiciary Committee's Subcommittee on Crime and Terrorism has held hearings related to China's cybersecurity threats. After the March 4, 2020, hearing, titled "Dangerous Partners: Big Tech and Beijing," Subcommittee Chair Sen. Josh Hawley (R-MO), along with Sen. Rick Scott (R-FL), introduced legislation to ban all federal employees from using TikTok on government devices.[20] Of his bill, which passed the Senate in August 2020 by unanimous consent, Sen. Hawley explained: "TikTok is owned by a Chinese company that includes Chinese Communist Party members on its board, and it is required by law to share user data with Beijing."[21]

On June 22, 2020, Sens. Elizabeth Warren (D-MA) and Cory Booker (D-NJ) sent a letter to four meatpacking companies requesting specific information about their exports to China.[22] The senators were responding to reports that these companies prioritized sales to China, which caused meat shortages and high food costs in the United States. Additionally, the senators raised concerns that these companies pushed their employees to work in conditions that led to the massive spread of COVID-19 in order to facilitate the Chinese exports. On July 24, 2020, the senators reported that the companies had failed to address their concerns and that enhanced worker protections are needed. They chastised the companies because their "responses—or lack thereof—fail to sufficiently explain why they claimed there were pending domestic shortages only to go on and export record quantities of meat to China, which recent reports indicate they continue to do even as frozen supplies fall."[23]

---

[19] Betsy Woodruff Swan, *Barr Lambastes Apple in China Speech*, POLITICO (July 16, 2020), https://www.msn.com/en-us/news/world/barr-lambastes-apple-in-china-speech/ar-BB16Px1d.
[20] No TikTok on Government Devices Act, S. 3455, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3455/text.
[21] *Senators Hawley, Scott Introduce Legislation to Ban TikTok From Government Devices*, Sen. Hawley Press Release (March 12, 2020), https://www.hawley.senate.gov/senators-hawley-scott-introduce-legislation-ban-tiktok-government-devices.
[22] *Letter From Senators Elizabeth Warren and Cory Booker* (June 22, 2020), https://www.warren.senate.gov/imo/media/doc/2020.06.22%20Letter%20to%20meatpackers%20investigating%20manipulation%20of%20COVID-19%20crisis.pdf.
[23] *Warren, Booker Release Information From Their Investigation Into Giant Meatpackers Exploiting Workers and Consumers During COVID-19*, Sen. Warren Press Release (July 24, 2020), https://www.warren.senate.gov/newsroom/press-releases/warren-booker-release-information-from-their-investigation-into-giant-meatpackers-exploiting-workers-and-consumers-during-covid-19.

Congress also has raised concerns about Chinese intrusion into US colleges and universities. The US Senate Permanent Subcommittee on Investigations (PSI) has held hearings and issued reports titled "China's Impact on the US Education System" and "Securing the US Research Enterprise From China's Talent Recruitment Plans." Flowing from these inquiries, in June 2020, PSI Chair Sen. Rob Portman (R-OH) and his Senate colleagues introduced the bipartisan Safeguarding American Innovation Act in order "to help stop foreign governments, particularly China, from stealing American taxpayer-funded research and intellectual property developed at US colleges and universities."[24] Among other things, the PSI has focused on compliance with Section 117 of the Higher Education Act, which requires universities to report foreign funding and gifts to the Department of Education.

Congressional committees likely will continue this trajectory of China-focused investigations, which create reputational issues and often result in referrals to law enforcement. Following the PSI's hearings, the Department of Education launched multiple investigations into US colleges and universities, and DOJ brought multiple criminal cases against researchers, professors and Thousand Talents Program participants related to their alleged work on behalf of the Chinese government.[25] Moving forward, we can expect additional supply chain initiatives from the China Task Force, a GOP congressional body launched in May.[26]

D. Looking Ahead: Operation Warp Speed

There is intense competition to be the first country to develop and distribute a COVID-19 vaccine. US pharmaceutical companies are competing with Chinese companies, including state-owned pharmaceutical company Sinopharm. Both the executive and legislative branches are focused on this issue. On July 21, 2020, the DOJ announced criminal charges accusing foreign hackers of targeting innovation related to the coronavirus, including vaccine research. The indictment alleges that the two defendants were working with the Chinese government, targeting firms developing vaccines. It includes trade secret theft and wire fraud conspiracy charges.[27] On the same day, during a House Committee on Energy and Commerce hearing, titled "Pathway to a Vaccine: Efforts to Develop a Safe, Effective and Accessible COVID-19 Vaccine," several members asked whether materials or production of a vaccine would be located in China.[28]

---

[24] *Portman, Carper, Rubio, Senate Colleagues Introduce Bipartisan Legislation to Stop Theft of US Research & Intellectual Property by Global Competitors*, Sen. Portman Press Release (June 18, 2020), https://www.portman.senate.gov/newsroom/press-releases/portman-carper-rubio-senate-colleagues-introduce-bipartisan-legislation.

[25] *Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018*, THE US DEPARTMENT OF JUSTICE, https://www.justice.gov/opa/information-about-department-justice-s-china-initiative-and-compilation-china-related.

[26] *Leader McCarthy Announces China Task Force*, Rep. McCarthy Press Release (May 7, 2020), https://www.republicanleader.gov/leader-mccarthy-announces-china-task-force.

[27] Eric Tucker, *US Accuses Chinese Hackers in Targeting of COVID-19 Research*, AP (July 21, 2020), https://apnews.com/7aa7a893d0dc15da21a5920ab7d9f221.

[28] House Committee on Energy and Commerce, Subcommittee on Oversight and Investigations Hearing, *"Pathway to a Vaccine: Efforts to Develop a Safe, Effective and Accessible COVID-19 Vaccine"* (July 21, 2020), https://energycommerce.house.gov/committee-activity/hearings/hearing-on-pathway-to-a-vaccine-efforts-to-develop-a-safe-effective-and.

VII. Impact of the 2020 US Presidential Election

Whether President Trump or former Vice President Biden wins the 2020 US presidential election, the next administration will likely treat China as a strategic adversary and will look to reduce US dependence on China for strategically important goods and services and restrict Chinese investment in the United States. As a political matter, showing toughness on China is a political necessity; indeed, recent polling shows over 70% of Americans have a negative attitude toward China. Further, as a policy matter, there is bipartisan agreement that China is a bad actor that continues to flout international trade rules and block the negotiation of new rules to address emerging challenges.

But while the two candidates' overall positions on China have many similarities, their styles and approaches are likely to be significantly different. These differences are consequential because the United States and China are the world's two largest economies and their bilateral relationship has fallen to depths not seen since the Tiananmen Square crisis. We will discuss some of the policies, including with respect to supply chains—where the candidates agree—and highlight major policy differences.

In the next several months and if he is reelected, President Trump is likely to more aggressively pressure China to comply with its commitments under the US-China Phase 1 trade agreement. In particular, he would be focused on China's purchases of US agricultural products, which have not kept pace with China's commitments: China has purchased just $5.4 billion of the $33 billion of agricultural products it needs to purchase this year to keep pace. President Trump also has discussed his interest in pursuing Phase 2 negotiations with China to address systemic issues such as the disproportionate role of state-owned enterprises in the Chinese economy, subsidies, data flows and steel overcapacity. It is expected that Trump's "America First" efforts would expand beyond the Administration's current focus on supply chains for medical supplies (COVID-19-related) and extend to manufactured goods, critical minerals and other areas. Trump would also continue to seek to undercut Chinese efforts to dominate high-tech manufacturing, including semiconductors and other telecommunications equipment. We expect new policies that would incentivize "bringing home" such key industries.

Vice President Biden is also likely to focus on "bringing home" more US manufacturing. In his recently released "Plan to Rebuild US Supply Chains," he outlined "fundamental reforms [to] shift production of a range of critical products back to US soil, creating new jobs and protecting US supply chains against national security threats."[29] While he expectedly focused on medical equipment and pharmaceuticals, he also emphasized the importance of greater resiliency for energy and grid technologies, semiconductors, and key electronics, as well as telecommunications infrastructure and raw materials. This proposal was touted to improve the nation's ability to fight the coronavirus and future pandemics. Biden promises that if elected, he will initiate immediately a 100-day review of "critical national security risks across America's international supply chain," while asking Congress to create a permanent, mandatory review process. Biden would likely not pursue Phase 2 negotiations

[29] *The Biden Plan to Rebuild US Supply Chains and Ensure the US Does Not Face Future Shortages of Critical Equipment*, https://joebiden.com/supplychains.

in the near term, if ever, as he has indicated that he wants to focus on domestic issues initially—much as President Obama did in his first term. He would likely seek to revive the WTO as a tool to resolve disputes with China.

While Trump has taken great pride in removing the United States from international organizations and agreements (World Health Organization, Paris Climate Agreement, Trans-Pacific Partnership) and threatening to leave others (NATO and WTO), Biden will aggressively work within such multilateral efforts. Biden will likely seek to rebuild/strengthen alliances with EU and Asia trading partners. It's plausible that some multilateral trading agreement based on the former Trans-Pacific Partnership will be created. Biden will also tout his long-term international relationships with world leaders including, while he was in office, over 25 hours of meetings with China's President Xi Jinping.

In the run-up to the election, we can also expect both candidates to claim the other is weak on China and to threaten stronger action against it. While China is accustomed to being scapegoated in US election campaigns and appreciates that campaign rhetoric is not policy, the current rhetoric is of a different magnitude. Whoever wins the election will carry this baggage as they seek to steer the US-China relationship onto steadier ground.

* * *

We continue to monitor US government actions directed at China as a competing world power and provide strategic advice to businesses affected by the prevailing legal and political environments.

For more information or assistance, please contact:

Authors

Jamie Gorelick
PARTNER

jamie.gorelick@wilmerhale.com
+1 202 663 6500

Stephen Preston
PARTNER

stephen.preston@wilmerhale.com
+1 202 663 6900