David R. Hanke
Visiting Fellow, National Security Institute (NSI)
at George Mason University's Antonin Scalia Law School*

Testimony before the
U.S.-China Economic and Security Review Commission

Hearing on U.S.-China Relations in 2021: Emerging Risks
Panel III: Assessing Export Controls and Foreign Investment Review

Wednesday, September 8, 2021

Chairman Bartholomew, Vice-Chairman Dr. Cleveland, hearing Co-Chair Commissioner Glas, and all Commissioners, thank you for inviting me to participate in today's hearing. I am honored to appear before this Commission as it examines some of the most critical national and economic security issues of our time. And it is always a pleasure to be back in my old stomping grounds on Capitol Hill, where I spent almost a dozen years of my career serving as a staffer.

Professional Background

From August 2007 through January 2019, I worked here in the Senate, first as a policy staffer and counsel to Sen. John Cornyn (Texas) and later as a Professional Staff Member on the Senate Select Committee on Intelligence. Senator Cornyn was the author and sponsor of the *Foreign Investment Risk Review Modernization Act (FIRRMA)*, and I had the distinct honor of working for him on the staff-level drafting and shepherding of this legislation.

I concluded my government service in January 2019 and have been in the private practice of law since then. Today, my client work is centered on two main areas. First, I advise and represent clients on regulatory matters involving foreign investment screening and the Committee on Foreign Investment in the United States (CFIUS), which includes working with both investors and target companies on various types of transactions, including mergers and acquisitions, venture capital investments, and private equity transactions. Second, I advise and represent clients on policy matters involving national security, strategic technologies, and U.S.-China competition. In addition, I am a Visiting Fellow with the National Security Institute, which affords me the chance to stay involved in policy discussions such as this one.

Today, I intend to focus my testimony mainly on foreign investment screening by CFIUS, *FIRRMA*, and closely related topics, leaving the bulk of the discussion on the finer points of export control policies and regulations to my co-panelists, who fortunately are experts in that area.

FIRRMA Origins and Context

In the fall of 2016, Senator Cornyn assigned me the task of studying the existing CFIUS process and rules and identifying any jurisdictional gaps or shortcomings, as well as recommending ways

*The views and opinions expressed in this testimony are mine only and do not represent the views of the National Security Institute, my law firm or its clients, or my former employers.

by which the overall system could be strengthened and modernized through legislation. His concern was both serious and timely, animated by the gathering national security threat posed by China and its acquisition of technology by any means possible. Sen. Cornyn's work and leadership on this initiative was groundbreaking in a number of ways, both specifically on CFIUS modernization and also more generally on evolving U.S. policy towards China. And his bipartisan effort set off a cascade of China-focused legislation on Capitol Hill.

Nearly two years after Senator Cornyn launched the *FIRRMA* initiative, this legislation was enacted as part of the *Fiscal Year 2019 John S. McCain National Defense Authorization Act (FY19 NDAA)*, proving that Congress can still drive major policy reforms with broad bipartisan support and tackle complex issues, including at the tricky intersection of national security and economics. While the executive branch did not initially embrace *FIRRMA* – either in the final months of the Obama Administration or in the first months of the Trump Administration – Senator Cornyn successfully persuaded then-Treasury Secretary Steven Mnuchin (as the CFIUS chair) and other key members of then-President Trump's cabinet to support his effort and help ensure the bill was properly balanced.

While Senator Cornyn drove the process and built a powerful bipartisan coalition of partners and supporters to get *FIRRMA* enacted, this legislation would never have become a reality without the help and support of indispensable players such as the Treasury Department and other CFIUS member agencies. Key congressional partners included then-Congressmen Robert Pittenger (North Carolina) and Denny Heck (Washington), who introduced the *FIRRMA* House companion bill and led the effort in their chamber, and Senator Dianne Feinstein (California), *FIRRMA*'s lead Democrat cosponsor in the Senate. The U.S. business community – led by the U.S. Chamber of Commerce, National Association of Manufacturers, and Information Technology Industry Council – as well as other leading business organizations also supported the final version of *FIRRMA*, in part because it was paired with the *Export Control Reform Act of 2018 (ECRA*), which I will return to shortly.

FIRRMA is widely considered to be the most sweeping overhaul of the CFIUS process in its 46-year history. The legislation was informed by hundreds of meetings and calls with stakeholders in the CFIUS process, including past and current CFIUS officials at most of the nine CFIUS member agencies, CFIUS practitioners, investor groups, U.S. companies of all sizes, foreign governments, trade associations, and think tanks. Those sessions and other research led us to several important conclusions.

First, the national security landscape had evolved, and CFIUS's legacy authorities were outdated and inadequate. China had "weaponized" investment and was using it to meet strategic government objectives. It had identified gaps in both CFIUS's jurisdiction and our export control rules and was exploiting them in order to vacuum up U.S. technology and know-how. The old CFIUS jurisdiction had been relatively narrow and, as a result, unable to address many modern-day national security threats from foreign investment. And the existing dual-use export control system had some inherent weaknesses, such as preventing the overseas transfer of U.S. know-how and keeping pace with the rapid evolution of technology.

Second, in the modern national security landscape, technologies beyond the Commerce Control List and the U.S. Munitions List were becoming increasingly important to our long-term national security. Therefore, transactions involving two particular areas needed more focus from CFIUS: (a) mature, well-understood technologies that had already been downgraded by the export control system as less sensitive, but for which the U.S. business still possessed substantial know-how with national security importance (these types of technologies were later captured in the statutory

term “foundational technologies”); and (b) cutting-edge technologies developed by startups and other small companies, which in the context of long-term national security had become just as important as large defense contractors (these types of technologies were later captured in the statutory term “emerging technologies”).

Third, driven mainly by Chinese transactions, CFIUS’s case volume had increased substantially, even before any jurisdictional expansion. CFIUS simply needed to become more efficient, and it needed more personnel and other resources.

Legislative Intent Behind *FIRRMA*

At its core, *FIRRMA* was about two things: China and technology. While CFIUS also routinely scrutinizes transactions involving other areas – such as infrastructure, data, and real estate – technology was the area in which China had been doing the greatest damage to U.S. national security in recent years. To understand legislative intent, there is no better source than the legislative history and the actual words of a bill’s author. On January 18, 2018, Senator John Cornyn described the challenge in testimony before the Senate Committee on Banking, Housing, and Urban Affairs at a hearing entitled, “CFIUS Reform: Examining the Essential Elements.” Senator Cornyn stated:

> It’s not just that China poses a threat, though, it’s that the *kind of threat* is unlike anything the U.S. has ever before faced – a powerful economy with coercive, state-driven industrial policies that distort and undermine the free market, married up with an aggressive military modernization and the intent to dominate its own region and potentially beyond. To close the technology gap with the U.S. and leap-frog ahead of us, China uses both legal and illegal means. One of these tools is investment, which China has weaponized in order to vacuum up U.S. industrial capabilities from American companies that focus on dual-use technologies. China seeks to turn our own technology and know-how against us in an effort to erase our national security advantage.

Two Main Gaps

Therefore, first and foremost, *FIRRMA* aimed to plug two gaps in the jurisdiction of CFIUS related to technology deals. The first of these gaps was technology joint ventures based overseas, primarily in China. To close this gap, the original *FIRRMA* bill, as introduced on November 8, 2017, sought to give CFIUS jurisdiction over transactions through which a foreign joint venture partner could conduct a de-facto acquisition of an industrial capability embodied in the U.S. business. With these deals, a central concern for Congress was the transfer of know-how related to technologies that the Commerce Department had de-controlled, such as older generations of semiconductors.

There was a clear inconsistency between the policies underlying CFIUS’s investment screening and the Commerce Department’s regulation of outbound flows of technology and know-how. At the January 18, 2018, hearing of the Banking Committee, Senator Cornyn explained:

> The rationale behind *FIRRMA* is simple: CFIUS should be able to review transactions that have, in effect, the same national security consequences as a traditional acquisition of a U.S. company or a piece of it. Foreign investors should not be able to circumvent CFIUS and get via the “back door” something they cannot get through the “front door.” To take advantage of these gaps and circumvent CFIUS review, China pressures U.S. companies

> into business arrangements such as joint ventures, coercing them into sharing their technology and know-how, enabling Chinese companies to acquire high-tech U.S. industrial capabilities and then replicate them on Chinese soil.

To address this challenge, a narrow provision was drafted in close coordination with the Treasury Department, and the new jurisdiction would have only applied where both intellectual property and know-how related to "critical technology" (as defined elsewhere in *FIRRMA*) were transferred through a collaborative arrangement between the foreign party and the U.S. business. Some in industry – especially U.S. technology and advanced manufacturing companies with large China-based operations that encompass the sharing of technology and know-how through joint ventures or related structures – aggressively opposed this narrow construct and generated enough opposition that the entire provision had to be dropped. Instead, a compromise approach was adopted, relying entirely on the export control system to address the problem. I will explain more on that below.

The second of these gaps was minority-position investments, typically involving Chinese-backed venture capital investors. These are investments that fall short of giving investors "control" of the target company, but still afford them certain rights or access that could have national security ramifications. Some deals involving foreign-controlled private equity funds and other types of investors can also fall into this category. Again at the January 18, 2018, hearing of the Banking Committee, Senator Cornyn observed that:

> China has also been able to exploit minority-position investments in early-stage technology companies in places like Silicon Valley, California, or the "Silicon Hills" in Central Texas to gain access to intellectual property (IP), trade secrets, and key personnel. The Chinese have figured out which dual-use emerging technologies are still in the cradle, so to speak, and not yet subject to export controls.

CFIUS 2.0 and the Successful Expansion of CFIUS Jurisdiction

The vast majority of *FIRRMA*'s substantive provisions survived Senate-House conference negotiations intact, though House negotiators successfully pushed for significant changes to the text in at least one key area, which I will describe below. As enacted, *FIRRMA* expanded CFIUS jurisdiction in a highly targeted fashion. It was narrowly tailored to address situations with heightened national security risks, aiming to avoid unnecessarily chilling foreign investment.

The term "CFIUS 2.0" has been adopted by some, including then-Commander of the U.S. Pacific Command, Admiral (Ret.) Harry Harris, to refer to the modernized CFIUS process under *FIRRMA*. In CFIUS 2.0, the most important new area of CFIUS jurisdiction is the previously mentioned minority-position investments. These are non-controlling, non-passive investments ("covered investments" in the parlance of the main CFIUS regulation) involving U.S. critical technologies, U.S. critical infrastructure, or the sensitive personal data of U.S. citizens. CFIUS has jurisdiction over such investments only in certain circumstances. First, the U.S. target company has to be engaged in at least one specific activity on a list, such as producing, designing, testing, manufacturing, fabricating, or developing a "critical technology"; owning, operating, manufacturing, or servicing a certain U.S. critical infrastructure system or asset; or maintaining or collecting certain types of sensitive personal data of US citizens. Second, the investment has to feature at least one of three specific non-passive triggering rights, which include (a) access to "material nonpublic technical information" in possession of the U.S. target company; (b) membership or observer rights on the company's board of directors (or the right to appoint such

individuals); or (c) involvement (other than voting of shares) in substantive decisionmaking of the target company regarding such technology, infrastructure, or data.

CFIUS jurisdiction was expanded by *FIRRMA* in two additional ways, though these are less relevant to today's topics. These are transactions that are "designed or intended to evade or circumvent" the jurisdiction of CFIUS, and transactions involving stand-alone real estate near sensitive locations (under a separate regulation, 31 C.F.R. Part 802).

Compromises in *FIRRMA* on the Way to Enactment

As mentioned, during congressional consideration of *FIRRMA*, some U.S. companies with major business interests in China aggressively opposed the specific provision that would have given CFIUS jurisdiction over certain technology joint ventures based overseas, arguing in favor of the status-quo hands-off approach taken by the U.S. Government to date on these particular types of joint ventures. As a result, that provision was stripped from *FIRRMA*, limiting CFIUS's jurisdiction to inbound transactions only, and a compromise provision was drafted with the help of the executive branch and substituted into *FIRRMA*. Opponents of *FIRRMA*'s original construct were much more comfortable with maintaining the locus of any outbound controls and critical technology definitions at the Commerce Department, which had been generally far less concerned about technology and know-how flows to China.

On paper, Section 1758 created a new export control framework for "emerging and foundational technologies." During *FY19 NDAA* conference negotiations on *FIRRMA* and *ECRA*, this provision migrated from *FIRRMA* over to *ECRA* and was then enacted as *FY19 NDAA* Section 1758 (codified at 50 USC § 4817). This provision was intended to address some of the shortcomings that Congress had identified in the existing dual-use export control system, such as its struggle to prevent the overseas transfer of important U.S. industrial capabilities and its inability to keep pace with the rapid evolution of technology. With this provision, Congress handed the Commerce Department a statutory mandate to lead an interagency process for identifying and unilaterally controlling emerging and foundational technologies "that are essential to the national security of the United States." This provision, coupled with one in *FIRRMA*, also created stronger connective tissue between the CFIUS and export control processes. CFIUS's previous regulatory definition of "critical technologies" already included the U.S. Munitions List and key portions of the Commerce Control List. *FIRRMA* expanded this definition by adding the concept of "emerging and foundational technologies." The provision requires unilateral controls initially for each technology, limited to a three-year period during which BIS must pursue multilateral controls for that technology.

The mandate for controls on foundational technologies was specifically intended to address the national security concerns regarding technology joint ventures based in China, such as those in the field of semiconductors, through which important U.S. industrial capabilities were being steadily acquired by Chinese entities. The authors of *FIRRMA* had originally intended for CFIUS to regulate these de-facto acquisitions of industrial capabilities, but instead the job would now remain with the export control system under the mandate of Section 1758.

Although the mandate for controls on emerging technologies is intertwined with the mandate on foundational technologies, it serves a somewhat different purpose. It was intended to play a distinct jurisdictional role for CFIUS. As mentioned above, in CFIUS 2.0, jurisdiction over non-controlling, non-passive investments in the technology sector depends explicitly on whether the U.S. target company works with a technology that meets the definition of "critical technology."

Without a critical technology, CFIUS has no jurisdiction whatsoever over these types of transactions.

When Congress expanded CFIUS jurisdiction to cover certain minority-position investments, the problem it was focused on was China's growing participation in venture capital deals involving early-stage technology companies. In January 2018, the Department of Defense's Defense Innovation Unit Experimental (DIUx) published a timely report, entitled "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation," which examined this very issue. Among its findings were the following: (1) Chinese participation in venture-backed startups had grown rapidly in recent years, reaching a record level of 10-16% of all venture deals from 2015 to 2017; and (2) China was investing in key technologies such as artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics, blockchain technology, and gene editing – many of which are of great interest to the U.S. military.

This eye-opening DoD analysis became one of the analytical underpinnings of the *FIRRMA* initiative. The members of Congress who drove *FIRRMA* recognized the growing national security importance of startups and other small companies and the types of technologies that they were developing, which by their very nature were "emerging" technologies. However, the proper way to determine which technologies were important or sensitive enough to warrant a CFIUS review of related investment deals was a matter of some disagreement between the Senate and the House.

The version of *FIRRMA* passed by the Senate on June 18, 2018, as part of the *FY19 NDAA* (which was identical to the version reported out by the Senate Banking Committee) would have codified in statute CFIUS's then-existing regulatory definition of "critical technologies." However, importantly, it would also have created a new prong of "critical technologies" with jurisdictional implications for CFIUS. Under this expanded definition, CFIUS would have been granted the authority to decide for itself, as an interagency committee, which kinds of "technology, components, or technology items" were "essential to national security" and thus might warrant CFIUS review of a related investment, beyond those technologies that already met the definition of critical technology per controls issued by the Commerce Department or State Department, for example.

As referenced above, during Senate-House conference negotiations, there was a burst of last-minute lobbying from companies aiming to expand their operations in and sharing of technology and know-how with China. This succeeded in pressuring House negotiators into taking the position that the key function of determining a particular technology's sensitivity or importance should remain beyond the reach of CFIUS. House negotiators successfully pushed to eliminate that authority for CFIUS and to instead hand unilateral authority to the Commerce Department to decide what additional dual-use technologies might be "essential to the national security of the United States" (as outlined above) and thus appropriate for CFIUS to prioritize in its investment screening role. As a result of that 11th-hour change to *FIRRMA*, today CFIUS has no ability whatsoever, as an interagency committee, to decide which technologies should be labeled "critical technologies" for the purpose of setting the proper scope of its own jurisdiction.

Assessing *FIRRMA* Implementation To Date – Process and Substance

Of course, no legislation is perfect – and *FIRRMA* is no exception – but even a very good piece of legislation must be properly implemented by the executive branch in order to meet

congressional intent. To assess the implementation of *FIRRMA*, it is most useful to look separately at what was done on the process side of CFIUS and what was done substantively.

Assessing the Process

On process, the Treasury Department was always the key player in *FIRRMA* implementation and, thankfully, its portion of implementation was completed on time prior to the end of the Trump Administration. There is a lot to celebrate in *FIRRMA*'s implementation on the process side of things. For example, Treasury launched the "Critical Technology Pilot Program" within 60 days of *FIRRMA*'s enactment, which was impressive speed, especially by government standards. More importantly, the permanent CFIUS regulations under 31 C.F.R. Part 800 and 31 C.F.R. Part 802 were thoughtful, carefully written, closely tailored to the problem set, and timely published. CFIUS did an admirable job of maximizing certainty and predictability for transaction parties wherever possible.

Of course, one of the central goals of *FIRRMA* was to make the CFIUS process more efficient. That necessitated, among other things, providing CFIUS with an overdue boost in resources to hire additional personnel and improve its infrastructure to prepare for a heavier workload per the jurisdictional expansion. That boost was funded in part by successful implementation of new authority for CFIUS to collect filing fees, which *FIRRMA* had granted. Among the additional personnel hired by CFIUS was the group referred to in a January 2021 *Wall Street Journal* article as a "buzzy SWAT team," whose mission is to identify transactions that were never filed for CFIUS review but nonetheless could pose a national security risk. That important work had been mandated by *FIRRMA* in *FY19 NDAA* Section 1710, which required CFIUS to establish a process for identifying these "non-notified and non-declared" deals.

FIRRMA's greatest process improvement was arguably the creation of a new short-form CFIUS filing called a "declaration," which is a streamlined, five-page filing that depending on the situation can be either mandatory or voluntary (for more benign transactions). In early drafts of *FIRRMA*, these short-form filings were strictly voluntary, intended to give parties an option for fast-track review and potential CFIUS clearance. Later, the concept of mandating declarations in certain situations was proposed and incorporated into the legislation. Treasury's implementation of the declaration concept has been excellent, and the use of these filings is already expanding as transaction parties and CFIUS practitioners gain a better understanding of where declarations are most appropriate and useful.

On mandatory declarations, the CFIUS member agencies (including the Commerce Department and the State Department, the key agencies on export controls) worked together to craft a clear rule, which was issued on September 15, 2020. The new rule ties CFIUS mandatory filing requirements to the question of whether a U.S. Government export license or other authorization would hypothetically be required to transfer the U.S. target company's critical technology to either the relevant foreign investor or parties holding significant interest in the foreign investor.

Treasury also utilized *FIRRMA*'s "country specification" authority (in *FY19 NDAA* Section 1703) to create a positive list of "excepted foreign states," allowing "excepted investors" from those nations to self-classify as meeting the full requirements to be exempt from two of the new areas of CFIUS jurisdiction. While only three nations – the United Kingdom, Canada, and Australia – qualify at the moment, the list is likely to be broadened in the coming years to include additional allied nations and narrow the pool of covered transactions, allowing CFIUS to deprioritize benign transactions. The employment of this list also has the effect of creating an important incentive for

foreign countries to set up or enhance their own foreign investment screening process, an important development that I will discuss in more detail below.

Additional efficiencies in the CFIUS review process have come as a result of the fact that, in *FIRRMA*, Congress lengthened the review period (the initial phase of the CFIUS process) by 15 days, making it 45 days instead of the previous 30 days. This has allowed CFIUS to complete more reviews during this first phase, without needing to cross into the second 45-day period (the investigation). It has also reduced the pressure on transaction parties to potentially have to withdraw and refile with CFIUS to restart "the clock" during more complex reviews.

One of the most important effects of *FIRRMA* stems from the provision in *FY19 NDAA* Sec. 1713 on establishment of a formal process for CFIUS engagement with allied and partner nations, intended to "facilitate the harmonization of action with respect to trends in investment and technology," provide for information-sharing regarding "specific technologies and entities acquiring such technologies," and "include consultations and meetings with representatives of the governments of such countries on a recurring basis." The Treasury Department took this task seriously and dedicated the time and energy necessary to get it right. In July, Tom Feddo, the former Treasury Assistant Secretary who oversaw the CFIUS process for the Trump Administration, posted some insightful statistics on this:

> With *FIRRMA*'s enactment Treasury expanded its CFIUS staff over five-fold and assembled a team dedicated to building international relationships and cooperation. It collaborated at length with the Five Eyes, Japan, and the EU, and by mid-2020, Treasury had engaged with "the G7 Finance Ministers, Australia, Canada, and the United Kingdom," "interacted over 260 times with nearly 50 counterpart countries or multilateral entities," and was leveraging "the rising tide of growing global interest in establishing and reforming investment review regimes." Treasury advised several allies on these reforms, and emphasized to others the critical need to establish mechanisms to protect cutting-edge technology from misappropriation.

Since *FIRRMA*'s enactment, many U.S. allies and partner nations have taken major steps to create or expand their own inbound investment screening mechanisms, and this is one of the most important legacies of *FIRRMA*. Making the screening of foreign investment more consistent across allied and partner nations not only more effectively addresses the potential risks to the national security of the United States and our allies and partners; it also helps maintain a more level playing field for companies whose global competitors might otherwise benefit from a proposed investment that is problematic from a national security standpoint.

The Biden Administration is continuing CFIUS's important multilateral engagement as the new E.U.-U.S. Trade and Technology Council gets off the ground, with cooperation in investment screening reportedly a major theme of the upcoming meeting.

Assessing the Substance

On the substantive side of *FIRRMA* implementation, the good news is that CFIUS's new jurisdiction over "non-controlling investments" in the areas of sensitive personal data and critical infrastructure is in great shape. The regulations did a fine job of employing CFIUS's newfound authority and addressing the national security risks, while also drawing clear lines for transaction parties.

However, on the technology-centric areas of CFIUS's expanded jurisdiction and the Commerce Department's mandate to control emerging and foundational technologies under Section 1758, the question must be asked as to whether the relevant U.S. Government agencies have closed the two gaps that Congress identified, implementing *FIRRMA* and *ECRA* as envisioned by Congress. First, on the challenge of overseas-based joint ventures involving foundational technologies and the transfer of related know-how, implementation of this portion of *ECRA* never got off the ground during the Trump Administration and unfortunately appears to remain stalled in the Biden Administration. Second, on the issue of Chinese-backed venture capital investments involving emerging technologies, implementation of these portions of *FIRRMA* and *ECRA* has not successfully closed the gap that Congress identified. Unfortunately, the last-minute changes that were made during the Senate-House conference negotiations in an attempt to water down *FIRRMA* have made CFIUS totally dependent on the Commerce Department to determine CFIUS's jurisdiction over these types of transactions, as explained above.

The Commerce Department's process for identifying and controlling emerging and foundational technologies has been highly deliberative, with a great deal of input having been solicited from and provided by industry and academia, including through the notice-and-comment process. It has also been incredibly slow. With both emerging technologies and foundational technologies, the Commerce Department is taking a two-step process: issue an Advance Notice of Proposed Rulemaking (ANPRM), then publish individual controls as they become ready (not all of them simultaneously). As Section 1758 requires, it will be an "ongoing" process, not a one-time exercise.

On foundational technologies, the Commerce Department published an ANPRM on August 27, 2020, soliciting public comment on potential approaches for identifying these technologies. It received several dozen public comments from industry and academia, but it has yet to impose any foundational technology controls or announce additional steps being taken to meet its mandate.

On emerging technologies, the Commerce Department issued an ANPRM on November 19, 2018, asking for input on how to identify and control these technologies. It listed 14 broad categories of "representational technologies" to give commenters some idea of what was under consideration. Over 200 comments were submitted to the Commerce Department. Since then, the Commerce Department appears to have issued one unilateral emerging technology control last January on "software specially designed to automate the analysis of geospatial imagery." In addition, according to its 2020 annual report, the Commerce Department has imposed controls on 36 other emerging technologies pursuant to *ECRA*, most of them multilateral controls through the Wassenaar process or the Australia Group.

In the export control context, multilateral and plurilateral controls are certainly preferable to unilateral controls in most ways, especially because they help maintain a level playing field for U.S. companies. However, multilateral controls suffer from one major disadvantage as compared to unilateral controls, and that is the amount of time it can take to impose them. In the investment screening context, relying on slow-moving multilateral controls to determine the jurisdiction of CFIUS over non-controlling, non-passive investments is highly problematic given the consensus nature and lumbering pace of action in organizations like the 42-member-country Wassenaar Arrangement. One must keep in mind that it can take two to three years, from start to finish, to actually impose a multilateral control through Wassenaar. In contrast, the technologies being developed by dynamic U.S. startups typically move and change much more rapidly than that, and venture capital investments (including those involving foreign investors) in these companies often happen quite quickly.

Unfortunately, the implementation of the emerging technology controls under Section 1758 has been fundamentally incompatible with a central task that Congress assigned to CFIUS when it enacted *FIRRMA*, namely to address Chinese-backed venture capital investments involving emerging technologies. CFIUS simply cannot fulfill its expanded national security role in the new era of strategic competition if it has to wait years to gain jurisdiction over foreign investments in U.S. companies that are developing the most vital technologies of the future. Relying on Wassenaar to help determine the jurisdiction of CFIUS is a major policy mistake, but that is the current state of play with the implementation of emerging technology controls under *FIRRMA*.

As things stand, for example, a state-owned enterprise (SOE) from a foreign adversary nation (e.g., China or Russia) could invest in a U.S. company that is successfully developing leading-edge quantum computing or machine learning technology in a place like Silicon Valley. The SOE could take a 10% voting interest in the company, a seat on its board of directors, and potentially other significant investor rights – and CFIUS would have no ability to even review the deal, so long as the U.S. Government has not yet imposed export controls on that specific technology. (Of course, regarding the foreign investor, entities that are subject to blocking sanctions by Treasury's Office of Foreign Assets Control would have restrictions.) This is a worst-case scenario that may be unlikely, yet it illustrates what is currently possible. The implications for U.S. national security are significant, and there are better ways to make technology determinations for the purpose of setting the proper scope of jurisdiction for CFIUS.

As this Commission noted in its June 1, 2021, report, "Unfinished Business: Export Control and Foreign Investment Reforms," authored by Policy Analyst Emma Rafaelof:

> Defining a list of "emerging and foundational" technologies is a crucial part of implementing the *Foreign Investment Risk Review Modernization Act (FIRRMA)* and the *Export Control Reform Act (ECRA).* Since these acts became law in 2018, there has been a significant delay in forming this list along with a lack of clarity on the process and methodology.
> . . .
> Lack of clarity from the Department of Commerce on what constitutes emerging and foundational technologies impedes the ability of the Committee on Foreign Investment in the United States (CFIUS) to fulfill its responsibilities. The years-long delay in developing these definitions may exacerbate national security risks.

A January 15, 2021, report by Ian Fergusson and Karen Sutter of the Congressional Research Service, entitled "U.S. Export Control Reforms and China: Issues for Congress," echoes these conclusions:

> The lack of new technology identification arguably impedes not only *ECRA* implementation but also congressional reforms that expanded the authority of the Committee on Foreign Investment in the United States (CFIUS) to review Chinese and other foreign investments in critical and emerging technologies below a traditional threshold of foreign control. CFIUS can only act against non-controlling foreign investments if the technologies involved in the transaction are controlled.

CFIUS, through no fault of its own, has likely been unable to review a single non-controlling, non-passive investment involving emerging or foundational technologies controlled under Section 1758 during the three years since Congress expanded CFIUS's jurisdiction through *FIRRMA*. Today, most venture capital deals in the technology space likely remain beyond the reach of CFIUS, typically because the technology does not meet the definition of "critical technology."

While the issuance of lists of emerging technologies and foundational technologies was what the congressional authors of *FIRRMA* envisioned, the Commerce Department has made clear that it does not plan to do that. Instead, it intends to issue very narrow, precise controls on specific items, software, and technologies, just as it does under the legacy export control system. Unfortunately, *FIRRMA* can never have its true intended effect until either the process for controlling emerging technologies and foundational technologies is carried out as Congress envisioned or Congress enacts a better approach.

Implementation Status for Other Provisions of *ECRA*

Beyond its CFIUS implications, *ECRA* itself is a solid piece of legislation, but more than three years after its enactment the implementation status for other parts of it remains in question. One example is *FY19 NDAA* Section 1759 (codified at 50 USC § 4818), which requires the Commerce Department to work jointly with the Departments of Defense, State, and Energy to conduct a review of license requirements for exports, reexports, or in-country transfers of items to China and other arms-embargoed countries. The deadline for compliance was May 2019.

It is also unclear whether an important *ECRA* provision that aimed to improve congressional oversight of the export licensing process has been implemented. In *FY19 NDAA* Section 1761, subparagraph (h) contains the following requirement:

> Any information obtained at any time under any provision of the Export Administration Act of 1979 (50 U.S.C. 4601 et seq.) (as in effect on the day before the date of the enactment of this Act and as continued in effect pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.)), the Export Administration Regulations, or under this part, including any report or license application required under any such provision, shall be made available to a committee or subcommittee of Congress of appropriate jurisdiction, upon the request of the chairman or ranking minority member of such committee or subcommittee.

The scope and scale of dual-use technology transfer to China that has occurred over the past two decades (both voluntarily and involuntarily) is staggering, but Congress has very limited visibility into the relevant export licensing decisions. Improving transparency in this area would enable better congressional oversight. It would also better equip any administration to draw lines at the appropriate places to protect U.S. competitiveness and innovation. If the U.S. Government does not have detailed information on the technology and know-how that is leaving our shores for China, it will invariably draw lines in the wrong place when it comes to regulating such flows.

Congress already conducts this type of oversight in the CFIUS process and other areas of export controls. For example, after CFIUS case decisions, notification is required by statute to be sent to Congress, which often takes advantage of the opportunity to receive briefings from CFIUS on the details of the transaction and its disposition. Similarly, for export control licensing decisions that fall under the purview of the State Department, my understanding is that State has a regular process of briefing its congressional oversight committees. Congress may wish to establish a similar process and flow of information with the Commerce Department.

Policy Recommendations

Tinkering with *FIRRMA*

Closing the two gaps that Congress identified at the outset of *FIRRMA*'s development would likely require both legislative and administrative reforms. With Section 1758, Congress created a flawed construct for the identification and control of emerging and foundational technologies, though both Congress and the Commerce Department have an opportunity to take meaningful steps to remedy the problem. Unlike when Congress enacted *FIRRMA* and *ECRA*, sweeping changes to the process are not required. Instead, some targeted "tinkering" with the current rules would go a long way, though many stakeholders would certainly be leery of the idea of revisiting CFIUS reform just three years after *FIRRMA*.

On the challenge of non-controlling, non-passive investments involving emerging technologies, legislation would likely be required to repair the broken mechanism that is currently used to define the jurisdiction of CFIUS in this area. The cleanest and simplest approach may be to loosen the jurisdictional linkage between *FIRRMA* and *ECRA* in this area, reverting to an approach similar to the one taken in an earlier version of *FIRRMA* that was passed by the Senate as part of the *FY19 NDAA*, as described above. That would give CFIUS the flexibility to decide for itself – as a powerful cabinet-level interagency committee with deep expertise in the full spectrum of national security issues – which technologies beyond the existing list of critical technologies are indeed essential to national security and thus might warrant CFIUS review of a related investment. CFIUS could use that authority to create and employ categories of technology for jurisdictional purposes, in a way that is much more useful and relevant than relying on ultra-narrow export controls buried in the nooks and crannies of the Commerce Control List.

There are compelling reasons to revisit these particular aspects of *FIRRMA* and *ECRA*. Many of the potential national security risks involved in CFIUS's screening of non-controlling, non-passive foreign investments in U.S. target companies are uniquely different from the risks that the export control rules aim to address. In considering whether to allow a specific foreign entity to invest in a particular U.S. company, CFIUS has to worry about the likelihood of the foreign party gaining less tangible things, such as insights into the company, its business practices, its past experience with and future plans for research and development, and its overall sector; connections with key company personnel and important suppliers, partners, and customers; and leverage regarding the company and the direction of its future technology pursuits. These present questions related more closely to economic espionage than to technology transfer, for example. On the investment screening side, there are a set of risks that are simply different from those on the export control side.

Members of Congress are already proposing reforms to Section 1758 and the CFIUS definition of critical technologies. Senator Thom Tillis (North Carolina) introduced legislation last year that would make a targeted change to authorize the Treasury Department (as chair of CFIUS) to designate emerging and foundational technology for CFIUS-only purposes (with no export control implications whatsoever), but only if one other voting member of CFIUS agreed.

The House Republican China Task Force report from September 2020 has likewise weighed in on the importance of full implementation of the Section 1758 mandate and has recommended looking at transferring the function to a different agency altogether: "If DoC's Bureau of Industry and Security is unable to make substantial and measurable progress in fulfilling this requirement, Congress should consider whether a different bureau or department can better fulfill this statutory obligation."

On the specific challenge of overseas-based joint ventures involving foundational technologies and the transfer of related know-how, the gap could still be closed by the Commerce Department administratively without the need for legislation action. The coming months may bring important developments in this area. However, there is mounting frustration on Capitol Hill about this particular issue, as well as on much broader ones involving China's desire to dominate and leverage global supply chains in areas such as personal protective equipment and pharmaceuticals.

New Proposals to Screen Outbound Investments

The National Critical Capabilities Defense Act, bipartisan legislation authored by Senators Bob Casey (Pennsylvania) and John Cornyn (Texas), is under active consideration now on Capitol Hill and with certain improvements would be an appropriate reform. This bill would create an interagency federal process, led by the U.S. Trade Representative (USTR), to screen outbound U.S. investments and the "offshoring of critical capacities and supply chains to foreign adversaries, like China and Russia . . . ."

The Biden Administration, at very senior levels, is also thinking about this set of problems and has expressed concern. President Biden's National Security Advisor Jake Sullivan recently said

> And then of course we have to work closely and especially closely with our partners on our export control and investment screening regimes to make sure they are postured for intense technology competition. In this regard, we are also looking at the impact of outbound U.S. investment flows that could circumvent the spirit of export controls or otherwise enhance the technological capacity of our competitors in ways that harm our national security.

Other executive-branch developments in the area of overseas-based joint ventures, potentially involving foundational technologies, are also worth noting. Recently, the White House and the USTR announced cooperative frameworks with both the European Union and the United Kingdom pertaining to civil aircraft. The Biden Administration is apparently working with both of them on "common approaches and enhanced cooperation regarding the screening of new outward investments in joint ventures and production facilities in non-market economies."

There seems to be an increasing alignment of interests and objectives between key members of Congress and key players in the Biden Administration in tackling this issue. As such, this may present a unique opportunity to build a carefully calibrated new interagency process, with the Casey-Cornyn legislation as the jumping-off point, setting the bar in the right place on the screening of outbound investments and technology flows. To strike the right balance, the private sector must be part of the thought process and willing to provide Congress and the Biden Administration with substantial input, as occurred during the development of *FIRRMA* and *ECRA*.

Other Potential Improvements to CFIUS

With CFIUS, the challenge remains how to properly address national security risks without overloading the process and "breaking" it. Of course, not all transactions present real national security risks, and therefore not all warrant the same level of scrutiny and commitment of CFIUS's time and resources. Focusing the work of CFIUS on transactions with actual national security risks, versus benign transactions, is the key. A particularly effective way to conduct this triage function would be to further differentiate deals based on a foreign investor's home country.

One option would be for CFIUS to tighten the focus of its reviews by employing a negative list of "foreign adversary" countries, much the same way the Commerce Department did with its January 19, 2021, rule on "Securing the Information and Communications Technology and Services Supply Chain." This rule established a screening process for ICTS transactions, focusing only on five specific "foreign adversaries" (China, Russia, Iran, North Korea, and the Maduro regime in Venezuela). CFIUS could certainly emulate such an approach in administratively re-scoping its jurisdiction, where appropriate. In fact, early drafts of *FIRRMA* had proposed utilizing this type of negative list of higher-risk countries to cabin the new areas of CFIUS jurisdiction. At the time, this proposed approach was rejected by the executive branch, though it received strong support from the House and from many key players in industry, including the U.S. Chamber of Commerce. Moreover, the previously mentioned "country specification" authority provided by *FIRRMA* is very broad, and could arguably be employed for this very purpose.

CFIUS remains a largely voluntary process, and that should continue to be the case. Mandatory filing requirements should be highly targeted and put in place only where truly necessary, because the filing of either full-length CFIUS notices or short-form CFIUS declarations necessitates CFIUS spending time and resources scrutinizing the transaction in response. However, creating a new, purely informational ultra-light filing (perhaps called a CFIUS "disclosure") could be a value-added tool for CFIUS. In the paper age, such a filing might have been referred to as a "postcard" filing. Today, it could be a very basic online filing that imposes only a minimal burden on transaction parties. It could be used by CFIUS to gain more visibility into deals that otherwise have no mandatory declaration requirement, but have a discernable nexus to a foreign adversary nation and involve specific sectors and areas that are of high priority to that nation, such as "Made in China 2025," China's Five-Year Plans, and other industrial policy.

In general, congressional oversight hearings on the implementation of *FIRRMA* and *ECRA* are long overdue. With implementation still incomplete, the onus is on Congress to assess the causal factors and decide on appropriate actions. Additionally, as CFIUS assesses national security risks on transactions in the pandemic era, Congress should ensure the process is taking into account the overall market share of the U.S. target company's general technology that is already held by any foreign country that is involved with the transaction.

Miscellaneous Reforms

Recently, Congress has also been considering reforms regarding the "Operating Committee," a key part of the interagency dispute resolution process for export licensing decisions. An amendment on this was recently proposed by Congresswoman Claudia Tenney (NY-22) during a markup of the House Foreign Affairs Committee, but it was voted down. The concern from some in Congress has been that, at the Operating Committee, the Commerce Department has the authority to overrule national security concerns raised by the other members – the Departments of Defense, State, and Energy – and grant an export license anyway. This may be a fruitful area for oversight and reform.

Lastly, the U.S. Government needs to improve its toolkit for helping worthy U.S. target companies that may find themselves in the crosshairs of CFIUS and end up having a transaction blocked or a divestment forced. Unfortunately, these companies sometimes have no other available sources of capital for the purpose of competing, expanding, scaling up, pursuing new technologies and product lines, and generally succeeding in the marketplace. It is in the U.S. national security and economic interest to ensure that these types of companies still exist and are thriving five or 10 years from now, and that will necessitate some new and creative approaches. Merely telling companies to avoid Chinese investment and hoping that private investors will save the day is not

going to be an adequate long-term policy in the era of strategic competition. In 2021 and beyond, a strong defense (i.e., CFIUS) must be paired with a good offense – some active mechanism for helping certain companies secure private capital or some type of short-term government support. Of course, the Senate recently passed the *U.S. Innovation and Competition Act (USICA)*, which takes some steps to provide alternative sources of funding, and the House has passed related legislation. This is a decent start, although *USICA*'s initial focus on technology has already been watered down and seems likely to get further diluted as the Senate and the House negotiate over a final version of the legislation. To get these policies right, more congressional attention will likely be needed in the near future.