**Testimony of Sen. John Cornyn**

**U.S. Senate Committee on Banking, Housing, and Urban Affairs**

**“CFIUS Reform: Examining the Essential Elements”**

#### January 18, 2018

**Introduction**

Thank you, Chairman Crapo and Ranking Member Brown, for convening this hearing to consider the proposal that Sen. Feinstein and I have put forward, the Foreign Investment Risk Review Modernization Act (FIRRMA).  I have been honored to collaborate on this legislation with my esteemed colleague, Senator Feinstein, who I serve alongside on both the Judiciary and Intelligence Committees.

We spent many months working on FIRRMA, and we wrestled with some tough issues in the process.  Based in part on the information we are exposed to on the Intelligence Committee, we believe these issues are urgent and complicated ones.  The bill we have put together takes a targeted approach to addressing the problem, while also aiming to not unnecessarily chill foreign direct investment.

Before we get into addressing the merits of the bill, however, I’d like to take a moment to highlight the list of people who have endorsed this legislation. That includes current U.S. national security leaders such as Secretary of Defense James Mattis; Secretary of the Treasury Steven Mnuchin; Attorney General Jeff Sessions; and Admiral Harry Harris, Commander of U.S. Pacific Command.

It includes former U.S. national security leaders such as former Secretaries of Defense Donald Rumsfeld and Bill Perry; former Secretary of Homeland Secretary Michael Chertoff; former Director of National Intelligence and Commander of U.S. Pacific Command, Admiral Dennis Blair; General Mike Hagee, former U.S. Marine Corps Commandant; General Edward Rice, former Vice Commander of Pacific Air Forces and Commander of U.S. Forces in Japan; and General J.D. Thurman, former Commander of U.S. Forces Korea and U.S. Army Forces Command.

The list includes private industry players such as telecommunications giant, Ericsson, Inc.; Oracle Corporation; Trinity Industries; Amsted Rail Company, Inc.; the Greenbrier Companies, the 20 member companies of the American Iron and Steel Institute; and the 260-member Railway Supply Institute. It includes China experts such as Dr. Larry M. Wortzel, a member of the U.S.-China Economic and Security Review Commission.

Mr. Chairman, with your indulgence, I encourage the committee members to review the comments of these supporters, and I ask consent to submit their letters and quotes for the record. I would also ask consent to submit for the record several summary and background documents on FIRRMA.

**Context: China**

The context for this legislation is important and relatively straight forward, and it’s China.  I have always been an ardent supporter of free trade, and I strongly support foreign direct investment in our country, consistent with the protection of our national security. However, the not-always-peaceful rise of China has significantly altered the threat landscape in recent years.

General Joe Dunford, Chairman of the Joint Chiefs of Staff, has said that by 2025, China will pose the greatest threat to U.S. national security of any nation.  And, last summer, CIA Director Mike Pompeo echoed that view, saying that, over the long-term, China represents a graver security risk than even Russia or Iran.

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.

In the modern era, the U.S. Military has always had a decisive technological advantage over our adversaries. This advantage is eroding before our very eyes, in part because some U.S. companies have willingly helped China build industrial capabilities with clear national security applications. It is time to tackle the underyling problems head-on, while there is still time.

If the trend continues for the foreseeable future, what might this mean for our national security? We would potentially have an adversary that can dominate the cyber realm, defeat our space weapons, and control the skies as well or better than the U.S. Military. Just imagine if China’s military was stronger, faster, and more lethal – such that China could unilaterally dictate which ships can transit through critical sea lanes in the Indo-Pacific region. Or, imagine if China could invade its democratic island neighbor Taiwan with impunity. The implications for the U.S. would be profound, both security-wise and economically. That is what the future likely holds, unless we act.

I encourage each member of this committee to get a classified intelligence briefing on these issues. I and my staff would be happy to set those up for you, if helpful.

**Rationale and Key Objectives of FIRRMA**

As it currently stands, the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS) is quite limited; it was designed for the last century, not the present one. China has found gaps in both the existing CFIUS process and the export control system and is exploiting them to the detriment of our national security, aiding its own military modernization and simultaneously weakening our U.S. defense industrial base.  FIRRMA takes a measured and targeted approach to close these gaps, with changes that are laser-focused on national security concerns. Its provisions also reflect the need to preserve as much certainty and predictability for investors as possible.

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.

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.

FIRRMA would expand the jurisdiction of CFIUS to cover some of these technology joint ventures and related arrangements and minority-position investments, as well as certain real estate transactions near military bases.

**China’s Civil-Military Integration Policies**

The problems are compounded by some of China’s carefully constructed policies on civil-military integration, under which China’s military suppliers and their activities are woven right into China’s commercial environment, unlike in our free market economy.  To help modernize its military, China [purposely blurs the lines between military and ostensibly commercial activities,](https://static1.squarespace.com/static/569925bfe0327c837e2e9a94/t/593dad0320099e64e1ca92a5/1497214574912/062017_Pointe+Bello_Military+Civil+Fusion+Report.pdf) combining its defense and civilian industrial bases. As such, U.S. technology and know-how transferred to “private” Chinese companies are likely to contribute directly and materially to China’s military modernization.

Here, our export control system does not address the problem because the diversion of U.S. dual-use technologies is no longer just a risk, but a foregone conclusion.  It is safe to assume that China will divert the fruits of any U.S. company’s cooperation with China to a military end-use.  It would be foolhardy to think these capabilities are not making their way into the hands of the Chinese military.

Further, U.S. companies doing business in China are entirely subject to the whims and dictates of the Chinese Communist Party.  And, there is no real difference between a Chinese state-owned enterprise and a “private” Chinese firm, in terms of the national security risks that exist when a U.S. company partners with one. Rule of law in China is often illusory, and the Chinese Communist Party can easily exercise control over both types of companies, as American Enterprise Institute economist, Derek Scissors, has pointed out.

There are also major concerns regarding U.S. data, especially the personally identifiable information (PII) of U.S. citizens, and export controls do not cover this. The Chinese Communist Party considers data to be a national strategic resource, so China is basically nationalizing all data. Therefore, when U.S. companies are forced to on-shore data into China, it can have major U.S. national security implications.

So, China is clearly not normal business environment for U.S. companies, and CFIUS modernization is the only way to effectively address the national security risks.

**Debunking Arguments by Opponents of FIRRMA**

I want to take a moment to debunk a few flawed arguments that some opponents of FIRRMA are making.

First, they say this bill represents regulatory overreach, which really misses the point. I am typically one of the loudest Senate voices of opposition to unnecessary regulation, as my track record demonstrates.  But, this is very different – CFIUS is not akin to something like the Consumer Financial Protection Bureau; instead, it is part of our national security apparatus. And, the federal government has no higher duty than to maintain our national security.

Second, opponents claim that the export control system can already address these national security risks, and that this update to the CFIUS statute is unnecessary. Without question, export controls are vital in preventing transfers of technology that would be damaging to national security, and I am committed to maintaining a strong export control system. That is why under FIRRMA the export control system would remain the first line of defense when it comes to technology transfers.

Export controls work reasonably well in many cases, but they have inherent limitations and are not enough by themselves. We need a second line of defense. The CFIUS process and the export control system are designed to be interactive and complementary, not mutually exclusive.  To effectively address the full range of mounting national security risks regarding China’s activities, these systems must be robust, interoperable, and seamless.

Our bill certainly does not *duplicate* the export control system. With transactions that represent pure technology transfers – basically, just the IP – FIRRMA leaves those to the export control system. It would only cover certain outbound U.S. transactions where they also include the transfer of know-how, which is the so-called “secret sauce.” These are the types of transactions that could help China acquire an industrial *capability* that is embodied in the U.S. business and accelerate China’s learning curve in areas of technology that are key to national security.

What’s more, FIRRMA includes safeguards to ensure that, with its expanded authorities, CFIUS would review transactions only when necessary. CFIUS would define circumstances in which transactions could be excluded because other provisions of law, such as export controls, are adequate to address any national security risks. This same provision also leaves ample room for future export control reform by giving CFIUS the flexibility to exempt transactions in the future that are adequately addressed through the export control regime.

CFIUS would also be authorized to create a “safe list” of certain allied countries, for which these new types of transactions would be exempt from review. This provision would drastically reduce the pool of transactions that would need CFIUS review, allowing CFIUS to focus its efforts on higher-risk deals.

Third, opponents argue that FIRRMA will flood and distract CFIUS with transactions that were previously routine. This argument questions whether addressing real national security threats is worth the financial cost; I assure you it is. For the price of a single B-21 bomber, we can fund an updated CFIUS process and protect our key capabilities for several years. That is a down payment on long-term national security. I am fully committed to securing the necessary funding for implementation to ensure the process continues to run smoothly, because this has to be a national security priority right up there with training and equipping our troops and intelligence professionals.

FIRRMA would also help provide additional resources, allowing CFIUS to charge modest filing fees and also submit a unified annual budget request covering all member agencies. And, the bill’s own provisions guard against an unfunded mandate, with the expansion only taking effect after CFIUS determines on its own that the necessary personnel and other resources are in place. FIRRMA also exempts outbound transactions that are done through “ordinary customer relationships,” ensuring harmless day-to-day activities do not have to be reviewed.

**Closing**

In closing, I also ask you to withhold judgment on FIRRMA until you have heard testimony from the Treasury Department and other key member agencies of CFIUS, who are on the front lines of this issue.

While it is certainly appropriate to consider what the potential impacts of this bill could be on foreign investment, that should not be done in a vacuum. We must also ask what the impacts on our *national security* will be if we do *not* take action on this.

As you hear from opponents of FIRRMA, I urge you to assess their credibility on this issue by asking some basic questions about their activities in China:

* What types of arrangements do you currently have in China with Chinese companies, what do you have planned for the near future, and is CFIUS able to review any of it?
* What dual-use technology and know-how has your company transferred to China over the last decade, and what impact has that had on our country’s relative national security advantage?

Increasingly, U.S. companies operating in China are being unfairly pressured into turning over valuable technology and know-how to Chinese companies, often as a condition of getting market access. Regardless, when U.S. companies engage in activities on Chinese soil that could negatively impact our national security, the federal government has a legitimate interest in being notified and afforded a chance to assess the national security risks. If CFIUS is not modernized to allow for this, we will continue to be in the dark here, and our national security will suffer.

I urge you to advance this bill for the sake of our long-term national security, which is being damaged before our very eyes. The time to modernize CFIUS is now, and we must not allow ourselves to be the frog in the boiling pot of water, so to speak.

Thank you, Mr. Chairman.