Bipartisan Innovation Act

Conference Committee Working Paper: Conceptual Draft of Narrowed Scope Changes to National Critical Capabilities Defense Act (NCCDA)

The Problem

"Last year, venture capital firms financed $114B in Chinese companies that are developing dual-use and sensitive technologies that are going to be weaponized against us or already are aiding and abetting the Russians."

- Former U.S. National Security Adviser H.R. McMaster

The U.S. has limited visibility into critical capabilities- U.S. direct investments, technology and know-how transfers *(e.g. technical personnel, not salespeople)***, and "smart capital" flows- into adversary countries like China and Russia, leading to gaps in regulation, unacceptable risk to U.S. national security, and the continuing enhancement of foreign adversary's military, surveillance, and industrial capabilities through support from U.S. firms.**

- Critical Capabilities are the supply chains or the ability to produce them that are vital to the U.S. national security.
- Unacceptable risk means that U.S.-enabled development of a critical capability would result in a foreign adversary possessing dependence, advantage, or concentration over the U.S. in the case of a geo-political or national security event between the foreign adversary and the U.S.
- This lack of visibility extends to our domestic supply chain vulnerabilities.

U.S. Multinational Companies Need to be Part of the Solution, Not Supporters of Building Adversary Capabilities and Leaders of Delay Tactics

The time has come for U.S. companies to work with the government to be part of the solution with China, not obscure the problem so it continues to metastasize.

- Even as American companies call for a transparent and predictable environment in which they can conduct business with foreign adversaries like China, the same companies actively shield such information from the U.S. government in their corporate vaults, preventing the U.S. government from knowing where to draw the line to properly regulating such flows to our adversaries, protect U.S. national security, and ensure supply chain integrity and resiliency.

Offering A Narrower Approach to Achieve Responsible, Thoughtful Solutions

To address corporate concerns and meet U.S. business half-way so that it supports responsible regulation of these flows to the People's Republic of China and other adversary countries, this is an option for narrowing the legislation as follows:

The legislation will only cover prospective investments; previous investments are grandfathered. This new scope, as with the previous, is prospective and for forward-looking investments only.

The revised legislation would narrow the scope of covered investments, know-how transfers, and smart capital flows. Notification of covered investments, know-how transfers, and smart capital flows from private entities to foreign adversaries will now be limited to the following:

1. **Recipients of taxpayer funding under the Bipartisan Innovation Act.** Recipients of taxpayer funds from the U.S. government such as those authorized in the Bipartisan Innovation Act.

2. **Sectors specified in Executive Order 14017.** Critical supply chains sectors limited to those in Executive Order 14017. Private sector input will be key in the identification of such supply chains.

3. **Beneficiaries of government procurement contracts with national security agencies or with a purpose to protect national security above a de minimis threshold.** U.S. companies that benefit from procurement opportunities with U.S. national security agencies (DOD, CIA, NSA, etc.) or to protect national security will be required to notice their investments in foreign adversary countries.

The legislation will be further circumscribed to include additional exemptions and protections to include:

1. **Investments below a de minimis threshold and that do not contain know how transfers** in sectors specified in the National Science and Technology Council February 2022 Critical and Emerging Technologies List Update or that are export controlled;

2. **Normal business transactions as originally envisioned under FIRRMA.**

3. **A trusted-participant program** whereby companies that have received thorough vetting by the U.S. government are deemed to comply with initial notifications.

4. **Express statutory prohibitions** to prevent U.S. government overreach of transactions not located in or controlled by the adversary or in an allied country.

<u>Jurisdiction and Reviews Should be Aligned with Government Resources at the Discretion of the President</u>

Jurisdiction will be subject to the decision of the President, but false narratives from U.S. industry must not delay passage. The legislation will ensure there is appropriate alignment between the scope of the legislation and the location of resources in the U.S. government to execute on its mandate. There is not flexibility, however, when it comes to efforts by members, backed by industry that wish to continue to build the scale and technological capabilities of foreign adversaries, to delay implementation of a meaningful outbound investment and

technology transfer screening process that will protect our national security. Non-notification of covered transactions would result in civil penalties and immediate remediation of a transaction. The Congress in 2018 mandated what it thought was a meaningful approach to outbound technology screening through so-called "connective tissue" between the Treasury-led CFIUS and DOC-led export controls, but that connective tissue never materialized because the Department of Commerce never designated consequential foundational or emerging technologies. Action should happen now, and jurisdictional squabble should not be an impediment to swift passage of the legislation.

As with the current legislation, this revised scope would provide explicit protection from duplication with Export Controls at the Department of Commerce and Foreign Direct Investment reviews via CFIUS. Rather, this new draft of the NCCDA would fill a gap between both as described above.

Working with Allies and Partners to Align Regimes is Critical But Must Not Hinder Immediate Adoption of an Effective Outbound Screening Regimes as part of the Bipartisan Innovation Act of 2022

It is time for the U.S. to align its own outbound investment and technology transfer screening regime with those of allies and partners such as South Korea and Taiwan who have already taken this critical step to protect their national security. As the Semiconductor Industry has highlighted in a report by Akin Gump for the association, South Korea and Taiwan have already adopted an outbound investment and technology transfer screening mechanisms in their domestic laws and regulations, particularly for the semiconductor industry. Next month, **Japan** will follow with a sweeping new Economic Security Law, which will bolster the Japanese government's ability to screen outbound investment and technology flows to countries like China.

We should prioritize use of the U.S.-EU Technology and Trade Council (TTC), the QUAD, and other plurilateral and bilateral engagements with allies and partners to secure near-term alignment with burgeoning U.S. efforts to screen outbound investment and technology transfers to foreign adversaries. The outbound technology screening language in last year's Joint U.S.-EU Cooperative Framework for Large Civil Aircraft could have provided the basis for meaningful joint action, but we have yet to see evidence of concrete cooperation beyond the rhetoric.

The absence of progress with allies and partners in Europe and feigned support by the American business community for plurilateral efforts on outbound investment and technology transfer screening – not to mention export controls – must not impede congressional passage of legislation to address outbound investment and technology screening gaps in 2022. The onus is on American business, which claims to support cooperation among allies and partners to address third-country challenges, and our government to jointly pressure the EU and key member states to deliver results that will protect our innovation, competitiveness and national security against our adversaries. Input from the business community is essential in striking a balance between national security and the continued free and fair flow of commerce with foreign adversary nations.