Regulatory Transparency and Substantive Review of Offshore Structures: A Study on Transaction Risks in Cross-Border Acquisitions by Chinese and U.S. Technology Companies

Qinglan (Ruby) Zhang

Research Scholar

Above and Beyond Leadership and Education (ABLE)

Research Advisor: Sherry Hu, Ph.D.

Above and Beyond Leadership and Education (ABLE)

Abstract

Offshore intermediate layers—typically a Singapore subsidiary interposed between a Chinese parent and a U.S. target—are often expected to isolate a cross-border acquisition from Chinese and U.S. regulatory jurisdiction. This paper tests that assumption against two recent cases, the Manus prohibition decision and the Suirui/Jupiter divestment enforcement, while stressing that the two engage different legal regimes and cannot be reduced to a single look-through formula. Using a scenario in which a Chinese parent with substantive domestic R&D acquires, through a Singapore subsidiary, a U.S. enterprise-AI software company whose customers include federal contractors and which holds U.S. user data, the paper distinguishes three Chinese regimes (foreign investment security review, outbound investment regulation, and technology export control), examines CFIUS's TID characterization and the actual triggers of mandatory declaration, and separates EAR export, reexport, and deemed export. The central claim is that convergence between the two sides is methodological, not normative: the U.S. axis is foreign acquisition of control over a TID U.S. business, while the Chinese axis is whether domestically formed technology, data, and teams move abroad without statutory procedures. The paper's original contribution is the interpretive proposition of "mutual evidentiary reinforcement," offered as an analytical framework rather than an empirical finding. Contractual and structural tools can screen and price regulatory risk, but cannot create a regulatory clean offshore identity; meaningful compliance lies in front-end identification.

Keywords: offshore structures; CFIUS; foreign investment security review; cross-border M&A

I. Introduction

In cross-border technology transactions involving both China and the United States, structuring a multi-tiered offshore framework—such as "Cayman–Singapore–China"—has long been regarded by industry practitioners as a pragmatic risk-management strategy. The underlying rationale is this: the operating entity based in China undertakes R&D and business operations, while a Singapore-incorporated subsidiary serves as the overseas acquiring entity or financing platform. By leveraging Singapore's corporate legal framework, its tax treaty network, and its geopolitical neutrality, some parties may hope that this structure reduces regulatory exposure; however, incorporation in Singapore does not itself remove U.S. or Chinese jurisdiction where the relevant legal tests are met. In such cases, the Singapore subsidiary is sometimes presented as an "isolation layer": to the U.S. side, it asserts that the acquiring party is not a Chinese entity; to the Chinese side, it maintains that the transaction occurs between overseas entities, without any transfer of domestic interests.

However, that situation has now been directly challenged in the Manus acquisition case. On April 27, 2026, the Office of the Working Mechanism for Security Review of Foreign Investment (the "Security Review Office"), housed within the National Development and Reform Commission ("NDRC"), issued a notice stating that it had "lawfully and in accordance with regulations made a decision to prohibit investment in the foreign acquisition of the Manus project and required the parties to revoke the acquisition transaction."[1] The notice does not disclose the specific statutory provision relied upon, the procedural posture of the review, or the factual findings underpinning the decision. Manus was founded by a team of Chinese entrepreneurs; its core technologies were initially developed in Beijing and Wuhan, and in March 2025 it garnered market attention upon launching a general-purpose AI agent product. Following the relocation of its headquarters to Singapore in June 2025 and a significant scaling back of its domestic operations, the U.S. technology company Meta announced in December of the same year that it would acquire Manus in a transaction reportedly valued at more than US$2 billion. On January 8, 2026, China's Ministry of Commerce, in coordination with relevant departments, announced the initiation of an assessment and investigation into whether the acquisition complied with laws and regulations governing export controls, import and export of technologies, and outbound investment, thereby formally triggering regulatory review. On April 27, Xinhua News Agency released an official statement: the Office of the Working Mechanism for Security Review of Foreign Investment (referred to as the "Security Review Office") had, in accordance with the law, issued a decision prohibiting foreign-capital

acquisition of Manus and ordered the parties concerned to unwind the transaction, even though, on paper, the deal was executed between two overseas entities.

On the other hand, in U.S. review proceedings, the Suirui/Jupiter case demonstrated the limits of relying on offshore structures to avoid review: SuiRui Group completed its acquisition of Jupiter Systems through a Hong Kong subsidiary in 2020 without prior CFIUS review; in March 2024, approximately four years later, CFIUS initiated a retroactive review. On July 8, 2025, a presidential order mandated divestiture within 120 days; CFIUS granted two extensions, pushing the deadline to February 3, 2026, which SuiRui failed to meet. In February 2026, the DOJ filed its first lawsuit, and the court issued a preliminary injunction, appointing a receiver to oversee Jupiter's operations until the divestiture was completed. Taken together, these two cases illustrate that the "structural isolation" purportedly achieved by offshore structures has, on both sides of the U.S.–China divide, been undermined by review approaches anchored in substantive connections.[1][2]

This paper begins with the following scenario: a technology company with substantive R&D activities and a core technology team in China ("Chinese Parent") proposes to acquire all shares of a U.S. technology company ("U.S. Target") through its Singapore subsidiary ("Singapore Subsidiary"). The U.S. Target's business involves enterprise AI software, holds a certain amount of U.S. user data, and its customers include U.S. federal government contractors. The analysis examines the three Chinese regimes, the CFIUS jurisdictional framework, and EAR export controls as they apply to this scenario, and then considers what the bilateral overlay means for transaction risk.

II. Presumptions of Functionality in Offshore Structures and Their Regulatory Limitations

The functions of the offshore intermediate layer in cross-border transactions can be understood at three levels. At the legal-form level, it enables the acquiring entity to be treated under the law of its place of incorporation as a separate legal person distinct from its Chinese parent company, thereby satisfying the appearance of being a "non-Chinese investor." At the

[1] Jupiter Out of Orbit: Court Grants Receivership in First Ever CFIUS Divestment Enforcement Litigation, Freshfields, July 2, 2026.

[2] United States v. Suirui Group Co., Ltd., Court Order Denying Motion for Stay, June 3, 2026, Civil Action No. 26-00369 (AHA).

regulatory-jurisdiction level, it seeks to characterize the transaction as one between a Singapore entity and a U.S. target, thereby arguing that China's foreign-investment security review, overseas-investment filing requirements, and the U.S. CFIUS's "country of concern" analysis of Chinese investors should not apply. At the operational-substantive level, it is accompanied by personnel relocation and contraction of domestic operations, seeking to weaken factual links to Chinese jurisdiction.

Recent regulatory practice demonstrates that formal incorporation and intermediary ownership do not, by themselves, determine the jurisdictional outcome. The applicable legal tests and the transaction's substantive connections must be assessed separately.

For instance, in the Manus case, the Foreign Investment Review Office did not specify the precise grounds for reversing the transaction. What can be confirmed from the text of the Measures for the Security Review of Foreign Investment is that Article 4 lists "important information technology and internet products and services" and "critical technology" as areas requiring proactive filing, and that the trigger is a foreign investor "acquiring actual control" of the investee. The Security Review Office deployed the most severe remedy available—prohibition plus revocation—against an offshore acquisition connected to technology developed in China, but the public notice does not establish which statutory trigger or factual findings the authority relied upon. Whether Article 4 applied, or any notification obligation was breached, cannot be determined from the notice alone. On the other hand, numerous lawyers and law firms contend that the transaction was prohibited primarily on the basis of a fundamental principle governing China's foreign investment security review: substantive scrutiny that overrides formalism. Specifically, Manus's core technologies, its core team, and its early-stage R&D achievements all originated within China; accordingly, the Foreign Investment Review Office may have characterized the transaction between overseas entities as a foreign investment that indirectly affects national security.[3][4][5]

The U.S.-side significance of Suirui/Jupiter lies in the survival of CFIUS's retrospective jurisdiction over non-notified transactions. The 2020 acquisition closed without CFIUS review;

---

[3] Measures for the Security Review of Foreign Investment (Order No. 37 of the NDRC and MOFCOM), arts. 2, 4, https://www.gov.cn/zhengce/2020-12/19/content_5712376.htm.

[4] She Huimin, "AI Going Global Must Not Cross Regulatory Red Lines," Economic Daily, May 4, 2026.

[5] Jincheng Tongda & Neal, Cai Jing & Chen Jiayue, "The Regulatory Logic of the Manus Case and Compliance Paths for Cross-Border Capital Operations of AI Companies."

CFIUS opened review in 2024; the President issued a divestment order in July 2025. The court's preliminary-injunction opinion confirms that the President's national security finding is unreviewable under 50 U.S.C. § 4565(e)(1), but that the government must still independently establish irreparable harm.[6] The core lesson is that closing does not produce finality, not that a Hong Kong subsidiary is per se ineffective.[7]

III. Relevant Reviews in China

(i) Security Review of Foreign Investment

The Measures for the Security Review of Foreign Investment regulate investments made by foreign investors in enterprises located within China. The Manus announcement raises questions about how authorities may assess transactions involving technologies and operations originating in China, but the published notice does not establish a general jurisdictional rule for all offshore acquisitions. In the scenario outlined in this paper, the key implication of this logic is that the Chinese parent company maintains "substantial R&D activities and a core technical team" within China—a potentially relevant factual connection, though not by itself a statutory trigger for foreign-investment security review. The target company is a U.S.-based entity, while the acquiring party is a Singaporean subsidiary; the applicability of China's foreign-investment security review must be established under its own jurisdictional requirements. Separately, the parties should examine whether the assets slated for acquisition—including the enterprise-level AI software technologies that will be integrated post-acquisition—substantively represent an extension or export of the Chinese parent company's technological capabilities. If the funds, personnel, or technologies employed by the Singaporean subsidiary in the acquisition originate from the domestic parent company, the presence of domestic elements becomes difficult to deny.

(ii) Oversight of Foreign Investments

The National Development and Reform Commission, in accordance with the Measures for the Administration of Overseas Investment by Enterprises (Order No. 11), subjects overseas investment projects to either approval or filing procedures. The competent commerce authorities are responsible for the filing or approval of overseas investments and for issuing

---

[6] Suirui, ECF No. 47, at 20–21 (citing 50 U.S.C. § 4565(e)(1)).

[7] The Manus Decision: China's First AI Security Review Block and Implications for Cross-Border AI Investment, May 6, 2026, Morgan Lewis & Bockius LLP.

certificates of overseas investment to enterprises, while the foreign exchange administration authorities handle registration and the remittance of funds abroad. In addition, a security review of overseas investment projects constitutes another mechanism distinct from the approval process for sensitive-category projects, primarily targeting overseas investments involving sensitive countries and regions or sensitive industries.

For the hypothetical transaction, the parties should assess whether the Singapore subsidiary's acquisition falls within China's outbound investment rules, taking account of the Chinese parent's control, funding arrangements, and the applicable filing or approval criteria. Whether an approval, filing, or foreign-exchange registration is required depends on the specific transaction and entities involved; these obligations should be confirmed before closing. Technology export controls require a separate analysis.

(iii) Export Controls on Technology

Technology export controls operate independently of the aforementioned investment review and approval regime. The Export Control Law and the Regulations on the Administration of Technology Import and Export govern the export of controlled items and restricted-category technologies, with no requirement that an "investment" be involved to trigger such controls. Moreover, the definition of technology export encompasses not only patent transfers and licenses but also "technical services and other forms of technology transfer." In the Manus case, the Ministry of Commerce's investigative assessment explicitly identified "export control" and "technology import and export" as distinct legal domains, highlighting a crucial distinction: acquiring a company (through an equity transaction) does not, by itself, constitute a technology export; however, if the transaction results in controlled technologies being "provided" to a foreign entity, it may independently trigger export control obligations. In the context of this article, the key issues to examine are whether the domestic core technologies of the Chinese parent company fall within the categories of restricted or prohibited technologies listed in China's Catalogue of Technologies Prohibited or Restricted from Export, and whether, following the acquisition, the Singaporean subsidiary or the U.S. target company will "obtain" these technologies through personnel collaboration, system access, or technological integration. If the answer is affirmative, export control obligations arise independently of ODI filing and national security reviews, thereby raising the issue of "deemed export."

(iv) Deemed Export

Even more far-reaching is the "deemed export" rule under the Export Control Law: when Chinese citizens or legal persons provide controlled items to foreign entities or individuals, such transfers are deemed exports, even if they occur outside China. Article 2 of the Regulations on the Export Control of Dual-Use Items reiterates and elaborates this framework, specifying that export control covers both "the transfer of dual-use items from within China to abroad" and "the provision of dual-use items by Chinese citizens, legal persons, and non-legal-person organizations to foreign entities and individuals," the latter category encompassing transfers—beyond commercial exports—that take the form of gifts, exhibitions, collaborations, assistance, or other means. This constitutes the substantive "deemed export" rule under Chinese law.

The provider of the controlled item must be a Chinese citizen, legal entity, or non-legal organization, regardless of where the activity takes place. The recipient is defined as a "foreign organization or individual." The term "provision" does not require physical cross-border transfer; it expressly encompasses intangible methods such as email transmission, cloud-based uploads, oral communication during meetings, visual presentations, and training or guidance. Even if access restrictions are imposed, uploading technical data to an overseas server may still be deemed an "export," because the operator of the foreign server objectively has the potential to gain access. Controlled items include goods, technologies, and services listed in the Dual-Use Items List, as well as technologies specified in the Catalogue of Technologies Prohibited or Restricted from Export by China. The parties should verify the currently effective version of the technology-export catalogue and any applicable approval or licensing rules before making a transfer; a change of corporate ownership is not, without more, proof that a regulated technology export occurred.[8]

In the context of this article, if, following an acquisition, a Singaporean subsidiary or a U.S.-targeted company employs Chinese-national core technical personnel who participate in AI software integration, model tuning, or system architecture decisions—activities that involve restricted technologies such as "data-driven personalized information-push services technology" listed in China's Catalogue of Technologies Prohibited or Restricted from Export—export licensing requirements may be triggered even in the absence of an explicit "technology transfer" contract. The particular risk of this mechanism lies in its opacity. Traditional transaction

[8] Yuzhou City People's Court, Henan Province, "The 'Deemed Export' Regime Helps Further Strengthen China's Technology Protection."

structures typically address explicit technology transfers by making "technology export approval" a condition precedent to closing; by contrast, deeming-as-export rules embed compliance obligations into the day-to-day operations of post-transaction integration, meaning that a deal that appears compliant at closing may, after closing, give rise to new compliance exposures due to personnel arrangements or modes of technical collaboration.[9]

The United States likewise faces the issue of "deemed export," which the author will discuss in Chapter Four.

(v) Data Export Issues

The fact that the target company "holds a certain amount of U.S. user data" requires careful analysis of its implications under China's framework for cross-border data transfers. The application of China's Measures for the Security Assessment of Cross-Border Data Transfers is contingent upon the "provision to overseas entities" of data collected and generated within China.

Data is the prerequisite. If the target company's U.S. user data is entirely collected and processed within the United States, and does not involve transmission to China or remote access by entities located in China, then the likelihood of triggering a direct assessment under China's data export regulations is relatively low.[10]

However, in the context of this paper, there are two indirect linkages that warrant vigilance. First, upon completion of the acquisition, if technical or managerial personnel of the Chinese parent company or the Singaporean subsidiary are granted remote access to the target company's data systems, regulatory practice may treat such access by an overseas entity to data stored within China as "data export" in itself. Even if the target data is hosted in the United States, should post-acquisition integration involve joint analysis or model training that combines U.S. data with existing data assets held by the domestic parent, the chain of data flows could become considerably more complex. Second, if the target company's AI software is integrated into the Chinese parent's product ecosystem following the acquisition and subsequently retrained or fine-tuned using data collected within China, subsequent

---

[9] Grandway Law Offices, "Cross-Border Transaction Practice 4: Technology Export Risk Prevention in Offshore Structuring—Lessons from the M Case," April 17, 2026.

[10] "Key Compliance Points for Cross-Border M&A by AI Companies: The Manus Acquisition," https://www.lexiscn.com/pghottopic/pg_ma/cn/pg_ma30.html#2.

data-processing activities could independently trigger assessment obligations. Consequently, the risk of data export is not a static issue that can be resolved once and for all prior to closing; rather, it is a dynamic risk that evolves in tandem with the implementation of post-transaction integration plans.[11]

IV. U.S. Side: TID Jurisdiction, Export Controls, and Supply Chain Security

(i) CFIUS Jurisdiction and Mandatory Filing

In the scenario presented in this article, the target company may qualify as a TID U.S. business, but that classification requires additional facts. First is the critical technology category: AI-related software or technology qualifies as CFIUS "critical technology" only if it falls within the applicable regulatory definition; being subject to the EAR alone is insufficient. Under CFIUS jurisdiction, it is not necessary for the target company to have already obtained an export license; rather, the requirement is that the technology "would require a license for export to the relevant parties." Second is the sensitive personal data category: the target company holds U.S. user data and its clients include federal government contractors. Under CFIUS rules, the scope of "sensitive personal data" encompasses information related to the security clearance status of personnel employed by government contractors, and the very act of "targeting products or services at intelligence, national security, or homeland security agencies or their personnel and contractors" constitutes an independent pathway for TID classification. Serving federal contractors does not, standing alone, establish that the target maintains sensitive personal data under the TID definition. There must be facts showing that the product or service is targeted or tailored to such entities or their personnel and contractors. The "more than one million individuals" threshold in § 800.241(a)(1)(i)(B) is a parallel pathway, not an alternative formulation of (A). Whether the target is a TID U.S. business therefore turns on (i) whether the AI technology is EAR-controlled critical technology; (ii) whether it targets or tailors to intelligence, national security, or homeland security agencies or their personnel and contractors, with data in a listed category; or (iii) whether the data-volume threshold is met. Federal contractor customers are not, by themselves, a sufficient condition for TID status.[12]

---

[11] "Key Compliance Points for Cross-Border M&A by AI Companies: The Manus Acquisition," https://www.lexiscn.com/pghottopic/pg_ma/cn/pg_ma30.html#2.

[12] M&A insight series: navigating complexity for tech general counsels, understanding CFIUS and recent regulations, from Mayer Brown.

The mandatory declaration required under 31 C.F.R. § 800.401 applies in two principal scenarios: First, the "substantial interest" scenario involving a foreign government (§ 800.401(b)): where a transaction results in a foreign person acquiring a "substantial interest" (typically 25% or more of direct or indirect voting rights) in a TID U.S. business, and where the national or local government of the single foreign government to which that foreign person is affiliated holds a "substantial interest" (generally 49% or more of voting rights) in that same foreign person. A key qualification in this category is the involvement of a foreign government's interest. For example, if the ultimate controlling shareholder of a Singaporean subsidiary is a Chinese parent company (a private enterprise), and the Chinese government does not hold 49% or more of the voting rights in that entity, then this scenario would not trigger the mandatory declaration requirement. Second, the critical-technology scenario (§ 800.401(c)): where a transaction involves a TID U.S. business engaged in the production, design, testing, manufacture, construction, or development of "critical technology," and where the relevant regulatory-authorization test is met for the specified transaction parties. Such specified persons include individuals who, through the transaction, could directly control the TID business, as well as those who have made a "covered investment." In this context, the critical qualification is the requirement for export-control authorization, rather than merely the "TID" nature of the activity. The CFIUS regulations expressly designate certain elements of the EAR license exceptions TSU, STA, and ENC as grounds for exemption from the mandatory declaration requirement—namely, if the export of the relevant technology to the designated parties can be effected under these license exceptions without necessitating an individual license, then the mandatory declaration may not apply.

Accordingly, in the context of this paper, the "acquisition of all shares of the U.S. TID entity" does not, by itself, automatically trigger a mandatory CFIUS filing obligation. Whether such a mandatory filing is triggered depends on: (1) whether any foreign government—specifically, the Chinese government—holds a "significant interest" in the ultimate controlling shareholder of the Singapore subsidiary; and (2) whether the target develops qualifying critical technology and the regulatory-authorization test is met for the relevant transaction parties. CFIUS jurisdiction and the mandatory declaration obligation are distinct issues at different levels: even if a mandatory filing is not triggered, CFIUS may still exercise voluntary review over "covered transactions."

CFIUS may also review covered transactions that were not notified before closing. The Suirui/Jupiter case illustrates the potential consequences of retrospective scrutiny.

(ii) Deemed Exports under the EAR and Post-Acquisition Integration Risks

15 C.F.R. § 734.13 defines "export" to include shipment or transmission out of the United States and "releasing or otherwise transferring 'technology' or source code (but not object code) to a foreign person in the United States" (a "deemed export").[13] Section 734.14 defines "reexport" to include shipment from one foreign country to another and "releasing or otherwise transferring 'technology' or source code subject to the EAR to a foreign person whose most recent country of citizenship or permanent residency is other than the foreign country where the release or transfer takes place" (a "deemed reexport").[14] BIS guidance confirms that a license is required for a deemed export or deemed reexport only if a license would be required for the actual export or reexport of the same technology to that foreign person's most recent country of citizenship or permanent residency.[15]

Three legally distinct scenarios must be separated in the present transaction:

First, actual transmission or transfer of controlled technology or source code to China. This is an "export" under § 734.13(a)(1) or a "reexport" under § 734.14(a)(1), and licensing depends on classification and destination. It is not a deemed export.

Second, release of controlled technology or source code to a Chinese national within the United States. This is the § 734.13 deemed export, fictively treated as export to China. Typical scenarios include Chinese engineers dispatched to the U.S. Target who can access controlled source code or technical data, or Chinese employees of the target granted access in the United States. Where Chinese technical personnel access U.S.-hosted controlled technology remotely from China, BIS enforcement practice may focus on substantive access rather than physical location, but the legal characterization is closer to export or reexport to China than to a strict § 734.13 deemed export; the parties should not assume that remote access necessarily falls within the deemed-export framework.

---

[13] 15 C.F.R. § 734.13(a)(2), (b).

[14] 15 C.F.R. § 734.14(a)(2), (b).

[15] BIS, Guidelines for Preparing Export License Applications Involving Foreign Persons (Deemed Exports/Reexports) § I, https://www.bis.doc.gov/index.php/documents/deemed-exports/709-guidelines-for-foreign-national-license-applications/file.

Third, release of controlled technology to a Chinese national outside the United States (e.g., in Singapore). Where that national's most recent country of citizenship (China) differs from the place of release (Singapore), this is a § 734.14 deemed reexport, not a § 734.13 deemed export.

If the post-closing integration plan expressly provides that the target's controlled technology stack will not be opened to Chinese nationals, that development remains in the United States and is conducted by U.S. citizens or permanent residents, and that the Chinese Parent acts solely as a financial investor without involvement in technology operations, the trigger conditions for deemed export and deemed reexport can be significantly reduced. China's "deemed export" rule is structurally asymmetrical: it anchors on a Chinese entity providing controlled items to an overseas recipient, irrespective of where the act occurs; the U.S. rule anchors on a release to a foreign person within the United States (or in a third country in the deemed-reexport variant), conditioned on whether the foreign person's country of nationality would itself require a license. The two regimes share an orientation toward knowledge-based control but differ in connecting factors and licensing logic; describing them as "symmetrical" obscures this difference.

V. Risk Reshaping and Limited Responses Under Regulation

(i) The Formation of the Convergence Effect

By juxtaposing the review frameworks on the Chinese and U.S. sides, one can discern a structure more complex than a mere "dual regulatory burden." Each side conducts its review independently, yet the combined effect is not simply an additive sum of risks; rather, the two systems reinforce one another through a mechanism of mutual evidentiary corroboration: China views the "Singapore Model" as a formal wrapper for the outward relocation of domestic factors, thereby bolstering the legitimacy of look-through scrutiny; meanwhile, Chinese regulatory actions might prompt additional questions about ownership and technology connections in a U.S. review, although this possible evidentiary interaction is not established as a general CFIUS practice. Following the Manus case, some law firms have highlighted this dynamic: restructuring "redistributes risk"—it does not eliminate risk but rather reallocates it across jurisdictions, with each side's regulatory assertions serving as leads for the other to take

action. Some analysts have termed this phenomenon "bilateral convergence," whose net effect is to "narrow the scope for designing compliant cross-border structures."[16]

In the context of this paper, the convergence effect implies that the more an architectural design seeks to project a "non-Chinese identity" through the Singapore-based layer, the more likely it is to trigger scrutiny on the Chinese side regarding potential circumvention intent; and a Chinese review might draw attention to the same underlying facts examined by U.S. authorities. Such an inference remains a hypothesis, not a demonstrated causal relationship.--

At the same time, the convergence observed in this paper is one of methodological orientation—emphasizing substance over form, and seeking to identify ultimate controllers and sources of technology—rather than a convergence grounded in regulatory frameworks. For the U.S., the CFIUS's regulatory focus centers on "foreign acquisition of control over U.S. businesses or covered investments," with the underlying legal interest being the protection of U.S. national security assets from foreign control. The Chinese regimes address different transactions and transfers under their respective legal criteria.

For China, the relevant inquiry differs across the applicable regimes: foreign-investment security review, outbound investment regulation, technology export controls, and data-transfer rules each have distinct statutory triggers. Technology origin and the location of personnel may be relevant facts, but they do not alone establish jurisdiction under every regime.

(ii) The Structural Erosion of Transaction Certainty

Traditionally, risk allocation in cross-border M&A has taken "closing" as the benchmark for risk transfer: prior to closing, the seller bears regulatory-approval risks, while after closing, the buyer assumes commercial and integration risks. The normalization of retrospective reviews fundamentally undermines this established benchmark. China's Measures on Security Review provide that unreported transactions may be ordered to "be restored to their pre-investment status," while the U.S. CFIUS's review of "non-notified transactions" and the five-year divestiture order in the Suirui case both indicate that closing no longer marks the end of regulatory risk exposure. In the scenario described herein, even after the buyer has paid consideration and completed equity closing, it still faces two distinct types of retrospective risks: China may, on grounds of security review or export controls, seek to invalidate all or part

[16] The Manus Decision: China's First AI Security Review Block and Implications for Cross-Border AI Investment, May 6, 2026, Morgan Lewis & Bockius LLP.

of the transaction's effects; the U.S., citing CFIUS post-review or enforcement of export control regulations, may demand divestiture or impose restrictions.[17]

This uncertainty has a structural impact on valuation. When the likelihood of retroactive deal cancellations or conditional restructurings cannot be reasonably estimated, traditional discounted cash flow models lose their reliable inputs. At the same time, the uncertainty itself drives up risk premiums, reducing the price buyers are willing to pay and thereby discouraging transactions that might otherwise have taken place. For sellers, if the buyer is the only bidder willing to bear the costs associated with China's regulatory review, the range of viable transaction options is already shaped by the regulatory framework.

(iii) Difficulties and Limits of Contractual Risk Allocation

At the contractual level, parties to a transaction can seek to make regulatory risks explicit and allocate them. Common tools include: conditioning closing on the completion of security reviews and CFIUS filings as well as customs clearance; incorporating price adjustments or termination rights triggered by changes in regulatory requirements; including specific representations in covenants regarding the origin of technology, data sources, and export control status; and establishing allocation mechanisms in indemnification clauses for losses arising from retroactive regulatory changes. While such arrangements are not without value, their limitations are equally apparent.

First, valuation adjustments and indemnity clauses are ill-equipped to address structural remedies such as "restoration to the pre-investment state." When regulatory requirements entail equity divestiture, technology segregation, or team separation—rather than monetary damages—the function of indemnity provisions is compensatory, whereas the remedy itself is restorative; the two operate on fundamentally different logical planes. Second, regulatory risks are both difficult to insure and hard to price. Regulatory outcomes associated with China's national security review or CFIUS fall outside the scope of standard M&A warranty insurance, making it challenging for buyers to transfer such risks through the insurance market. Third, the interests of sellers and buyers regarding regulatory risk are asymmetric. Sellers typically exit after closing and lack sustained incentive to bear the long-term risks of retrospective scrutiny, while buyers must internalize in the transaction price a risk they cannot control or accurately

[17] King & Wood Mallesons, "Regulatory Risk Allocation in Cross-Border Technology Transactions: When 'Completed' No Longer Means 'Finished'," May 9, 2026.

quantify. According to practical analysis by King & Wood Mallesons, for transactions involving sensitive technologies, "the preferable strategy is to identify national security risks at the outset, allocate those risks within the transaction documents, and steer clear of deals that could trigger excessively stringent regulatory scrutiny." This effectively acknowledges that the role of contractual mechanisms is limited to screening and pricing, rather than eliminating risk altogether.[18]

(iv) From Structural Segregation to Proactive Compliance Identification

If offshore structures cannot provide structural exemptions, the focus of compliance efforts should shift from "seeking safe harbors" to "proactive identification and substantive alignment." In the context of this paper, measures that carry practical significance include:

First, preliminary verification of the technology's origin and export control classification. Prior to initiating the transaction, conduct an EAR-based classification assessment of the target company's AI software technology stack to determine whether any software or technology is subject to control under an Export Control Classification Number (ECCN), and evaluate whether the post-acquisition technology integration plan would trigger reexport or deemed export licensing requirements. At the same time, review the core technologies held within the Chinese parent company in accordance with the Catalogue of Technologies Prohibited or Restricted from Export (中国禁止出口限制出口技术目录).

The Chinese parent should also classify its technology under the applicable Chinese export-control lists and technology-export catalogue, and assess whether planned collaboration would involve a regulated transfer. The purpose is not to eliminate all risk, but to identify potential authorization requirements and reflect them in the transaction structure and closing conditions.

Second, a thorough analysis of data flow pathways. This entails not only examining the storage and processing locations of the target company's U.S.-based data, but also assessing potential post-acquisition data access relationships—such as remote access to the target system by personnel within China, joint data-analysis arrangements, and the sources of retraining data for AI models. Any form of "cross-border access" should be brought within the scope of compliance assessments for outbound data transfers.

[18] Jupiter Out of Orbit: Court Grants Receivership in First Ever CFIUS Divestment Enforcement Litigation, Freshfields, July 2, 2026.

Third, the need for transparency in filing strategies. In CFIUS reviews, attempts to obscure Chinese affiliations by using a Singapore-based intermediary structure carry significant risks, particularly in light of the Suirui and Manus cases. A more viable approach is to disclose, in the filing, the ultimate control structure and the substantive role of the Chinese parent company, while also proposing verifiable mitigation measures—such as security-isolation arrangements, technical access controls, and the appointment of U.S. citizen security officers—to seek conditional approval rather than outright rejection. CFIUS practice demonstrates that conditional approval represents a more realistic exit strategy than litigation or post-transaction divestiture, and the federal courts' strong deference to CFIUS's national security determinations in the Suirui case further reinforces this conclusion.

Fourth, a prudent assessment of the "structural restructuring" strategy. Following the Manus case, some argued that thorough "de-China-ization"—including dissolving domestic entities, relocating teams, and segmenting markets—could circumvent jurisdiction. However, regulatory responses have made it clear: the substantive links among technology sources, data origins, and the core team cannot be severed through entity dissolution or personnel relocation. An analysis by Morgan Lewis explicitly states that contractual mechanisms such as entity dissolution, team relocation, and market segmentation do not eliminate regulatory risk; rather, they merely reallocate risk across jurisdictions while creating exposures on both sides. In the scenario described in this paper, if the Chinese parent company indeed maintains "substantial R&D activities and a core technical team," any structural design that seeks to formally sever these connections will not only struggle to secure a "non-Chinese" characterization on the U.S. side but may, on the Chinese side, be construed as evidence of an intent to evade regulation.

VI. Conclusion

Comparative scholarship supports a functional convergence between the Chinese and U.S. national security review regimes despite differences in legal design and institutional context. That literature describes convergence at the level of regulatory function and institutional orientation, not identity of legal elements.[19]

[19] Robin Hui Huang, China's National Security Review of Foreign Investment: A Comparison with the United States, 56 Vand. J. Transnat'l L. 1261 (2023) ("functional convergences despite some formal divergences"), https://scholarship.law.vanderbilt.edu/faculty-publications/1365/.

The “mutual evidentiary reinforcement” described in this paper—where one side’s jurisdictional assertion becomes a factual clue for the other side’s “China nexus” analysis—is the author’s analytical proposition, not a legal conclusion established in the literature. It is offered as an interpretive framework for understanding the overlay effect of bilateral review, not as an empirically verified regularity. The convergence observed here is methodological (substance over form; look-through to ultimate controllers and technology origin), not a convergence of normative baselines: the U.S. axis is foreign acquisition of control over a TID U.S. business or a covered investment; the Chinese axis is whether domestically formed technology, data, and teams have moved abroad without statutory procedures.

First, the Security Review Office publicly issued a decision prohibiting the Manus acquisition and requiring revocation, but the notice does not state the specific legal basis; the decision warrants examining technology origin and team location as possible relevant facts, without treating them as proven grounds of the decision, not in establishing a generally applicable look-through formula. Second, Suirui/Jupiter confirms that CFIUS retains retrospective jurisdiction over completed, non-notified transactions, and that courts afford substantial deference to the executive’s national security evaluation while still requiring an independent showing of irreparable harm; the initiation and form of relief remain case-specific rather than automatic. Third, U.S. mandatory declaration is not automatically triggered by acquiring a TID business; deemed export is confined to releases to foreign persons within the United States; and China’s “deemed export” rule anchors on provision of controlled items to overseas recipients, with different connecting factors and licensing logic from the U.S. rule.

The concept of mutual evidentiary reinforcement is offered as an interpretive framework: China may view the Singapore structure as a formal wrapper for outward migration of domestic elements, while U.S. reviewers may independently examine some of the same factual connections, so that the structure produces a signal-amplification effect rather than isolation. This proposition is explanatory, not an empirical description of coordination between the two regulators, and should not be read as asserting that the two substantive standards have converged. Methodological convergence is supported by the literature but must be qualified; normative asymmetry is the paper’s central comparative claim. For practitioners, the implication is sober: offshore structures may continue to serve financing, tax, and governance purposes, but they cannot be entrusted with a regulatory-isolation function; the task is not to design a structure that is not seen, but to ensure that when it is seen, the substantive relationships can be shown to be acceptable to both regulators.

References

1. “Manus Acquisition Review Rescinded: AI Going Global Enters an Era of Substantive Security Regulation?”, MaoFaTong, May 9, 2026.

2. “The Regulatory Logic of the Manus Case and Compliance Paths for Cross-Border Capital Operations of AI Companies,” Jincheng Tongda & Neal, Aug. 26, 2026.

3. Freshfields, “Jupiter Out of Orbit: Court Grants Receivership in First Ever CFIUS Divestment Enforcement Litigation,” July 2, 2026.

4. U.S. Department of Justice, “Justice Department Files Action to Protect National Security by Enforcing President’s Order of Chinese Company’s Divestment from U.S. Company,” Feb. 10, 2026.

5. Morgan Lewis, “The Manus Decision: China’s First AI Security Review Block and Implications for Cross-Border AI Investment,” May 6, 2026.

6. Liu Boyuan & Wang Jing, “Retrospective Review: The Battle for ‘Transaction Certainty’ in Cross-Border M&A,” MaoFaTong, June 18, 2026.

7. “Regulatory Risk Allocation in Cross-Border Technology Transactions: When ‘Completed’ No Longer Means ‘Finished’,” King & Wood Mallesons, May 9, 2026.

8. “Grandway Observations | Cross-Border Transaction Practice 4: Technology Export Risks in Overseas Structuring from the M Case,” Grandway Law Offices, Apr. 17, 2026.

9. “Grandway Observations | Cross-Border Transaction Practice 5: Cross-Border Data Transfer Risks in Overseas Structuring from the M Case,” Grandway Law Offices, May 13, 2026.

10. “AI Companies ‘Via Singapore’ Going Global Still Face Multiple Regulatory Tests in China, Singapore, the U.S., and Europe,” ALB China, Mar. 26, 2026.

11. Cleary Gottlieb, “Sensitive Personal Data and TID U.S. Business under CFIUS Regulations.”

12. Mayer Brown, “Navigating Complexity for Tech General Counsels: Understanding CFIUS and Recent Regulations.”

13. 31 C.F.R. Part 800 (July 9, 2026 version), §§ 800.241 (sensitive personal data), 800.248 (TID U.S. business), 800.249 (transaction definition), eCFR, https://www.ecfr.gov/on/2026-07-09/title-31/subtitle-B/chapter-VIII/part-800.

14. 31 C.F.R. Part 850 (OISP Regulations), eCFR, https://www.ecfr.gov/current/title-31/subtitle-B/chapter-VIII/part-850.

15. Measures for the Security Review of Foreign Investment (Order No. 37 of the NDRC and MOFCOM), effective 2021.

16. U.S. Department of the Treasury, “Treasury Announces Enforcement Penalty for Violation of Outbound Program,” Oct. 7, 2026.

17. Bureau of Industry and Security, U.S. Department of Commerce, “Guidelines for Preparing Export License Applications Involving Foreign Persons (Deemed Exports/Reexports),“ https://www.bis.doc.gov/index.php/documents/deemed-exports/709-guidelines-for-foreign-national-license-applications/file.

18. Robin Hui Huang, “China's National Security Review of Foreign Investment: A Comparison with the United States,” 56 Vand. J. Transnat'l L. 1261 (2023), https://scholarship.law.vanderbilt.edu/faculty-publications/1365/.

19. She Huimin, “AI Going Global Must Not Cross Regulatory Red Lines,” Economic Daily, May 4, 2026.