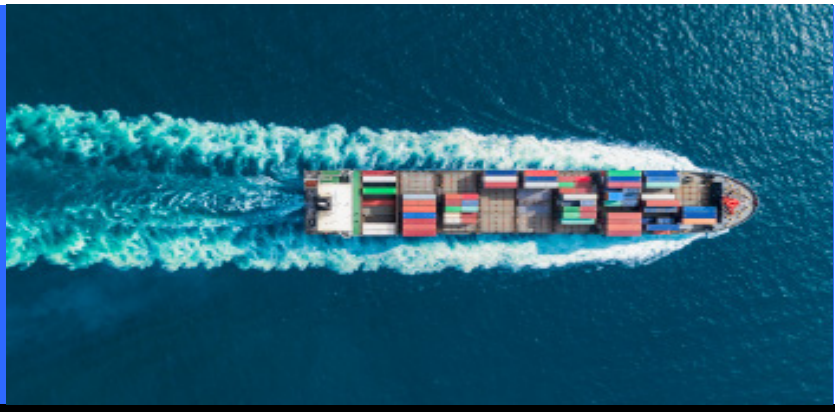
View on our website.

GIBSON DUNN



International Trade Advisory & Enforcement Update July 30, 2026

Risky Business: CFIUS Provides Clarity into Higher-Risk Transactions and Enforcement Priorities

New CFIUS Risk Matrix identifies categories of transactions that pose elevated national security risks and provides sample mitigation measures that the Committee has imposed across a variety of sectors.

On July 29, 2026, the U.S. Department of the Treasury, in its capacity as Chair of the Committee on Foreign Investment in the United States (CFIUS or the Committee) announced the creation of a revamped CFIUS website and issued a CFIUS Risk Matrix (included below), identifying eight categories of transactions that pose elevated national security risks and providing sample mitigation measures that the Committee has imposed across a variety of sectors. Although the contents of the matrix are not novel to CFIUS practitioners, the document's issuance reflects efforts by the Trump Administration to increase transparency in the CFIUS process, while also foreshadowing potential enforcement efforts and mitigation steps.

What the matrix says:

The matrix describes eight transaction profiles that raise elevated national security risks. Consistent with CFIUS's standard risk-based analysis, as outlined in 31 C.F.R. § 800.102, the matrix evaluates each profile across three factors, namely:

- **Threat**: Intent and capabilities of a foreign person to take action to impair the national security of the United States;
- **Vulnerability**: Extent to which the nature, location, or relationships of the U.S. business presents susceptibility to impairment of national security; and

- **Consequences**: Potential effects on national security that could reasonably result from the exploitation of the vulnerabilities by the threat actor.

For each transaction profile, the matrix describes how the Committee assesses the risk calculus, explains the purpose of mitigation efforts, and provides an illustrative set of mitigation measures that may be implemented to address the relevant threat, vulnerability, and consequences of the national security risk.

The bigger picture:

The release of the matrix should be considered through the lens of other Trump Administration initiatives, most notably the America First Investment Policy, described in detail in our previous client alert. That policy aims to protect key sectors and encourage investment from allied countries, while screening for non-passive investment from certain "foreign adversaries," including, in particular, China. As part of an effort to encourage investment from allied countries and minimize the regulatory burden associated with transactions that pose minimal national security risk, Assistant Secretary for Investment Security Chris Pilkerton recently expressed a desire to "increase our focus on customer service" by "demystify[ing] the process and increas[ing] transparency and predictability for filers."

The matrix, coupled with the Committee's recently introduced pre-filing consultation website function, provides additional insight into the Committee's risk assessment process and aligns with CFIUS's goal of increasing engagement with industry even before a filing is imminent. The matrix's discussion of common mitigation measures and their purposes similarly reflects the Committee's efforts to be more strategic in mitigation agreements and to avoid what had been a growing number of potentially complex and open-ended agreements.

There is, however, also a warning inherent in the release of the matrix. The matrix takes a broad view of potential national security risks across commercial sectors. The Committee has signaled—and has increasingly shown—a willingness to exercise its review authority through non-notified outreach. Parties to higher-risk transactions, especially ones with profiles similar to those in the matrix, should exercise heightened caution when evaluating whether to forgo engagement with the Committee, including decisions regarding voluntary filings.

What this all means for prospective filers:

- Continue to focus on the core national security risk framework: threat, vulnerability, consequence.
- Be mindful of the risk examples shared in the matrix; look for parallels to your own transaction.
- Consider proactive engagement with CFIUS, especially for transactions that may raise significant risks, but maintain appropriate caution when sharing information with the Committee.

Ultimately, the matrix offers a valuable window into how the Committee frames national security risk, but it is not a substitute for case-by-case analysis. Each review remains inherently fact-specific, turning on the particular national security threats, vulnerabilities, and consequences raised by a given transaction. Parties should treat the matrix as a starting point for identifying potential concerns—not a checklist for clearing them—and undertake a nuanced, transaction-specific assessment, in consultation with counsel, in deciding when and how to engage with the Committee.

COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) RISK MATRIX*

Category of Risk	**Threat** *A function of the intent and capability of a foreign person to take action to impair the national security of the United States*	**Vulnerability** *The extent to which the nature of the U.S. business presents susceptibility to impairment of national security*	**Consequence** *The potential effects on national security that could reasonably result from the exploitation of the vulnerabilities by the threat actor*	**Purpose of Mitigation** *CFIUS must determine that mitigation resolves the national security concerns posed by the transaction*	**Sample Mitigation Measures** *Terms must be reasonably calculated to be effective, allow for verifiable compliance, and enable effective monitoring of compliance and enforcement*
Critical Infrastructure	Show intent and capability to impair or disrupt U.S. critical infrastructure systems or assets, or take actions that could result in such impairment or disruption	U.S. business owns, operates, or services critical infrastructure systems or assets	Potential impairment to or disruption of U.S. critical infrastructure systems or assets	Safeguard integrity and security of U.S. critical infrastructure systems and assets	CFIUS-specific governance structures, restrictions, and oversight mechanisms to limit foreign influence over the U.S. business; Controls to ensure operational continuity of infrastructure systems and assets; Implementation of specific plans and policies subject to CFIUS approval, including those governing cyber, data, and
Cybersecurity	Show intent and capability to introduce and/or exploit potential cyber vulnerabilities, or take actions that could result in such introduction or exploitation	U.S. business provides cybersecurity for sensitive businesses or assets or lacks robust safeguards to counter cyber vulnerabilities	Potential introduction and/or exploitation of cyber vulnerabilities by foreign threat actors	Detect and prevent unauthorized access, introduction, or exploitation of cyber vulnerabilities	
Information Security	Show intent and capability to	U.S. business collects and	Potential access to and exploitation	Prevent unauthorized	

	access and/or exploit sensitive operational or technical data, or take actions that could result in such access or exploitation	maintains sensitive operational or technical data	of sensitive operational or technical data by foreign threat actors	access to, and ensure the security of, sensitive operational or technical data	technology security controls; Periodic source code reviews and testing; Restrictions on integration, communications and information sharing; Segregation of protected technology, information, data, systems, etc.; Restrictions on physical and logical access to data and systems, and prohibition of business ties with foreign actors of concern; Requirements to maintain existing design, development, and production processes; Restrictions on access to properties; Third-party vendor risk management and vetting; Continued supply of covered products and/or
Personal Data Security	Show intent and capability to access and/or exploit sensitive personal data, or take actions that could result in such access or exploitation	U.S. business collects or maintains sensitive personal data	Potential access to and exploitation of sensitive personal data	Prevent unauthorized access to, and ensure the security of, sensitive personal data	
Product Integrity	Show intent and capability to modify, alter, or degrade product quality and/or production processes, or take actions that could result in such modification, alteration, or degradation	U.S. business provides products needed for critical national security missions	Potential degradation of or inability to use products needed for national security	Ensure products maintain required quality, performance, and production processes	
Proximity Concerns	Show intent and capability to exploit physical proximity to sensitive facilities, or take actions that could result in such exploitation	U.S. business or real estate is located near a USG installation, facility, or property	Potential exploitation of physical proximity to sensitive facilities by foreign threat actors	Address risk associated with co-location of properties in or near sensitive USG facilities	
Supply Assurance	Show intent and capability to	U.S. business provides	Potential degradation or	Ensure continued supply of products	

	limit or alter existing and/or future supply of products or services to USG or other sensitive buyers, or take actions that could result in such limitation or alteration	products or services needed for critical national security missions	loss of access to products or services needed for national security	or services to USG, including future supply of products/services or their orderly replacement	services for specified period and notification requirements prior to altering supply; Third-party monitorships and audits; and Compliance certifications, reporting, and CFIUS access and inspection rights.
Technology Transfer	Show intent and capability to allow unauthorized transfer or use of sensitive technology and/or know-how, or take actions that could result in such transfer	U.S. business owns and/or develops sensitive technology and/or know-how, including with dual-use or military applications	Potential transfer or use of sensitive technology and/or know-how to foreign threat actors	Prevent unauthorized transfer or use, whether intentional or unintentional, of sensitive technology or know-how	

* *CFIUS staff share this document for informational purposes only. Nothing in this document constitutes legal, professional, or investment advice. The simplified risk categories and sample mitigation measures shown in this document are illustrative, non-exclusive, and non-exhaustive in nature and should not be construed as a final position, policy, commitment, or recommendation. This document does not impose any obligations on, or limit any rights of, any of CFIUS, the U.S. Department of the Treasury, or the U.S. Government. CFIUS makes no representation as to its judgment regarding the sufficiency of the sample measures in this document to mitigate any national security risk arising from any individual transaction and may, in its sole discretion based on CFIUS's individualized assessment of the national security risk arising from a transaction, propose mitigation terms that are materially different from those in this document, or forego proposing mitigation terms and refer a transaction to the President with a recommendation to prohibit.*

The following Gibson Dunn lawyers prepared this update: Chris Mullen, William Huesken, and Stephenie Gosnell Handler.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these issues. For additional information about how we may assist you, please contact the Gibson Dunn lawyer with whom you usually work, the authors, or the following leaders and members of the firm's International Trade Advisory & Enforcement practice group:

United States:
Adam M. Smith – Co-Chair, Washington, D.C. (+1 202.887.3547, asmith@gibsondunn.com)
Ronald Kirk – Co-Chair, Dallas (+1 214.698.3295, rkirk@gibsondunn.com)
Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Donald Harrison – Washington, D.C. (+1 202.955.8560, dharrison@gibsondunn.com)
Christopher T. Timura – Washington, D.C. (+1 202.887.3690, ctimura@gibsondunn.com)
Matthew S. Axelrod – Washington, D.C. (+1 202.955.8517, maxelrod@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202.887.3786, dburns@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213.229.7269, nhanna@gibsondunn.com)
Courtney M. Brown – Washington, D.C. (+1 202.955.8685, cmbrown@gibsondunn.com)
Samantha Sewall – Washington, D.C. (+1 202.887.3509, ssewall@gibsondunn.com)
Roxana Akbari – Orange County (+1 949.475.4650, rakbari@gibsondunn.com)
Karsten Ball – Washington, D.C. (+1 202.777.9341, kball@gibsondunn.com)
Sarah Burns – Washington, D.C. (+1 202.777.9320, sburns@gibsondunn.com)
Hugh N. Danilack – Washington, D.C. (+1 202.777.9536, hdanilack@gibsondunn.com)
Justin duRivage – Palo Alto (+1 650.849.5323, jdurivage@gibsondunn.com)
Dorkas Laura Medina – Washington, D.C. (+1 202.777.9444, dmedina@gibsondunn.com)
Chris R. Mullen – Washington, D.C. (+1 202.955.8250, cmullen@gibsondunn.com)
Sarah L. Pongrace – New York (+1 212.351.3972, spongrace@gibsondunn.com)
Anna Searcey – Washington, D.C. (+1 202.887.3655, asearcey@gibsondunn.com)
Erika Suh Holmberg – Washington, D.C. (+1 202.777.9539, eholmberg@gibsondunn.com)
Audi K. Syarief – Washington, D.C. (+1 202.955.8266, asyarief@gibsondunn.com)
Scott R. Toussaint – Washington, D.C. (+1 202.887.3588, stoussaint@gibsondunn.com)
Shuo (Josh) Zhang – Washington, D.C. (+1 202.955.8270, szhang@gibsondunn.com)

Asia:
Kelly Austin – Denver/Hong Kong (+1 303.298.5980, kaustin@gibsondunn.com)
David A. Wolber – Hong Kong (+852 2214 3764, dwolber@gibsondunn.com)
Fang Xue – Singapore (+65 6507 3692, fxue@gibsondunn.com)
Qi Yue – Beijing (+86 10 6502 8534, qyue@gibsondunn.com)
Dharak Bhavsar – Hong Kong (+852 2214 3755, dbhavsar@gibsondunn.com)
Soo-Min Chae – Singapore (+65 6507 3632, schae@gibsondunn.com)
Hui Fang – Hong Kong (+852 2214 3805, hfang@gibsondunn.com)
Arnold Pun – Hong Kong (+852 2214 3838, apun@gibsondunn.com)

Europe:
Attila Borsos – Brussels (+32 2 554 72 10, aborsos@gibsondunn.com)
Patrick Doris – London (+44 207 071 4276, pdoris@gibsondunn.com)
Michelle M. Kirschner – London (+44 20 7071 4212, mkirschner@gibsondunn.com)
Penny Madden KC – London (+44 20 7071 4226, pmadden@gibsondunn.com)
Irene Polieri – London (+44 20 7071 4199, ipolieri@gibsondunn.com)
Benno Schwarz – Munich (+49 89 189 33 110, bschwarz@gibsondunn.com)
Nikita Malevanny – Munich (+49 89 189 33 224, nmalevanny@gibsondunn.com)

Melina Kronester – Munich (+49 89 189 33 225, mkronester@gibsondunn.com)
Vanessa Ludwig – Frankfurt (+49 69 247 411 531, vludwig@gibsondunn.com)