Simpson Thacher

To read Treasury's Press Release, please click here.

Report from Washington

CFIUS Issues New Risk Matrix and Mitigation Guidance

July 29, 2026

On July 29, 2026, the U.S. Department of the Treasury ("Treasury"), as Chair of the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee"), published new guidance for the public in the form of a CFIUS Risk Matrix. The Matrix identifies eight categories of common national security risks often identified during the CFIUS process (*i.e.*, critical infrastructure, cybersecurity, information security, personal data security, product integrity, proximity concerns, supply assurance and technology transfer), as well as an explanation of the vulnerabilities that can arise with respect to foreign ownership in businesses with such risks. In addition, the Matrix also sets out the purpose of mitigation for each category and provides a list of sample mitigation terms frequently used in mitigation agreements. The Matrix is replicated in the attached Appendix.

The Matrix is a notable development for dealmakers and their advisors as it provides structured insight into and memorializes for the public many of the national security considerations relating to national security risk and the potential for mitigation that are often advised by CFIUS practitioners. It also provides a baseline understanding of common mitigation terms that may arise when parties are considering a CFIUS filing. This guidance should prove particularly useful as parties consider and weigh potential mitigation that might arise in the CFIUS context, and will allow buyers, sellers, and their counsel to align on what terms are typical for certain categories of transactions. This should also facilitate earlier and more informed discussions between buyers and sellers regarding potential CFIUS conditions and may help parties more efficiently negotiate CFIUS-related provisions in transaction documentation.

Contemporaneously with the issuance of the Matrix, CFIUS has also implemented a new portal through which transaction parties can submit questions about CFIUS and provide information about their transactions to engage with the Committee early in the process. This tool is intended to help parties better understand CFIUS processes and filing options—including the distinction between short-form declarations and full notices—and to support more efficient reviews. Early engagement with CFIUS has long been considered a best practice by experienced practitioners, and the formalization of this portal should encourage broader use of pre-filing consultations across the deal community.

These developments represent a significant step to enhance the accessibility of the CFIUS process. As Treasury Secretary Bessent noted, the Administration is "significantly upgrading CFIUS's customer service, making it easier for companies, investors, and their counsel to find the information they need, understand our processes, and facilitate greater foreign investment in the United States." We encourage clients and deal teams to review the new risk Matrix and mitigation guidance, and to consider how these resources may inform CFIUS-related risk assessments, transaction structuring, and mitigation negotiations on pending and future transactions.

For further information about this Report, please contact one of the following members of the Firm's National Security Regulatory Practice:

WASHINGTON, D.C.

Malcolm J. (Mick) Tuesley
+1-202-636-5561
mick.tuesley@stblaw.com

Mark B. Skerry
+1-202-636-5523
mark.skerry@stblaw.com

Abram J. Ellis
+1-202-636-5579
aellis@stblaw.com

Claire M. DiMario
+1-202-636-5536
claire.dimario@stblaw.com

Jennifer Ho
+1-202-636-5525
jennifer.ho@stblaw.com

Vineeta Kamath
+1-202-636-5879
vineeta.kamath@stblaw.com

Jim Perry
+1-202-636-5717
james.perry@stblaw.com

Ryan D. Stalnaker
+1-202-636-5992
ryan.stalnaker@stblaw.com

Jill Boggs
+1-202-636-5917
jill.boggs@stblaw.com

Sean Patrick Boyle
+1-202-636-5910
sean.boyle@stblaw.com

Alexis V. Capati
+1-202-636-5813
alexis.capati@stblaw.com

Rocquel Donofrio
+1-202-636-5500
rocquel.donofrio@stblaw.com

Michael Kalinin
+1-202-636-5989
michael.kalinin@stblaw.com

Austin Lowe
+1-202-636-5862
austin.lowe@stblaw.com

Liam Murray
+1-202-636-5585
liam.murray@stblaw.com

Noah Sissoko
+1-202-636-5574
noah.sissoko@stblaw.com

Ryan Daniel Thomas
+1-202-636-5586
ryan.thomas@stblaw.com

Peter Tian
+1-202-636-5882
peter.tian@stblaw.com

Feven K. Yohannes
+1 202-636-5944
feven.yohannes@stblaw.com

Shinae Yoon
+1-202-636-5903
shinae.yoon@stblaw.com

The contents of this publication are for informational purposes only. Neither this publication nor the lawyers who authored it are rendering legal or other professional advice or opinions on specific facts or matters, nor does the distribution of this publication to any person constitute the establishment of an attorney-client relationship. Simpson Thacher & Bartlett LLP assumes no liability in connection with the use of this publication. Please contact your relationship partner if we can be of assistance regarding these important developments. The names and office locations of all of our partners, as well as our recent memoranda, can be obtained from our website, www.simpsonthacher.com.

APPENDIX

CFIUS Risk Matrix – Categories of National Security Risk and Sample Mitigation Measures

Source: CFIUS.gov (July 2026).

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 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 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.
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 access and/or exploit sensitive operational or technical data, or take actions that could result in such access or exploitation	U.S. business collects and maintains sensitive operational or technical data	Potential access to and exploitation of sensitive operational or technical data by foreign threat actors	Prevent unauthorized access to, and ensure the security of, sensitive operational or technical data	
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 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	U.S. business provides products or services needed for critical national security missions	Potential degradation or loss of access to products or services needed for national security	Ensure continued supply of products or services to USG, including future supply of products/services or their orderly replacement	
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	