citba.org
Customs and International Trade Bar Association

April 15, 2024

Safeguarding National Security Amidst Foreign Investment in Defense Tech
By Phillip Euell, Of Counsel, Diaz, Reus & Targ, LLP

In recent years, the U.S. tech industry has seen a significant shift towards embracing national security and defense. This transition is part of a wider cultural evolution within Silicon Valley, transitioning from a traditionally cautious stance on military collaborations to actively supporting national defense initiatives. This change is driven by a variety of factors, including economic and geopolitical threats, such as escalating tensions with Russia and China, and the acknowledgment of advanced technologies' pivotal role in modern warfare and security.

The increasing focus on national security and defense innovation has attracted substantial investment from venture capital firms, many of whom now prioritize the defense tech sector. As a result, defense tech startups have experienced a surge in funding, which supports the development of technologies like hypersonic missiles, performance-enhancing wearables, and satellite surveillance systems. This influx of capital demonstrates the strategic significance of the defense tech sector and boosts investor confidence in its potential for growth, anticipated to expand markedly in the forthcoming years.

Significant returns on investment in the defense tech sector have not only benefited American venture capitalists but have also drawn attention from foreign investors. However, unlike their American counterparts, the investments of foreigners are subject to federal scrutiny under the Committee on Foreign Investment in the United States (CFIUS) regulations, as revised by the Foreign Investment Risk Review Modernization Act (FIRRMA), which broadened CFIUS's scope. Post-FIRRMA, transactions that had traditionally come under the review of the CFIUS resulting from non-U.S. person control, now include certain minority investments that do not grant control but involve critical technologies, executing critical infrastructure functions, or gathering specific sensitive personal data from over one million U.S. citizens. Under the law, such businesses are designated as a "TID U.S. business" or TID; and, typically, startup defense tech enterprises qualify as TID under the critical technologies component, as many of their technologies or products are listed on either the Commerce Control List (CCL) or the United States Munitions List (USML).

As a consequence, now even minority investments by non-U.S. persons lacking controlling stakes in defense tech, as TIDs, fall under the purview of CFIUS as “covered investments” if the investment provides a non-U.S. individual with access to significant non-public technical information, membership or observer rights on a board of directors or similar governing body of the business, or any other form of involvement in substantial decision-making processes. However, despite this enlarged purview, CFIUS has exempted some deals from these covered investment regulations if the only non-U.S. investors originate from closely allied countries like Australia, the United Kingdom, and Canada, and can demonstrate clean compliance records verified by CFIUS.

Additionally, after FIRRMA, CFIUS’s final regulations established the investment fund safe harbor, which shields U.S.-controlled investment funds from falling within CFIUS jurisdiction if they might otherwise qualify as a "covered investment" due to the involvement of foreign limited partners. Under the safe-harbor provision, a non-U.S. limited partner's participation in an investment fund won't be categorized as a "covered investment" in a U.S. business, provided the following conditions are met: (1) the fund must be exclusively managed by a general partner, who is a U.S. person and solely controlled by U.S. nationals; (2) the non-U.S. limited partner, along with any non-U.S. limited partners on an advisory board, should lack the authority to approve, disapprove, or control investment decisions of the investment fund, or decisions made by the general partner regarding entities in which the fund invests; (3) the non-U.S. limited partner shouldn't possess the power to unilaterally dismiss, prevent the dismissal of, select, or determine the compensation of the general partner; (4) the non-U.S. limited partner should not have access to significant non-public technical information; and (5) the investment must not grant the non-U.S. limited partner any "covered investment" rights over the business, such as access to significant non-public technical information, board or observer rights, or involvement in substantive decision-making regarding critical technologies.

Further, FIRRMA and the subsequent CFIUS final regulations introduced mandatory filing requirements for certain transactions, which entail an additional compliance obligation for non-U.S. investors and funds with non-U.S. limited partners. These mandatory filings are classified into two categories. The first category includes deals where the general partner of a fund is owned 49% or more by state-owned entities from the same non-U.S. country, and the fund acquires a 25% or greater interest in a TID. And, the second category involves investments in TIDs engaged in developing critical technologies utilized in 27 industries, including aircraft manufacturing, computer manufacturing, guided missile and space vehicle manufacturing, military vehicle manufacturing, chemical manufacturing, and research and development in nanotechnology or

biotechnology, among others.

Thus, when foreign investment in a defense tech business is contemplated, CFIUS regulations present challenges for investment funds, particularly if they do not carefully structure their limited partnership agreements and organize their transactions and due diligence processes. To navigate these challenges, generally speaking, U.S. investment funds need to prioritize strategies to ensure that non-U.S. investors are devoid of the authority to veto or exert control over the investment decisions made by the fund or the general partner. Moreover, U.S. investment funds need to curtail the extent of non-U.S. investors' rights over the general partner, particularly in matters pertaining to dismissal, selection, and compensation. Also, measures should be taken to prevent non-U.S. investors from obtaining positions on, observing, or appointing directors to the boards of directors of U.S. portfolio companies, instead restricting their involvement to membership on a limited partner advisory committee, which can offer industry expertise but does not wield decision-making authority over the fund or its portfolio companies. Finally, to prevent non-U.S. investors from gaining access to significant non-public technical information, information shared about defense tech businesses should be limited strictly to financial data.

In conclusion, the convergence of the U.S. tech industry and defense technology offers a significant opportunity for the nation to bolster its defense capabilities through innovation and investment. And, while foreign equity investment in the startup defense sector can provide a valuable resource, it is imperative for the U.S. to remain vigilant in safeguarding its national security interests. FIRRMA’s regulatory changes achieve this by requiring careful scrutiny of foreign investments in critical sectors because, while these foreign investments can fuel growth and foster technological advancement, they also pose potential risks to national security if not properly managed. Therefore, as the U.S. continues to attract foreign investment in its defense tech startups, it must continue to strike a delicate balance between capitalizing on opportunities for growth and ensuring robust safeguards to protect sensitive technologies and information