United States House of Representatives
Committee on Financial Services
Subcommittee on Monetary Policy and Trade

Examining the Operations of the Committee on Foreign Investment in the United States (CFIUS)

Opening Remarks of The Honorable Alan F. Estevez
Former Principal Deputy Under Secretary of Defense for Acquistion, Technology, & Logistics (2013-2017)

December 14, 2017

Chairman Barr, Ranking Member Moore, distinguished members of the subcommittee, thank you for opportunity to appear at this hearing and to testify regarding the Committee on Foreign Investment in the United States, or CFIUS.

While I am now at Deloitte, I want to be clear that the views I express today are my own. My expertise in this area derives from my previous position in government. I was the Principal Deputy Under Secretary of Defense for Acquisition, Technology, & Logistics, in an Acting capacity from 2011 to 2013, and confirmed in the position from 2103 to 2017. In that role, from 2011 to 2017, I managed the CFIUS process for the Department of Defense (DoD), and I was the DoD representative to the CFIUS.

Before I discuss my experience and views with regard to CFIUS, I believe it is important to review why CFIUS is critical to national security. There are many reasons that the United States has the finest military in the world, most importantly the innovative, dedicated men and women that volunteer to join the force. However, another reason is the technological superiority of our military force, or, in other words, our technological advantage over our adversaries. The US never wants to send our great force into a fair fight, we always want the advantage, and our technological superiority helps to ensure that. With that said, our technological advantage over potential adversaries has eroded. This happened for a number of reasons, to include the now 16-year focus on the war against terrorists, the inevitable globalization and commercialization of technology, and the devastating impacts of the Budget Control Act on DoD buying power. On the other hand, CFIUS is one of the tools that helps our military to retain its technological competitive advantage.

Based on my experience, the CFIUS interagency process worked, and, in fact, it worked well in protecting the national security of the United States. That does not mean that we did not have to adjust the process to make it more effective over time. However, I can say that over the hundreds of CFIUS cases that I processed as the DoD representative to CFIUS, I never signed off nor ever asked the Deputy Secretary of Defense to sign off on a CFIUS case resolution that would in any way imperil national security. In my view, the DoD always achieved the mitigation terms we asked for in cases that merited

mitigation, or received Committee support to propose a prohibition for those cases in which mitigation was too risky. This was true whether DoD was the lead agency along with the Department of Treasury, or the DoD was in support of another Department.

My second point is that current CFIUS authorities, along with the authorities in other Departments, such as the export control authorities of Commerce, allowed the Committee to properly adjudicate the wide variety of cases that came before the Committee. I'll address areas where I think authorities need to be expanded in a moment, but for the types of cases currently within CFIUS jurisdiction that we adjudicated during my time, we had adequate authorities to rely on.

When I assessed CFIUS transactions from the DoD perspective, I personally used a construct, which I called the three C's plus one. The C's represented Country, Company, and Commodity (which includes technology). The plus one was Co-location, that is when a foreign company proposed buying a company that was located near a sensitive military site. This framework helped me and my staff to assess the risk to national security involved in each transaction we processed. For each case, we would assess whether the home country of the purchasing party was a country of concern. The country of concern definition not only included potential adversaries or malicious actors, but also could include, for example, countries that were lax in protection of technology or were lax in the protection of personal identifiable information. This framework was not targeted at any particular country, but would incorporate intelligence community identification of the threat posed or potentially posed by any given country for any particular transaction.

In assessing companies, we would determine if the company was a state-owned enterprise, whether the company had been created for the specific deal, or if the company or its ownership was reliable and stable. To assess commodities and technology, we would assess criticality to DoD weapons systems, both current and future, how cutting edge the technology was, whether the technology was already globally available, and what the impact of a supply chain disruption would be.

Co-location cases, again, cases in which land or facilities near critical military training and test ranges was being purchased, became more prevalent over time. In these cases, we would assess what activities were taking place at a given location and whether the purchasing party would be able to observe or impact those activities.

If the DoD assessment raised a concern over any one of the C's, DoD would perform a deeper assessment of a given transaction. If we had concerns with two or more C's, my experience was that such cases were likely headed to mitigation of some kind or a recommendation to block. As I noted, current CFIUS and agency authorities allowed us to properly adjudicate cases regardless of whether the country involved, the company involved, the commodity or technology involved, or co-location was the issue.

Before moving onto areas where I believe CFIUS authorities need to be expanded or clarified, I do want to compliment the Treasury staff and the intelligence community for

the support that they provided to CFIUS. The Treasury staff worked very closely with the DoD, which I believe had co-leadership on most of the difficult cases. Treasury did an excellent job of making the process more efficient during my time as a Committee member, and they were always willing to adjust the internal process as the cases grew in complexity. The intelligence community provided much needed background on cases and they also altered their process to shorten timelines and provide additional detail, again as the cases grew in complexity.

I'd like to now turn to areas where I believe CFIUS needs expanded authorities. I recognize there are proposals currently being reviewed by this Congress. My comments are not based on any specific legislation, but rather, they are based on my CFIUS experience.

The first area I believe CFIUS needs to have increased jurisdiction over is Joint Ventures. Some Joint Ventures, in which companies form partnerships with other companies and in which ownership of the original company does not change, may put national security at risk through technology or intellectual property transfer. While I'm sure the vast majority of Joint Ventures do not threaten national security, the same three C's plus one framework I applied to CFIUS acquisition transactions involving foreign companies should be applied to Joint Venture transactions.

Coverage over entities in bankruptcy is another area where I believe we need to expand CFIUS authorities. Bankruptcies of US companies, especially those involved in futuristic or cutting edge technologies, could end in the sale of technology or intellectual property assets to countries or companies of concern. Again, CFIUS should be allowed to review these transactions, and if required, allowed to mitigate or block them.

The final area I believe we need to assess with regard to CFIUS authorities is what I called "connecting the dots." Under current CFIUS authorities, each transaction is reviewed separately, which generally works. However, during my time as a CFIUS representative, we noticed trends in which specific countries, and many times, companies, were engaged in multiple transactions involving segments for industry. These trends usually mirrored a country's stated goal of increasing its own capacity in a given industry segment. Most times, the companies and technologies being purchased were relatively small, not state-of-the-art, and not critical to national security. However, just as in merger and acquisition anti-trust assessments, there comes a point when too much of a particular segment of industry is under foreign control. In addition, while these small, not state-of-the-art companies may in and of themselves not be critical to national security, they may play a role in the supply chain of more critical companies. Control of multiple entities in a particular industry segment may also allow the mapping of the supply chain for the broader industry. Again, this may put national security at risk and should be assessed. I don't know what the tipping point for too much outside control of an industry segment is, and it likely varies by industry and by technology, but I believe that CFIUS must be given authority to assess trend analysis and weigh in on transactions based on that analysis when necessary.

The last area I would like to address is resources. The reality is that just to handle, manage, and mitigate the cases in the current workload, CFIUS needs more resources. The cases coming before the Committee are growing in their complexity, and I firmly believe that certain countries are actually testing the CFIUS process and seeking the gaps to overcome CFIUS. Resources are needed to adequately perform the due diligence on the cases that come before CFIUS in the time frames required by the CFIUS legislation. If CFIUS authorities are expanded in the ways I have outlined above or as outlined in proposed CFIUS legislation, CFIUS, both centrally and within each CFIUS member agency, will need more resources to process cases. Resources are also needed to adequately assess unfiled transactions, potentially the lower part of an iceberg of CFIUS-related threats to national security.

CFIUS also needs resources to perform mitigation oversight. As cases have grown in their complexity, mitigation agreements have also grown in complexity. To expect these agreements to be enforced from within existing staff resources is simply not realistic. Even when companies pay for the mitigation, the Federal government oversight is still required and must be resourced. I make this plea not as someone who currently has responsibility for managing stretched federal government resources, but as a private citizen with deep experience in this area and concern for our national security.

I thank the Committee for holding this hearing. This is a critical topic for continuing the long-term viability of our technological superiority – and technological superiority remains one of the foundations for our military capability. I look forward to your questions.