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

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.

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	