WILMERHALE

JANUARY 10, 2019

Regulatory Efforts to Protect US Innovation from China:

Implications for Private Sector Businesses

By **Jamie S. Gorelick** and **Stephen W. Preston**[1]

The US Government has embarked on a broad and sustained campaign aimed at blocking China's access to advanced US technologies and countering efforts to compromise sensitive government information and defense systems. **We are struck by the scope and momentum of this campaign – unlike any seen in our professional lifetimes – and the associated expansion of federal regulatory authority.** In this paper, we discuss key policy and regulatory developments in recent months and the potential consequences for a range of industry sectors and business activities. We conclude that companies should take a fresh, hard look at their compliance and diligence functions, and their dealings with Chinese or other foreign entities, to address the increased risks resulting from these changes.

Introduction

Concerns in the United States about China's theft of intellectual property and access to strategically important technologies are certainly not new and have been escalating over the past decade, mainly among national security professionals and the American companies most adversely affected. In the past two to three years, however, these concerns have greatly intensified, gaining the sometimes-fevered attention of policy makers and now the general public. Among the principal contributing factors are these:

- China's stated ambition to dominate global markets in critical technologies, as reflected in Xi Jinping's "Made in China 2025" program, which targets 10 key industries, from aerospace and telecom devices to agricultural equipment and biopharmaceuticals (plus artificial intelligence by 2030);
- Increasing awareness of the apparent inadequacy of US foreign investment, export control, and other regulatory regimes, and China's evident success in exploiting deficiencies in or otherwise circumventing those regimes; and
- The current political environment in which competition with China is an issue that the Trump Administration has found resonates with its base and that has Republicans and Democrats in Congress battling to show who is tougher on China.

[1] Jason Chipman, David Cohen, David Horn, Barry Hurewitz, Robert Kimmitt, Robert Lehman, Benjamin Powell, Blake Roberts, David Ross and Leah Schloss contributed to the preparation of this paper.

In our view, the government's aggressive, multifront response to China as an economic rival and potential military adversary is laying a veritable minefield for any company that is, directly or indirectly, dealing with Chinese entities or supplying the Department of Defense or other federal agencies. Moreover, while the recent regulatory changes may have been motivated chiefly by concerns about China and US military superiority, most are not limited to China or defense production and apply to foreign actors and US technology more generally. And as these issues have become highly politicized, the risk of public scrutiny as well as enforcement has grown. In short, this has become (or should be) a C-suite-level concern, and staying on top of these developments is critical to avoiding a misstep that could have dramatic financial and reputational consequences.

There follow brief descriptions of the regulatory changes to which we are referring.

Committee on Foreign Investment in the United States Reform

In August, Congress passed and the President signed into law the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), which among other things expands the power of the Committee on Foreign Investment in the United States (CFIUS) to review corporate transactions involving critical technology, critical infrastructure, or sensitive personal data of American citizens. FIRRMA has quickly influenced M&A activity around the country with regard to foreign investment in US companies. As of November, for the first time, CFIUS's "pilot program" regulations provide for mandatory notification of foreign investment in a US business, operating in any of 27 specified industries, that develops/produces critical technology (broadly defined), even if the investment does not result in "foreign control" over the US business. More mandatory filing requirements will likely be promulgated in the coming months. If parties do not notify CFIUS of these deals, the Committee has the power to levy civil penalties up to the value of the transaction. These changes are creating new risks for both foreign investors and US companies, particularly those developing advanced technologies. The new rules also create complexities for investment funds with limited partners from foreign countries and place a premium on evaluating deal risks as new investments are pursued.

US Export Control Reform

In recent months, both Congress and the Administration have acted to limit China's access to sensitive US technologies through enhancements to the export control regime. Most significantly, the Export Control Reform Act of 2018 enacted in August not only provides new, permanent statutory authority for the US export control regulations, but also includes a requirement for a Commerce Department-led review to identify "emerging and foundational technologies" that merit new controls. In November 2018, Commerce issued an advance notice of proposed rulemaking in which it sought public comment on its implementation of this requirement. The Commerce Department's initial list of "representative" emerging technologies includes artificial intelligence, nanobiology and other biotech, microprocessor technology, data analytics, quantum information and sensing technology, robotics, brain-computer interfaces, advanced surveillance technologies,

and additive manufacturing (including 3D printing). This effort is designed to directly confront Chinese competition in these areas, and we expect it to be a precursor to new export restrictions, likely in the coming year.

The Commerce Department has likewise been aggressively exercising existing powers, most notably by putting prominent Chinese technology firms on its list of entities to which US companies may not export without a license. In August 2018, Commerce added 44 Chinese companies to the 90 Chinese entities already on its Entity List because of national security and foreign policy concerns, and it continues adding to this list (*e.g.*, Fujian Jinhua Integrated Circuit Company Ltd. in October).

Enhanced Cybersecurity/Data Protection Requirements

Cybersecurity and data protection remain significant concerns for DoD and across the federal government. This concern is due, in no small part, to China's efforts to penetrate US networks in order to obtain sensitive defense and national security information or steal commercially valuable information.

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, nearly all 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.

While DoD has led the way, other federal agencies are following suit. In 2016, the Federal Acquisition Regulatory Council published a final rule requiring contractors to implement certain "basic" security controls. Several new broadly applicable government contract clauses are expected to be issued in 2019 to extend requirements similar to those in the DFARS to contractors across the federal government.

New Supply Chain Security Requirements

Increasing concern about the security of US technology and the viability of US technology industries has brought significant new attention to supply chain risk management in the federal government contracting sector. Supply chain risk management refers to a wide range of long-established considerations, including efforts to monitor and sustain the health of innovative companies in the US defense industrial base, prevention and detection of counterfeit electronic components, requiring domestic production of select products and materials, and implementing

cybersecurity safeguards and information assurance regimes to promote the reliability of software and hardware used in sensitive applications.

Several new initiatives have expanded and made permanent important supply chain risk management measures that may affect any company that sells products or services directly or indirectly to the federal government. For example, the ongoing "Deliver Uncompromised" initiative is formally adding "security" as a central pillar of the federal acquisition process, supplementing the traditional triad of schedule, cost, and performance. The current-year National Defense Authorization Act made permanent a "blacklisting" authority under which contractors can be excluded from consideration for security reasons, without a right to appeal and in some instances without government disclosure of the underlying reasons for the exclusion. The same law also implemented new measures to prohibit federal agencies and recipients of federal funding from acquiring, or using within larger systems, certain information technology supplies and services from specific, named Chinese suppliers that are not otherwise subject to US sanctions. Another provision compels contractors to disclose to contracting agencies whether their software code has been previously made available for review by foreign persons or governmental authorities or has been the subject of an export license application.

More Active Congressional Oversight

There is a growing concern among Members of Congress on both sides of the aisle that China is succeeding in gaining access to sensitive US technologies and intellectual property through cyber-attack, telecommunications companies, academia, and joint venture businesses. Furthermore, many influential policy makers believe this new-age "espionage" is a long-term component of China's efforts to become a global economic, military, and political power.

During a US Senate Intelligence Committee hearing in February, FBI Director Christopher Wray stated that Chinese nontraditional collectors "are exploiting the very open research and development environment that we have, which we all revere. But they're taking advantage of it, so one of the things we're trying to do is view the China threat as not just the whole-of-government threat, but a whole-of-society threat on their end, and I think it's going to take a whole-of-society response by us." In response to these threats, Congress recently passed legislation to expand the reach of CFIUS and US export controls, as noted above.

We expect additional pushes from Congress for more transparency in and oversight of all types of collaborations with Chinese entities. With the change in control of the House, especially, the Democratic majority may be expected to significantly increase Congressional scrutiny of the private sector, concerning both its own activities and its interactions with the Trump Administration.

And the List Goes On …

Suffice it to say, these are not the only recent efforts intended to safeguard advanced US technology and intellectual property from Chinese and other foreign entities. To name just a few others:

- Trade sanctions imposed on China, specifically tariffs on $250 billion of Chinese goods in response to, and to remedy, China's use of foreign ownership restrictions to require or pressure tech transfer and its theft of intellectual property;

- Increased scrutiny of US universities with sponsored research agreements, grants, and other relationships with Chinese telecom giant Huawei and other Chinese entities;

- Renewed attention to, and more expansive application of, the Foreign Agents Registration Act, fueled by influence efforts of foreign governments including China;

- Stepped-up enforcement of US economic sanctions and elevated risk of violations for companies dealing with Chinese entities that in turn are dealing close to, or over, the edge with Iran, North Korea, Venezuela, or Russia;

- More rigorous security requirements from the Defense Security Service, the DoD component that oversees facility clearances for businesses, including a new NISPOM for companies that handle classified US Government information;

- Longer-term DoD industrial base policy recommendations directed at technology security and supply chain integrity (*see* "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," Department of Defense, September 2018); and

- New or enhanced foreign direct investment and export control regimes in other countries, such as the European Union regulation establishing a framework for screening foreign direct investment in Europe to address security concerns, and German legislation enlarging the range of transactions subject to national security review.

Conclusion

With the propagation of far-reaching requirements and a heated political environment, gone (at least for now) are the days in which a company can safely make categorical conclusions that a given line of business is unaffected by this or that regulatory regime. Some of the recent changes are clearly aimed at China but also reach other foreign actors and US businesses dealing with them. Some are most directly applicable to defense contractors, but also reach deeply into commercial supply chains. In addition to problems of legal compliance, enforcement, and sanctions, there are significant implications for diligence, valuation, and regulatory clearance in

M&A transactions, personal and corporate reputations at risk in Congressional investigations, and issues of corporate governance. While some of the current uncertainty will abate over time (with, for example, the promulgation of implementing regulations), we anticipate no appreciable lessening of public attention to these issues and government enforcement interest in the foreseeable future.

American companies (and other businesses subject to US jurisdiction) should take a fresh, hard look at both their compliance and diligence functions and their dealings with or possibly implicating China (and other foreign actors) – through each of these lenses and as a whole – to identify legal and political risks that simply did not exist before or have been substantially heightened by these recent changes and growing animus towards China.

For more information and guidance on how to address these potentials risks, please contact:

Jamie S. Gorelick
Partner
Chair, Regulatory and Government Affairs Department
Co-Chair, Crisis Management and Strategic Response Group
Washington, DC
+ 1 202 663 6500
Jamie.Gorelick@wilmerhale.com

Stephen W. Preston
Partner
Chair, Defense, National Security and Government Contracts Practice
Washington, DC
+ 1 202 663 6900
Stephen.Preston@wilmerhale.com