SAFEGUARDING OUR INNOVATION

PROTECTING U.S. EMERGING TECHNOLOGY COMPANIES FROM INVESTMENT BY FOREIGN THREAT ACTORS

THREAT

Venture capital (VC), private equity, and other foreign-origin private investment can provide vital funding for United States (U.S.) technology startups. Foreign threat actors can also use these investments to exploit U.S. startups and harm U.S. economic and national security interests.

- **U.S. startups can lose market share and fail** if foreign threat actors obtain their proprietary data in the investment process, then use it to compete against them in global markets.
- **Startups can be denied U.S. government contracts or funding** if foreign threat actors gain a footing in their firms.
  - To help mitigate foreign risk, federal agencies that grant Small Business Innovation Research or Small Business Technology Transfer awards are required to have due diligence programs to assess small businesses seeking these awards.
- **Startups can also suffer undue foreign influence** that forces corporate decisions or direction benefiting foreign threat actors at the expense of the U.S. company.
- **Foreign threat actors can acquire data and technology** from U.S. startups that advances their nation's economic and military capabilities at the expense of the U.S.
- **Foreign threat actors can also target startups** that contract with the U.S. government—and other critical U.S. sectors—to threaten U.S. national security.

U.S. startups seeking capital can face challenges in determining the ownership and intent of foreign investors. **For example, foreign threat actors may:**

- **Structure their investments to avoid scrutiny** from the Committee on Foreign Investment in the United States (CFIUS), which reviews certain mergers, acquisitions, and investments into the U.S. for national security risks.
- **Route investments through intermediaries** in the U.S. or other third countries to obscure the money's origin.
- **Use minority and limited partner investments.**
- **Attempt to acquire sensitive and proprietary data** from U.S. startups under the guise of due diligence, before investing.

In 2018, the U.S. Trade Representative warned that **the People's Republic of China (PRC) government directs the investment in, and acquisition of, U.S. companies by China-based firms** to obtain technologies and Intellectual Property (IP), and to facilitate technology transfer to support PRC state plans. VC investment from China has focused on U.S. emerging technology sectors like Artificial Intelligence and other PRC government priorities. Recent developments have heightened these concerns:

- **In January 2024, the U.S. Department of Defense (DOD) added IDG Capital, a China-based VC/private equity firm, to its list of "Chinese military companies"** operating directly or indirectly in the U.S. The firm has invested in more than 1,600 companies, including several in the U.S.
- Last year, the CEO of a U.S. startup (which is suing defendants in China for trade secret theft) told U.S. Congress that **some China-based VC firms may target and pay employees of U.S. startups to acquire technology**, then fund competitors in China who try to monetize the stolen technology.
- Some U.S. and European firms have alleged **China-based investors offered them investments, then withdrew the offers** after obtaining their proprietary data in the due diligence process.
- One U.K. firm, after agreeing to a takeover by an investor in China, began transferring technology to its would-be acquirer in exchange for part of the firm's sales price. The investor in China later abandoned the acquisition. **The U.K. firm was left facing bankruptcy after sharing its IP.**

POTENTIAL INDICATORS

Below are activities that may be associated with investment efforts by foreign threat actors, although some of them are also routine legal tactics. U.S. technology startups should be diligent if foreign investment involves:

- **Complex Ownership:** A foreign investor whose structure includes separate entities with the same key personnel or shell companies with no substantive purpose. Entities are often incorporated in offshore locations lacking transparency and effective regulatory oversight.
- **Investments Through Intermediaries:** A foreign investor that routes investment through funds, partners, or intermediaries in the U.S. or other countries. This tactic can help foreign threat actors avoid or complicate outside scrutiny through degrees of separation.
- **Limited Partner Investments:** A foreign investor that invests in U.S. companies indirectly through U.S. firms or others in which they are limited partners. Some limited partners are truly passive, while others can gain influence over corporate decisions or access to proprietary data.
- **Requests for Sensitive Data:** A foreign investor that requests proprietary or other sensitive data from a U.S. firm before making an investment or while feigning interest in an investment. All investors conduct due diligence. Startups should be alert to intrusive requests for sensitive data.
- **Preying on Struggling U.S. Firms:** A foreign investor that preys on struggling U.S. companies, which can lead to the transfer of a company's IP in exchange for an infusion of capital.

MITIGATION

U.S. technology startups are not helpless. Below are some steps U.S. companies can take to guard against investment by foreign threat actors.

- **Identify and Protect Critical Assets:** Before seeking investment, identify and compartmentalize your company's "crown jewels."
  - Put physical and virtual protection around these assets.
  - Restrict access only to those who require it.
  - Identify a risk manager empowered by leadership to organize protection efforts.
  - Include protections for your assets within contracts and investment documentation.
  - Ensure legal and contractual agreements are enforceable in the investor's home country.
  - Implement a structure that ensures risk management over time.
- **Know Your Investor:** Scrutinize prospective investors to assess risks.
  - Verify who they say they are, who owns them (e.g., foreign governments or militaries), and the origin of their funding.
  - Determine if investors are subject to sanctions, export controls, or similar designations.
  - Research the laws where the foreign investor operates. Determine if they must share data with or assist their host government.
  - Confirm that their values and intentions align with your own.
- **Limit Your Exposure:** Before negotiating with investors, determine what is appropriate to share.
  - Limit data sharing to only that which is appropriate, before and after investment.
  - Identify red lines and responses if an investor requests information beyond what you would share with other investors.
  - Set protocols for investors to handle sensitive data appropriately.
  - Consider what you could lose if an investor reneges on a deal.
- **Engage:** Engage federal agencies and others in your industry to gather and share up-to-date threat information and risk mitigation resources.

REPORTING

- To report a tip about a potential foreign investment with national security implications, contact **CFIUS.tips@treasury.gov** or **(202) 622-1860**.
- If you believe that you, your personnel, or your company's data have been targeted, or are at risk of compromise, contact your local FBI Field Office: **https://www.fbi.gov/contact-us/field-offices**.
- To report foreign investment of concern in U.S. DOD critical technology sectors, contact the Department of the Air Force Office of Special Investigations and the Naval Criminal Investigative Service at **https://www.osi.af.mil/Submit-a-Tip/** or **https://www.ncis.navy.mil/Resources/NCIS-Tips/**
- For more threat awareness materials or publications, visit the National Counterintelligence and Security Center (NCSC) website at **www.ncsc.gov** or contact **DNI_NCSC_OUTREACH@dni.gov**.