FRESHFIELDS

June 2026

Foreign Investment Monitor

ISSUE 12

Contents

Executive summary

Regulators are not only focused on who is investing. They are asking what the investment enables: what it controls, what critical systems it touches and what strategic influence it gives rise to.

This edition of *Foreign Investment Monitor* examines key FDI developments shaping the global investment landscape, including:

1. **Digital infrastructure: Data centers enter the security frame**
   As AI and cloud demand accelerates, data centers are being reassessed as strategic infrastructure. For investors, FDI risk now turns on data access, control and resilience.

2. **Crossroads for media deals: Plurality, foreign ownership and regulatory scrutiny**
   Media transactions are attracting increased, multi-layered scrutiny as European governments reassess who controls news, information and public discourse.

3. **From screening to structuring: FDI risk reshapes M&A deal terms**
   Foreign investment controls are no longer just a customary regulatory condition to closing. In sensitive cross-border M&A, they now influence price, timing, remedies and contractual risk allocation from the outset.

4. **CFIUS: Is the Known Investor Program the golden ticket for investors?**
   The Treasury's proposed KIP points to a more efficient CFIUS for repeat, low-risk investors, but its value will depend on whether it delivers meaningful procedural advantages.

5. **Japan builds its CFIUS: Broader scope, deeper scrutiny**
   Japan is tightening foreign investment review, but the more significant change is institutional. A regime once focused on formal filings is becoming more substantive, intelligence-led and security-driven.

6. **Austrian FDI: Managing heightened scrutiny, Phase II proceedings and policy shifts**
   Active enforcement and broader interpretation of sensitive sectors underscore an evolving European landscape of increasingly interventionist investment screening.

The question is no longer simply whether a transaction can be cleared, but how it will be assessed against national policy priorities.

Digital infrastructure: Data centers enter the security frame

In brief

Data centers now sit at the center of the digital economy. They support cloud services, AI, financial infrastructure and essential public functions. That role is changing how regulators assess foreign investment in the sector. Screening authorities are looking beyond land, power and physical infrastructure to the functions data centers enable: access to sensitive data, resilience of essential services and concentration of critical processing capacity. Approaches differ across jurisdictions. Europe is moving towards broader scrutiny of digital infrastructure, the US remains comparatively open to passive investment and China retains broad discretion to intervene where national security concerns arise.

> Data centers are assessed less as real-estate or energy-intensive assets and more as nodes within a broader digital ecosystem.

Data centers were once viewed, from a transaction perspective, as infrastructure assets. They required land, power, cooling, capital and long-term customers. They still do. But the regulatory lens has changed.

As demand for cloud services, AI and data-intensive applications accelerates, data centers are becoming more than physical facilities. They are control points in the digital economy. They determine where data sits, who can access it, how resilient essential services are and how dependent a jurisdiction becomes on foreign-owned infrastructure.

That shift matters for foreign investment review. Screening authorities are increasingly asking not only who owns the asset, but what the asset enables. The answer can bring data center investments within scope even where data centers are not expressly listed as protected assets in the relevant legislation.

Data as a strategic resource

Recent FDI enforcement practice reflects a shift toward a function-based assessment of data centers. Rather than focusing on their formal characterization as physical infrastructure, screening authorities are examining whether an investment confers the ability to influence data-dependent activities that may give rise to security, resilience or public-order risks. In this context, data centers are assessed less as real-estate or energy-intensive assets and more as nodes within a broader digital ecosystem.

In practical terms, scrutiny tends to focus on access, control and availability. Authorities may examine whether an investor's ownership stake, governance rights or operational role could affect sensitive datasets, including personal data, government or emergency services data, or commercially critical information. They may also consider concentration risk, particularly where disruption or misuse could impair essential digital services.

This reconceptualization of data as a strategically sensitive resource has enabled data center transactions to fall within the scope of existing FDI screening regimes even where data centers are not expressly listed as protected assets in some legislation.

Europe moves towards digital infrastructure scrutiny

In the EU, these developments coincide with a significant overhaul of the FDI screening framework. In May 2026, the European Parliament approved a revision of Regulation (EU) 2019/452. The reforms seek to strengthen and harmonize national screening regimes, deepen cooperation between Member States and the European Commission and expand the minimum mandatory scope of review, including by identifying "digital infrastructure" as an area of strategic relevance. Some Member States have already moved to strengthen controls of data center-related investments. Others have already closed, or are moving to close, potential review gaps. The direction of travel is visible across Europe; the Netherlands, Germany and the UK offer three useful examples of how selected jurisdictions are already strengthening, or preparing to strengthen, scrutiny of data center-related investments.

The Netherlands

The Netherlands, which hosts a significant concentration of data centers and is regarded as one of the larger data center hubs in Western Europe, imposed a mandatory notification requirement in October 2020 for certain data center transactions. This includes acquisitions of 30% or more of the voting rights in data centers with a minimum installed capacity of 50 MW, as well as providers of data center services to critical government authorities. The regime is notable because it does not provide an exemption for domestic or EU investors: the filing obligation applies irrespective of the acquirer's origin.

Under the Dutch investment screening regime, there are currently no publicly known prohibition decisions or remedies imposed relating to data center acquisitions. But the wider policy environment is restrictive. In 2022, the Dutch government introduced a nationwide moratorium on new hyperscale data centers with a capacity of 70 MW or more. That moratorium operates alongside increasingly stringent spatial planning rules, which significantly limit the location and development of new data center facilities. In parallel, the government has identified digital autonomy as a strategic priority, reflecting a broader objective to safeguard Dutch and European control over critical digital infrastructure and reduce reliance on non European technology providers.

> "Screening authorities are looking beyond land, power and physical infrastructure to the functions data centers enable: access to sensitive data, resilience of essential services and concentration of critical processing capacity.

Germany

Germany has been screening investments in data centers with a minimum installed capacity of as little as 3.5 MW for several years. It is also pursuing a similar strategic objective through its policy on digital sovereignty. Its Digital Strategy 2025 seeks to reduce dependencies on technologies from the US and China and ensure that Germany has the capability to develop and train AI models on domestic infrastructure. To this end, the government intends to make substantial public investments in AI and cloud technologies, with the aim of fostering a sovereign, end-to-end domestic technology stack.

Beyond investment screening considerations, the regulatory requirements for data center operators have tightened significantly following Germany's implementation of the EU NIS2 Directive and the EU Directive on the Resilience of Critical Entities. These laws create a dual framework. The KRITIS Umbrella Act focuses on physical security, requiring operators to conduct risk assessments, prepare resilience plans and implement technical measures such as access controls and resilient power supplies. Operators must also register critical facilities and report significant physical incidents.

In parallel, the NIS2 Implementation Act targets cybersecurity. It requires operators to manage digital risks, secure their supply chains, and adhere to strict reporting deadlines for cyber incidents, often starting within 24 hours. The result is a more comprehensive responsibility for both the physical and digital security of their infrastructure, coupled with direct compliance accountability at senior management level.

The UK

In the UK – the largest data center hub in Western Europe – data centers (and associated data infrastructure) are currently caught by the FDI regime only if they provide services directly or indirectly to certain public sector authorities. However, Ministers are now moving to close that gap: proposed reforms will bring all third-party-operated data centers within scope of the regime either later this year or in early 2027.

The direction of Europe is therefore clear. Data center investment is increasingly assessed through a sovereignty and resilience lens. FDI screening is one part of that picture, but it is not the whole story.

The US remains open, but structure matters

The US presents a somewhat different picture. Data center investment has been subject to fewer investment policy and regulatory constraints, and the current administration has been explicit about attracting that capital into the sector, particularly from government-linked investors. That openness, however, should not be mistaken for a relaxed CFIUS environment.

Digital infrastructure: Data centers enter the security frame

During his May 2025 Middle East trip, President Trump announced a $20bn Saudi-backed investment in US data centers and energy infrastructure, following a pre-inauguration announcement of a comparable $20bn commitment from Emirati developer DAMAC Properties. This openness reflects the scale of investment required. A McKinsey analysis suggests that by 2030 roughly $2.8tn will be deployed into US data center infrastructure, a level of investment likely to require foreign capital alongside domestic financing.

The link between data center build-out, technological competitiveness and national security is clear. The question is whether CFIUS timing, process risk and mitigation could chill that capital at a critical moment. The administration's policy framework suggests a more permissive posture. The America First Investment Policy expressly welcomes passive investment, including from sovereign wealth funds. Executive Order 14318 establishes an expedited pathway for large-scale data center projects without adding new foreign investment restrictions. At the same time, the administration has shown a lower appetite for mitigation, including by revisiting agreements reached during the prior administration.

> "For data center investors, the central question is no longer simply whether an asset is in scope of an FDI regime; it is whether the transaction gives the investor a role in the digital systems on which governments, businesses and citizens increasingly depend.

CFIUS scrutiny remains strict where a transaction gives a foreign investor control, governance rights, information access or operational influence over assets that may implicate sensitive data, critical infrastructure or government-linked customers.

The practical implication is straightforward. Transactions should be structured to align with the administration's preference for passivity. Investors should avoid governance or information rights that are not essential to the investment thesis and should be cautious about accepting rights that trigger CFIUS concerns where they are not needed. Early engagement with CFIUS can further reduce friction by framing individual transactions within a broader and credible investment strategy.

Asia growth brings a wider security question

Asia is experiencing a data center boom, driven by AI workloads, cloud adoption, 5G rollout and hyperscale expansion. Major hubs include China, India, Japan, Korea and Singapore, while several emerging Southeast Asian markets, including Indonesia, Malaysia, Philippines, Thailand and Vietnam, are also experiencing significant growth. For a closer look at the execution issues shaping Japanese data center transactions, see our recent analysis on Japan's data center execution test.

The regulatory picture is not uniform. Some markets are actively seeking capital and infrastructure capacity. Others are tightening controls around data, cybersecurity, foreign ownership, critical infrastructure and national security. Investors therefore need to assess not only whether a filing is required, but whether the transaction sits within a broader technology or industrial policy concern.

China illustrates the point. Digital and intelligent development, underpinned by computing power, algorithms and data, is a key pillar of China's national strategy. Although data centers are not expressly mentioned as a sector captured by the Chinese national security regime (NSR), they are plainly relevant to areas of broad strategic interest, including AI, digital transformation, data analytics and digital markets.

To date, there have been no publicly reported interventions targeting foreign investment in data centers in China. However, NSR jurisdiction is broad, and the Chinese authority has wide discretion to intervene where foreign investment is perceived to threaten national security. Recent enforcement under the regime shows that the Chinese authority is increasingly tightening controls on FDI in the AI sector. Given that data centers are essential infrastructure for AI, foreign investors considering data center investment in China should conduct rigorous and early risk assessment.

Looking ahead

For data center investors, the central question is no longer simply whether an asset is in scope of an FDI regime; it is whether the transaction gives the investor a role in the digital systems on which governments, businesses and citizens increasingly depend.

- FDI authorities increasingly assess data center investments by reference to the functions they enable. Scrutiny is focused on access to, control over and the resilience of data-dependent activities, including whether a transaction could affect sensitive data flows, essential digital services or system-wide resilience within a jurisdiction (rather than only the traditional national-security, public-order or supply-chain concerns).
- Deal structure plays a material role in how regulators assess risk and intent. Meaningful information rights and operational involvement are treated as indicators of influence capable of triggering regulatory concern. As a result, minority or non-controlling investments warrant the same early screening analysis as controlling acquisitions, especially where they involve access to sensitive data.
- Approaches remain jurisdiction-specific. The EU is moving rapidly toward stricter, broader and more harmonized screening of digital infrastructure investments. The US environment remains comparatively permissive, particularly where investments are structured as passive. In China, investments are generally feasible but fall within the scope of a discretionary national security review regime, making careful upfront risk assessment essential.
- Taken together, this means that early and deliberate calibration of ownership, governance, information and operational rights - anchored in a clear investment rationale - can materially influence whether a transaction is reviewed, the depth of scrutiny applied, and the risk of delay, conditions or ongoing compliance obligations.

With thanks to Freshfields Ninette Dodoo, Uwe Salaschek, Colin Costello, Ruzica Ciric, Iona Crawford and Max Immerzeel for their contributions to this update.

Crossroads for media deals: Plurality, foreign ownership and regulatory scrutiny

In brief

Government scrutiny of media mergers is intensifying across Europe. Media assets have long been treated as strategically important – shaping democracy, public opinion and national identity – but concerns over social media, AI-generated content, foreign interference, ownership concentration and the financial fragility of local news have pushed the issue higher up political and regulatory agendas. The result is a more complex regulatory deal environment, with transactions increasingly exposed to overlapping national and supranational merger control, FDI, and sector-specific reviews, including the new European Media Freedom Act. Recent transactions show that the impact is not limited to formal prohibition: political attention, post-closing scrutiny, stakeholder pressure and uncertain review pathways can all shape deal execution.

A series of high-profile transactions – and the political and popular debates they have ignited – has pushed control of media, especially by foreign or state-backed investors, firmly back up political and regulatory agendas.

The result? A reshaped landscape for media transactions across Europe with new and expanded media plurality, merger control and FDI regimes. Even if deals may ultimately be cleared, media groups and investors must now plan for more intrusive, complex and politically charged reviews, often involving multiple regulators, overlapping legal tests and uncertain timelines.

The regulatory landscape

European governments do not rely on the same type of frameworks to scrutinize media mergers, nor do they necessarily rely on only one. Transactions may therefore face simultaneous merger control, including specific media tests, FDI and sector-specific media reviews, with overlapping remedies and approval timelines.

Frameworks vary considerably at the national level. Some jurisdictions operate specific media plurality regimes, with distinct sector-specific rules, as is the case in France, Germany and Italy, where filing obligations arise when certain revenue and market or viewer share thresholds are met.

Beyond dedicated media plurality regimes, many jurisdictions such as Spain, Germany and France have designed FDI regimes specifically to capture media activities, while the UK has recently introduced a Foreign State Intervention (FSI) regime aimed at addressing concerns around foreign state involvement in media ownership.

> “Transactions may therefore face simultaneous merger control, including specific media tests, FDI and sector-specific media reviews, with overlapping remedies and approval timelines.

Other countries address plurality concerns through the merger control framework itself, including Austria and the UK. For a transaction to fall within the UK’s Public Interest Intervention Notice (PIIN) regime, it must meet the merger control filing thresholds but below-threshold mergers can be caught by the Special Public Interest Intervention Notice (SPIIN). Thresholds are equally varied: some regimes can be triggered by minority stakes, board rights or significant influence falling short of majority control.

A more significant structural shift is taking place at EU level. For the first time, the European Media Freedom Act 2023 (EMFA) introduces a common EU framework for assessing media market concentrations through the lens of media pluralism and editorial independence.

Subject to the required implementation laws at EU Member State level, national

regulatory authorities are now required to conduct mandatory impact assessments of qualifying media mergers, complementing – but not replacing – standard competition law review. They can then request that the European Board for Media Services (the Board) issue an opinion, or the Board may do so proactively where a media transaction is likely to affect the functioning of the internal market. These opinions are non-binding, but should carry significant normative weight and influence national decisions.

EMFA's scope is deliberately broad, with "media" covering television and radio broadcasters, on-demand audiovisual media services, audio podcasts, press publications, providers of online platforms granting access to media content, as well as providers of video-sharing platforms or very large online platforms exercising certain editorial responsibility. Notably, only one party to a transaction's activities need to fall within this definition for the framework to apply.

Implementation progress has, however, been uneven with only a limited number of Member States having completed full implementation, Finland being one example. Austria has recently amended its existing media merger regime to implement the EMFA. Many Member States are still aligning domestic legislation with their EMFA obligations. Germany is developing a Digital Media State Treaty to implement it, which is expected to deviate significantly from the current media regime, while the Commission on Concentration in the Media (KEK) is expected to retain a central role. Italy's Communications Regulatory Authority (AGCOM) and France's Audiovisual and Digital Communication Regulatory Authority (ARCOM) are also moving towards implementation. Other Member States are further behind in their implementation journey.

Against this backdrop, the evolving landscape creates a period of regulatory flux that deal practitioners must navigate carefully.

> At EU Member State level, national regulatory authorities are now required to conduct mandatory impact assessments of qualifying media mergers, complementing – but not replacing – standard competition law review.

Remedies?

For transactions subject to review – whatever the applicable framework(s) – remedies may in some cases be required in order to address a range of potential concerns.

1. **Editorial and governance remedies** to safeguard independence. These may include independent editorial boards, editor lock-ins to prevent post-acquisition changes in editorial direction, guarantees to maintain a certain number of journalists and independence charters.
2. **Strategic and operational remedies** to address sovereignty concerns. These may include retaining domestic headquarters, server localization and local content quotas.
3. **Structural and economic remedies** to target plurality directly. Such remedies may include divestments of overlapping assets and enhanced transparency of ownership structures.

Media mergers in the spotlight

Recent transactions illustrate the unpredictable and politically charged environment in which media deals now proceed.

Hungary - Ringier Hungary

The acquisition of Ringier Hungary Kft., publisher of Blikk, one of the most widely read daily newspapers in Hungary, by Indamedia Network Zrt. resulted in the first EMFA opinion in April 2026. Indamedia is one of the largest players in the Hungarian media market that was considered to have close ties to, and be aligned with, the previously ruling party Fidesz and former Prime Minister Orbán. The Acquisition had was initiated and closed Orbán and the Fidesz party were still in power. At that time, the media Council did not conduct a national-level assessment and did not consult the Board, upon which the Board stepped in proactively. It concluded that the concentration posed risks to media pluralism and editorial independence, citing increased capacity to influence public opinion and further consolidation of Indamedia's dominant position in online news.

Crossroads for media deals: Plurality, foreign ownership and regulatory scrutiny

The Board determined that, despite being primarily domestic, the acquisition would likely affect the internal market for media services, as the merged group would reach a large share of Hungarian print and digital audiences in an already highly concentrated market, further disadvantaging independent and foreign media.

Since then, the Hungarian Competition Authority (GVH) picked up the transaction post-closing by exercising its below threshold call-in powers. It claimed this was on the basis of having received a complaint regarding the accuracy of previously received information and clarified that it could only assess the merger's impact on competition, whereas the diversity of media sources was the responsibility of the national media authority.

Italy - GEDI

Antenna Group, the Greek media conglomerate owned by the Kyriakou family, completed its acquisition of GEDI from Exor, the Agnelli-Elkann holding company, in March 2026, gaining control of *La Repubblica* newspaper alongside a broad portfolio of digital and radio assets.

The transaction was strategically simplified upfront by a separate agreement to sell *La Stampa* to Italian publishing group SAE. At a national level, based on public information the deal did not appear to have triggered filing obligations with either the Italian Competition Authority (AGCM) or the Italian Authority for Communications (AGCOM), and it is unclear whether Italy's Golden Powers FDI regime was formally invoked.

Both AGCM and AGCOM can nonetheless still be assumed to have considered the transaction, given their respective roles. The acquisition also sparked fierce political debate, calls for employment and editorial safeguards and sustained newsroom resistance including ongoing strikes. Notably, despite Italy's EMFA transposition still being in progress, there were reports, apparently based on submissions from *La Repubblica* journalists, that the GEDI acquisition could have been among the first transactions reviewed by the Board under EMFA's new media plurality framework.

The UK - The Telegraph

The Telegraph sale is a clear example of the regulatory risks affecting media transactions. Political sensitivity and prolonged scrutiny demonstrate how these factors can shape deal outcomes. Since October 2023, four successive bidders have attempted to acquire the newspaper, the majority encountering multi-layered regulatory reviews. An initial bid by RedBird IMI, a joint venture between US private equity firm RedBird Capital Partners and International Media Investments – a UAE-backed media group – was blocked by the introduction of the FSI regime.

The FSI regime was specifically designed and introduced to prohibit foreign state ownership of national newspapers, in light of the proposed RedBird / IMI transaction. A revised RedBird structure was devised but subsequently abandoned in late 2025 after protracted delays generated significant reputational attrition. DMGT, the Daily Mail's owner, then agreed a deal in November 2025. However, the deal faced intervention by the Secretary of State under a PIIN and the prospect of an in-depth competition and media plurality reference in February 2026 to assess whether the planned acquisition would have reduced the plurality of persons with control of newspaper enterprises serving specific audiences.

In March 2026, German publisher Axel Springer displaced the DMGT bid and the Secretary of State confirmed she was not minded to intervene under either the UK's public interest media or FSI regimes.

Looking ahead

Several practical conclusions emerge from the current environment:

- **Cross-border media deals face heightened scrutiny, even where the regulatory outcome remains unresolved.** Governments, regulators and stakeholders are paying closer attention to media ownership, particularly where foreign, state-linked or non-EU investors are involved. The risk is not confined to formal prohibition: process uncertainty, political pressure, post-closing review and reputational impact can all affect transaction strategy.
- **EMFA adds a new supranational layer, but its practical effect is still developing.** The first cases suggest that the European Board for Media Services may be willing to engage where national assessment is absent or incomplete. But national implementation remains uneven, and the relationship between EMFA, domestic plurality regimes, merger control and FDI review will need to be tested in practice.
- **The regulatory ecosystem is converging in some areas, but enforcement tone, political appetite and national implementation vary considerably.** That creates meaningful jurisdictional uncertainty, particularly for transactions involving media assets with public-interest sensitivity or cross-border ownership structures.
- **Successful transactions will be built on early risk mapping and proactive engagement.** Parties should identify potential plurality, editorial independence, foreign ownership and public-interest concerns at the outset, and engage regulators and key stakeholders early. In sensitive deals, commitments to plurality and editorial independence should form part of the transaction rationale, not appear as concessions extracted late in the process.

With thanks to Freshfields Geronimo Benedict and Iona Crawford for their contributions to this update.

From screening to structuring: FDI risk reshapes M&A deal terms

In brief

Foreign direct investment regimes have moved from the edge of cross-border M&A to the center of deal execution. As screening regimes expand, the central question is increasingly not only who is buying, but what is being bought. Targets with sensitive technology, data, government customers, critical supply chain roles or links to public functions can trigger intensive scrutiny, even where the investor itself appears low-risk. For dealmakers, the implications are practical and immediate. Long-stop dates, conditions precedent, cooperation obligations, "hell or high water" clauses, reverse break fees, warranties and post-closing covenants all need to reflect the realities of FDI review.

Foreign direct investment controls have changed the mechanics of cross-border M&A. They have not simply added another filing to the transaction checklist. They have fundamentally redrawn the strategic calculus of deal structuring, negotiation and contractual draftsmanship.

This shift reflects a broader change in screening practice. FDI regimes are proliferating, existing regimes are being reinforced and regulators are interpreting sensitive sectors more broadly. The traditional focus on investor identity remains important, particularly where the buyer has state links or connections to jurisdictions of concern. But the dominant question is increasingly asset-led: what is being acquired, what does it enable and what would happen if control passed to a foreign investor?

That matters because the perimeter of sensitivity has widened. Technologies, data, supply chain position and proximity to state functions can all determine the intensity of scrutiny. Sectors such as biotechnology, AI, critical raw materials and food security now sit alongside more established categories such as defense, energy and telecoms. In the EU, this direction of travel is clear: the revised FDI Screening Regulation makes national screening mechanisms mandatory across Member States, establishes a minimum harmonized scope of review and extends scrutiny to EU-based investors ultimately controlled by non-EU entities. The shift is already visible in practice. FDI notifications across the EU increased by nearly 75% in 2024, and the revised framework is likely to add further pressure to an already active screening environment.

For M&A practitioners, the consequence is immediate. Where the target touches a strategic domain, FDI risk must be built into the deal architecture from the start. It affects timetable, conditionality, remedies, termination rights and post-closing integration. In sensitive transactions, the SPA is no longer just documenting commercial agreement, it is allocating national security risk.

FDI is now a deal strategy question

A reactive approach to FDI is increasingly untenable. Transactions can fail not because the underlying commercial logic is weak, but because the parties underestimate the regulatory terrain, engage too late or fail to explain the transaction in terms the authority can accept.

That requires a different approach from merger control. FDI regulators are government entities, and their analysis is increasingly shaped by security, political sensitivity, industrial policy and strategic dependance. The timing and content of engagement therefore need to be calibrated accordingly.

> Where the target touches a strategic domain, FDI risk must be built into the deal architecture from the start.

The first step is a detailed initial risk assessment. This should map the target's technologies, intellectual property, customers, government and defense contracts, supply chain role,

data flows and links to critical infrastructure. It should also identify whether any limited activity, product line, customer relationship or dataset could change the regulatory analysis.

That point is often decisive. FDI review does not always tolerate a de minimis approach. In competition analysis, a small revenue stream or limited market overlap may be peripheral. In FDI, one sensitive contract, technology or dataset can change the risk profile of the entire transaction.

Early assessment also shapes the regulatory narrative. The parties should anticipate the questions screening authorities are likely to ask and prepare credible answers before the review begins. Where potential concerns are identifiable, mitigation should be considered early. The most sophisticated dealmakers no longer wait for regulators to define the problem, they test which safeguards may be needed, whether those safeguards are commercially acceptable and how they can be framed as proportionate responses to specific risks.

The judgment is delicate. Too little mitigation may increase the risk of delay, escalation or prohibition. Too much may erode the commercial value of the deal. In the most sensitive transactions, the negotiation effectively takes place on two fronts: with the counterparty and with the state – and requires both legal rigor and commercial creativity.

Turning regulatory risk into contract terms

The results of that FDI assessment must then be reflected in the contractual documentation. This is where the policy shift becomes concrete.

Long-stop dates are often the first pressure point. FDI reviews can be unpredictable, particularly in multi-jurisdictional transactions where reviews may run sequentially or where one's authority's concerns influence another's. Political attention can also extend timelines beyond the formal statutory process. In complex cross-border deals, long-stop dates of 12 to 18 months are no longer unusual, and even those may prove insufficient in highly sensitive cases.

> "The judgment is delicate. Too little mitigation may increase the risk of delay, escalation or prohibition. Too much may erode the commercial value of the deal.

The drafting must account not only for the formal statutory timelines, but also for pre-notification engagement, information requests, remedy discussions and 'stop the clock' delays. In jurisdictions such as the US, pre-filing engagement can materially extend the process in high-stakes transactions. An aggressive long-stop date may look attractive at signing, but it can become a false economy, creating artificial pressure that weakens regulatory strategy and forces the parties to abandon an otherwise viable transaction.

Conditions precedent need precision. The SPA should identify all FDI clearances required before closing. But the exercise does not end with mandatory filings. In some cases, conditions should also cover voluntary filings or potential call-in risk, where an authority can review a transaction that was not mandatorily notifiable but may raise national security concerns. Where post closing intervention could lead to unwinding or intrusive remedies, prudent parties may decide that closing certainty requires resolving that risk before completion.

Cooperation obligations require equally careful drafting. FDI authorities often request sensitive details about the buyer (and its direct or indirect shareholders) and the target. The buyer needs enough information to satisfy its regulatory obligations, while the seller needs to protect the commercially sensitive material before closing. Counsel-to-counsel and regulator-only disclosure mechanisms can manage that tension, allowing sensitive material to reach the authorities without passing through the counterparty's commercial team. The position can be complicated where a state-owned enterprise buyer is not prepared to divulge certain information to worldwide FDI regulators. This constraint should be clearly addressed in the transaction documents and may introduce additional risk for the seller, albeit one that is often non-negotiable.

"Hell or High Water" clauses have become one of the most contested issues in FDI-sensitive deals. A traditional commitment requires the buyer to accept any remedies needed to obtain clearance. That is increasingly difficult in the FDI context, where remedies can be less predictable and more intrusive than antitrust remedies. On the other hand, FDI regulators often show greater flexibility towards behavioral remedies than their merger control counterparts, underscoring the need to distinguish between these regimes when negotiating such commitments.

From screening to structuring: FDI risk reshapes M&A deal terms

> FDI risk is not just something to clear. It is something to price, allocate and draft for.

Potential (largely behavioral) FDI remedies may include structural separation, restrictions on management involvement, exclusion of certain critical shareholders or limited partners, limits on technology or data access, IT segregation, localization commitments, investment obligations or constraints on future governance. Some may directly undermine the strategic rationale for the acquisition. Buyers are therefore less willing to sign open-ended commitments.

As a result, more transactions use limited or commercially reasonable efforts standards, often combined with negotiated remedy caps. These caps define the maximum burden the buyer is prepared to accept, whether financial, operational or structural. Their value lies in forcing the parties to confront FDI risk at signing, rather than after the regulator has already framed the risk.

Reverse break fees may help where parties cannot agree on remedy obligations. A fee, payable by the buyer if the transaction fails for lack of FDI approval, compensates the seller for delay and opportunity cost, while giving the buyer an economic incentive to pursue approval. The amount will depend on the perceived clearance risk, the buyer's control over the regulatory outcome and the commercial value of the transaction.

Warranties also need to become more FDI-specific. Standard representations may not be enough where the target operates in sensitive areas and where the target's activities often determine where a mandatory filing is required. The SPA may need targeted warranties covering government and defense contracts, dual-use technologies, classified programs, export-controlled items, sensitive data, critical infrastructure, supply chain dependencies and prior engagement with national security authorities. A disclosure gap in this context is not merely a diligence issue. It may lead to unexpected filings, delay, remedies or refusal of clearance.

Post-closing covenants are just as important where remedies are likely. FDI commitments can affect integration planning, IT migration, data access, governance, supply arrangements, intellectual property transfers and cross-licensing. If the post-closing plan conflicts with clearance conditions, the buyer may inherit immediate compliance risk. The SPA should therefore preserve enough flexibility to implement a remedy-compliant integration plan, rather than hard-wiring steps that may later become impossible or unlawful.

Looking ahead

FDI controls will continue to shape M&A deal terms as screening regimes expand and national security analysis becomes more asset-focused.

- Deal teams should assess FDI risk at the outset, including the target's technologies, data, government customers, supply chain role and links to critical infrastructure.
- Long-stop dates should reflect real-world review risk, including pre-notification, multi-jurisdictional sequencing, information requests and remedy discussions.
- Conditions precedent should address mandatory filings and, where appropriate, voluntary filings or call-in risk.
- Cooperation clauses should manage the flow of sensitive information through counsel-to-counsel or regulator-only channels.
- "Hell or high water" commitments, remedy caps and reverse break fees should be calibrated to the nature and severity of potential FDI remedies.
- FDI-specific warranties and post-closing covenants should support accurate regulatory submissions and compliance with any remedies imposed.

The principle is simple. In sensitive cross-border M&A, FDI risk is not just something to clear. It is something to price, allocate and draft for.

With thanks to Freshfields Jérôme Philippe and Basile Marin for their contributions to this update.

CFIUS: Is the Known Investor Program the golden ticket for investors?

In brief

The current US administration has signaled a more open posture towards foreign investment, supported by the America First Investment Policy, more targeted CFIUS mitigation practice and a stated commitment to faster, more efficient reviews. Two developing initiatives could become central to that shift: the Known Investor Program and pre-certified technology risk protocols. But both will depend on execution. In its current form the Known Investor Program risks asking repeat investors for extensive disclosure without offering a clear enough procedural benefit. Vulnerability protection protocols may be more promising, allowing parties to address common technology, data and infrastructure risks upfront. Together, they point towards a CFIUS process that rewards transparency, passivity and demonstrable risk mitigation.

Policy and procedural changes by the current US administration are improving the environment for foreign investment into the United States compared to the prior administration. This started with the America First Investment Policy (AFIP), which signaled the administration's early commitment to facilitating investment, including investment by allies into sensitive technologies, and was followed by noticeable changes in practice by the Committee on Foreign Investment in the United States (CFIUS) – including more targeted mitigation agreements and improved review timelines—and then the appointment of a new Assistant Secretary who has consistently signaled a commitment to a more efficient CFIUS process.

Therefore, aside from the decision (which we think was not compelled by law) by CFIUS not to start any new cases during the prolonged US government shutdown due to the lack of funding for one member agency (the effects of which parties may still feel for several months), there is reason for optimism.

CFIUS has undertaken multiple initiatives in an effort to translate the rhetoric into action. We focus here on two of these initiatives – still in the works – that have the potential to be the most consequential by reducing the barriers to investment consistent with US national security interests. The first is the development of the Known Investor Program, a pilot program that in its current form resembles political theater but, if CFIUS has the will, has the potential to become a significant improvement in the CFIUS process. The second is the idea of establishing pre-certified technology risk protocols that function essentially like pre-packaged mitigation that parties can offer to smooth the path to rapid CFIUS clearance of transactions in appropriate instances.

Known Investor Program – needs a major rethink

The AFIP touted a "fast track" program for certain investors. Treasury translated this into a "Known Investor Program" (KIP) that it began piloting last year, offering the opportunity for investors to complete an extensive questionnaire that ostensibly would help CFIUS be better positioned to review any transactions that the investor filed. The particulars of the KIP, including eligibility and how it would benefit an investor, however, were unclear.

CFIUS, however, has signaled its intent to roll out the KIP more broadly, formally seeking public input earlier this year and since then holding it out as a priority. (See Freshfields' comment letter on the KIP here).

CFIUS has an opportunity to give the KIP real meaning. But it would not be the program that CFIUS has thus far described publicly. The burden of assembling, certifying, disclosing, and continually updating the extensive and highly sensitive information that is

> "The Known Investor Program has the potential to become a significant improvement in the CFIUS process.

required to participate in the program could be significant, going well beyond the level of disclosure required in most CFIUS processes. And it is only proposed to be available to foreign investors that have submitted at least three transactions to CFIUS for review in the prior three years. In the KIP's current form, it is very likely that the burden of participation will not be commensurate with the benefit that the investor is likely to receive.

Does the stated benefit actually deliver value for investors? Treasury has said that, in return for the extensive disclosure provided by an investor, the KIP would allow CFIUS to front-load the analysis for repeat foreign investors, thus allowing for more efficient reviews once a new transaction comes before CFIUS.

But how much additional efficiency will there really be if, as Treasury has stated, the KIP will not replace CFIUS's case-by-case analysis, offer preapprovals, or even guarantee conclusion without need for a withdraw/refile? At best, KIP participants may marginally reduce the likelihood that their filing requires a Phase 2 investigation driven by the need for additional CFIUS due diligence. Otherwise, KIP participants face the same odds of receiving mitigation as they would have if they did not participate.

Moreover, how will additional disclosure actually benefit a repeat investor? As a repeat investor, the investor will already be well-known to the Committee. This is why, when a repeat investor comes again to the Committee, the focus is more on the unique considerations presented with a given target. Indeed, this approach was written into the 2018 CFIUS law, which permitted the Office of the Director of National Intelligence to independently publish a threat report within the first few weeks of a case for a repeat investor, in lieu of coordinating a threat report with the more than a dozen intelligence agencies that provide input into the threat analysis for new investors, a much more time- and labor-intensive process that takes 30 days.

Ironically, the investors that would most benefit from front-loading CFIUS's understanding of the investor – those that have never filed with CFIUS before – would not be eligible to participate in KIP because it requires the investor to have made multiple filings in preceding years.

Is demonstrating distance from China—the real key to KIP entry – worth the cost for investors who need it the most? The other purpose is to give investors an opportunity to show that they have distanced themselves from adversaries. If an investor's responses to the KIP questionnaire show that the investor has extensive investments in sensitive areas in China, that the investor engages in critical R&D or manufacturing in China, or that the investor is critically dependent on China as a market, or is otherwise vulnerable to pressure from China, then the investor is likely to have a difficult time realizing any benefits from the KIP, notwithstanding having provided an enormous amount of disclosure to the Committee. Many investors are trying to steer a middle path in this bipolar geopolitical environment. Treasury would like to hold entry into the KIP out as an incentive for companies to consciously decide to tilt towards the US market and away from China. The problem, however, is that the benefit that CFIUS offers through the KIP (moving through the process marginally faster on non-sensitive transactions) may not be worth the commercial and geopolitical risk investors may incur by abandoning a middle path. And for investors that are already keeping their distance from China, those investors likely already capture any incremental timing advantage that distance provides, raising the question of what additional value KIP participation would offer them.

> "Ironically, the investors that would most benefit from front-loading CFIUS's understanding of the investor would not be eligible to participate in KIP.

CFIUS can provide a benefit that will justify participation and enhance national security. CFIUS should afford approved Known Investors a form of excepted-investor treatment. Under the current rules, a narrow band of investors from Australia, Canada, New Zealand, and the United Kingdom ("excepted investors"), are exempted from non-control ("covered investment") jurisdiction, real estate jurisdiction, and mandatory filing requirements. Affording investors who qualify through the KIP a status similar to that of excepted investors would be a strong incentive for investors to accept the

resource and disclosure costs of participating in the program and to change corporate strategy as it relates to China.

Extending such benefits to KIP participants is well-founded from a national security perspective insofar as the KIP would involve an individualized threat determination based on investor-specific information, prior CFIUS experience, and US government threat analysis, as opposed to relying principally on country-level assumptions as a proxy for threat, like the current excepted-investor framework. CFIUS could establish a two-tier system that builds on the existing approach: the current regime would remain for investors that currently qualify as an excepted investor, while a second tier would extend benefits to approved Known Investors from a wider set of US allied and partner nations.

This framework would align with the AFIP by allowing trusted foreign investors to deploy capital to US businesses more quickly and by reducing the number of filings that CFIUS must review. This outcome would benefit CFIUS, foreign investors, and US businesses alike – including both start-ups and well-established businesses.

Vulnerability Protection Protocols – Pre-packaged mitigation could be a win-win

In recent public remarks, Treasury signaled that it is working on developing technology risk mitigation protocols that parties could certify to at the time of filing, with the goal of enabling a more efficient review. Beyond that, Treasury has not elaborated on what the program would look like in practice. It is, however, a potentially valuable initiative – and one that, if implemented thoughtfully, addresses a structural feature of the current CFIUS process that creates real friction for investors.

CFIUS analysis has been increasingly driven by vulnerability – or target sensitivity – assessment. In recent years, CFIUS has increasingly focused not only on whether a foreign investor is itself a threat, but on whether the transaction creates or amplifies vulnerabilities in the US business that any foreign investor – even one not identified as a threat – might inadvertently expose. The concern is often not malicious intent but rather ordinary business decisions that a foreign-owned or foreign-influenced company might make – decisions about where data is stored, which vendors are used, how IT systems are integrated – that could, in CFIUS's view, create risk. This means that even investors with a clean threat profile can find themselves subject to mitigation requirements driven entirely by the characteristics of the target business.

This is where pre-certified protocols offer the greatest potential. If the risk that CFIUS perceives is not a function of adversarial intent but of operational and structural vulnerabilities – the same types of vulnerabilities that exist across industry more broadly – then those risks are, by definition, more readily addressed by industry best practices than by bespoke, negotiated mitigation agreements. An investor and target that can demonstrate at the time of filing that they have already implemented the relevant controls are, in a meaningful sense, self-mitigating the very risk CFIUS would otherwise spend weeks or months investigating and, in some cases, negotiating to address.

While Treasury framed this initiative in terms of technology risk – and there are natural applications across a range of technology areas, including AI systems, semiconductor-related businesses, and cybersecurity software – the underlying logic extends beyond technology transactions. Critical infrastructure investments present similarly defined and well-understood vulnerability profiles, and are equally amenable to a protocol-based approach.

In most cases, the target would need to certify to the relevant protocols, since the vulnerabilities CFIUS is concerned about are primarily characteristics of the US business. But where the transaction involves integration of the target into the acquirer – including connection of IT systems, shared services, or a merger of operations – the acquirer may need to certify as well.

Given the vulnerability-focused nature of the risk, the ideal solution (both from a fairness perspective for the parties and from a national security perspective more generally) is promulgation of law

> “In recent years, even investors with a clean threat profile can find themselves subject to mitigation requirements driven entirely by the characteristics of the target business.

> Confirmed low-threat status plus pre-certified vulnerability mitigation – is precisely what an expedited clearance framework should reward.

or regulation that resolves such vulnerabilities on an industry-wide basis. However, in practice, that is not likely to happen reliably and does not address the CFIUS's need in the context of a particular transaction to address the risk before it. Reliance upon standardized risk mitigation protocols is the next best option.

CFIUS should lean on existing industry standards. On the question of what protocols CFIUS should require parties to certify to, the answer should, to the maximum extent possible, be existing, published industry-standard frameworks rather than CFIUS-developed ones. This is not merely a matter of convenience. Industry-standard protocols have been tested in practice, are well understood by companies and their advisors, have established auditing infrastructure, and do not require negotiation in the context of a particular transaction – which is what this initiative presumably is intended to avoid. There will be circumstances where a custom, CFIUS-published protocol is appropriate for risks that do not map cleanly onto existing standards, but those should be the exception.

The offered benefit should be a more defined path to clearance. The most practical path would be an internal CFIUS policy establishing that it will clear a transaction on a Declaration – or clear a Notice at the review stage without proceeding to investigation – where it concludes that the investor presents a low threat and the relevant parties have certified to the applicable protocols. Participants in the KIP would have the significant advantage of entering any given transaction already knowing that CFIUS views them as a low-threat investor, positioning them to take full advantage of the protocol certification pathway from the outset. That combination – confirmed low-threat status plus pre-certified vulnerability mitigation – is precisely what an expedited clearance framework should reward. Publishing template National Security Agreements and standard mitigation provisions alongside these protocols would further reinforce the framework, giving parties greater certainty and reducing the need to withdraw and refile notices solely to accommodate mitigation negotiations.

Looking ahead

The direction of travel is encouraging, but neither initiative will succeed on rhetoric alone. To make the CFIUS process more efficient without weakening national security review, Treasury will need to give trusted investors a clearer reason to participate and give parties a more predictable path to clearance where risks can be addressed up front.

- The KIP needs a more meaningful incentive structure. If participation requires extensive and sensitive disclosure, investors will need benefits that go beyond a general promise of a smoother review.
- Excepted-investor-style treatment could give KIP real force. A second-tier framework for approved Known Investors from allied and partner countries could reduce unnecessary filings while preserving CFIUS scrutiny where transaction-specific risks remain.
- Vulnerability protection protocols could address a core source of friction. Where CFIUS concerns are driven by target-side risks rather than the investor threat, pre-certified controls could allow parties to demonstrate mitigation at filing.
- Existing industry standards should be the starting point. Protocols will be more credible and workable if they draw on established frameworks than bespoke CFIUS requirements developed transaction by transaction.
- The strongest path to expedited clearance would combine confirmed low-threat investor status with pre-certified vulnerability mitigation. That is where KIP and the protocol initiative could reinforce each other most effectively.

With thanks to Freshfields Christine Laciak, Aimen Mir, Brian Reissaus, Colin Costello and Andrew Gabel for their contributions to this update.

Japan builds its CFIUS: Broader scope, deeper scrutiny

In brief

Japan's foreign investment regime is moving into a more assertive phase. A bill to amend the Foreign Exchange and Foreign Trade Act (FEFTA), now approved by Japan's parliament, will bring certain indirect acquisitions into scope, expand post-closing intervention powers and formalize a broader inter-ministerial review framework sometimes described as a "Japan CFIUS.", combining to create a materially more substantive environment for investors in sensitive sectors. At the same time, Japan is expected to reduce the filing requirement for lower-risk areas, freeing up resources to focus on more problematic investments.

Japan's foreign investment regime is being recalibrated for a less benign world. The country remains open to foreign capital, and the government continues to stress the importance of sound investment. But openness now comes with a sharper security filter focused on specific countries and certain asset types.

That shift predates Prime Minister Sanae Takaichi's appointment in October 2025. Japan has been moving steadily toward a more economic security-focused model for several years, with greater scrutiny of sensitive technologies, critical infrastructure, data and supply chains. The latest reforms accelerate that trend. They also make the review process less about the formal route by which the investment is made and more about the substance of influence, control and access to security information.

The resulting regulatory environment is something more nuanced and more challenging for investors, who cannot so easily test issues most relevant to the government's assessment such as foreign government influence.

A wider lens on control

The amendment to FEFTA is expected to make three practical changes that matter most for investors.

First, certain indirect acquisitions will become reportable. At present, Japan's FDI regime focuses largely on direct acquisitions of shares or voting rights in Japanese companies. That leaves a gap where control over a Japanese business is acquired indirectly through a foreign holding structure. The amendment is designed to close that gap.

Two types of indirect acquisition are expected to become reportable. The first is the acquisition, directly or indirectly, of 50% or more of the voting rights in a foreign entity that itself holds certain interests in a Japanese company. The second is the exercise of voting rights to appoint board members in that direct holder or its parent, where the result is that the foreign investor and related persons gain majority board control.

Investors acquiring non-Japanese companies will need to look through the structure and identify whether the target group holds interests in Japan. Board appointments in foreign entities may also require FDI analysis if those entities sit above Japanese assets.

This is a material change for cross-border M&A. Japan may no longer be a secondary diligence point simply because the immediate target is outside Japan..

Call-in risk

Second, regulators are expected to gain broader call-in powers including post-closing.

> The country remains open to foreign capital, and the government continues to stress the importance of sound investment. But openness now comes with a sharper security filter focused on specific countries.

Japan builds its CFIUS: Broader scope, deeper scrutiny

Under the current regime, Japanese authorities have limited formal ability to review investments outside the listed sensitive sectors that require prior notification. In practice, regulators have not always been passive. They have used informal channels to raise concerns and influence outcomes. But the amendment will give a clearer legal basis for intervention where a transaction that did not require prior approval can be considered to raise national security concerns.

The new call-in power is expected to apply for up to five years after closing. It would be limited to certain categories of investment, including direct acquisitions of listed and unlisted companies, mergers and business transfers. Indirect acquisitions appear to be outside the scope of this particular post-closing power on the face of the legal text, but actions may be taken in a more informal manner for indirect acquisitions too.

For investors, the message is not that every non-sensitive Japanese investment becomes risky. It is that "not notifiable" will not always mean "beyond scrutiny". Where a transaction touches sensitive technology, data, infrastructure or strategic industrial capability, investors may need to consider early informal engagement even if no mandatory filing is triggered.

> "The government is moving toward more institutionalized intelligence gathering and sharing, following the model used by the CFIUS regime in the US.

The exact modality for informal engagement has not been established yet, including how much clarity investors can obtain and when. This is to be further developed after the reforms are in place.

Lower-risk filings may be narrowed

Third, Japan appears to be trying to reduce unnecessary burden in lower-risk areas.

The current regime captures a wide range of transactions, including some that present little obvious national security risk. That has contributed to a heavy volume of prior notifications and has made the regime less targeted than policymakers may now want. Discussions are underway to rationalize the designated sectors requiring prior notification, particularly in areas such as information technology where current definitions can be broad.

The bill itself does not appear to set out the detail of this rationalization. Such changes are more likely to come through subordinate regulations, notices or guidance.

This is the other side of the reform. Japan is not simply expanding review. It is trying to distinguish more clearly between routine investment and transactions that warrant close examination. If implemented well, this should reduce friction for benign investments. On the flip side, it also potentially means that transactions that do attract scrutiny may face a more intensive review.

"Japan CFIUS"

The institutional reform may matter as much as the legal thresholds.

The government is moving toward more institutionalized intelligence gathering and sharing, following the model used by the CFIUS regime in the US.

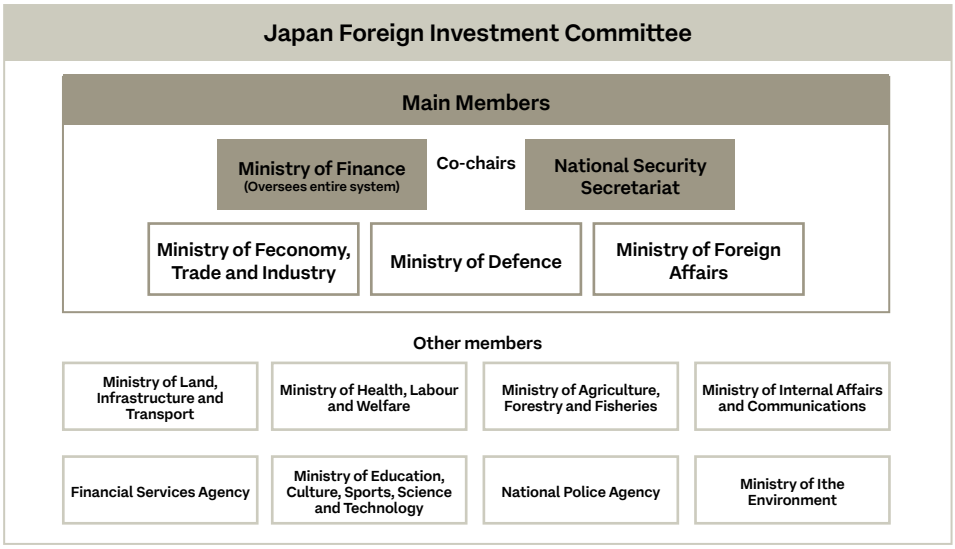
The Minister of Finance and the ministers responsible for relevant business sectors will be able, where necessary, to seek opinions from the Prime Minister, the Minister for Foreign Affairs and other relevant authorities. In practical terms, this will mean a wider group of security, diplomatic and sectoral agencies can feed into the FDI review.

This will likely change the character of the process. Reviews may become less formalistic and more intelligence-led. Regulators will be better placed to assess indirect foreign government influence, potential technology leakage, data exposure, supply chain vulnerability and risks to critical infrastructure.

For transaction parties, this creates a familiar problem in a new setting. The issues that matter most to the government may not be visible to the transaction parties. Review timetables may be affected by information the parties do not have and cannot easily test. Sensitive transactions may therefore feel less predictable, even where the legal rules are clearer.

Japan builds its CFIUS: Broader scope, deeper scrutiny

Overview of Japan CFIUS



Source: Liberal Democratic Party website.

Enforcement is moving first

Japanese regulators have been issuing more detailed requests for information, including questions designed to probe links with particular governments or state-linked interests. More transactions also appear to be subject to ring-fencing or other mitigation measures as a condition of clearance.

Public statistics have not fully reflected the rapid uptick of enforcement. This is because Japanese authorities often use administrative guidance - such as informal, nonbinding requests - that encourage parties to modify, delay or abandon transactions before the process escalates to a formal prohibition or remedy order. That tool gives regulators flexibility and insulates diplomatic sensitivity. Some transactions may be stopped or reshaped without appearing in official prohibition statistics.

The proposed acquisition of Makino by MBK Partners shows how far the regime can go when sensitive technology is involved. In April 2026, the Japanese government opposed MBK's bid for Makino, a leading machine tool manufacturer with technology used in defense-related applications. This is the first time in 18 years that the government used its official powers to block a foreign investment. The government stressed that restrictions on foreign investment should be minimal as a rule. In the case of MBK Partners, however, Makino's dual-use machine tools were deemed too sensitive to be acquired by a foreign entity.

Japan has not suggested that foreign investment is unwelcome. It has drawn a harder line around assets it sees as strategically sensitive. For investors, that line will not always be obvious at the outset.

Security logic is spreading

The same security logic is beginning to influence adjacent areas of policy. The Japan Fair Trade Commission has published guidance and case materials addressing national security considerations in merger review. Those materials suggest greater willingness to recognize industrial resilience and technology protection as relevant policy concerns.

Corporate takeover policy may also move in the same direction. The Ministry of Economy, Trade and Industry is considering whether national security concerns should be reflected in target management's assessment of competing bidders. If that approach develops, national security may become part of a target board's judgment about a prospective deal as well as regulatory review.

This is the broader point. Japan's FDI reforms are part of a wider reordering of economic policy around national resilience. Competition law, takeover policy and investment screening are not merging into one regime. But they are increasingly being pulled by the same gravitational force.

> Low-risk investment may become easier to process.

Looking ahead

Japan is not closing itself to foreign investment. It is asking a harder question: when does investment become strategic influence which needs to be addressed?

For investors, four practical points follow:

- Screen for Japanese interests across the full group structure, not just the immediate target.
- Treat indirect control, board appointment rights and foreign government links as early diligence issues.
- Build potential FDI engagement into deal timetables where sensitive technology, data or infrastructure is involved.
- Do not assume that a non-notifiable transaction is insulated from later review.

The landscape is clearly shifting. Low-risk investment may become easier to process. Sensitive investment will likely entail detailed scrutiny and require a coherent narrative as to why it does not raise national security concerns.

With thanks to Freshfields Kaori Yamada, Yusuke Kanbayashi and Shuntaro Muto for their contributions to this update.

Austrian FDI: Managing heightened scrutiny, Phase II proceedings and policy shifts

In brief

Austria's FDI regime is broad in scope and actively enforced. Investors therefore need to assess each transaction carefully, with particular attention to acquisition structures, voting rights, aggregation rules, sensitive sectors and assets deals. Heightened scrutiny at both national and EU levels, together with the potential for conditions or even outright prohibitions, means investors need a clear strategy for navigating in-depth reviews.

Broad in scope, proactive in enforcement, far-reaching in practice

Austria has established itself as one of the EU's most active FDI screening jurisdictions. For investors looking to invest in an Austrian company or its assets, FDI analysis is not a box-ticking exercise. The regime's broad scope, expansive interpretation and the Federal Ministry for Economy, Energy and Tourism's (BMWET) active enforcement approach all require a cautious, case-by-case assessment.

An FDI filing under Austria's Investment Control Act (ICA) is triggered when a non-EU, non-EEA or non-Swiss investor (foreign investor) acquires, directly or indirectly, an Austrian company, control over such a company or its substantial assets, or voting right shares in such a company that meet or exceed specific thresholds. These thresholds are 10% or 25%, depending on the sector, or a general threshold of 50%, provided the company operates in a sector falling within the scope of the ICA.

> The policy shift at both national and EU levels points towards sustained, and intensified, scrutiny. Investors must therefore continue to prioritize strategic transaction planning.

In practice, the Austrian regime reaches further than a first reading of the ICA might suggest.

- **Far-reaching "foreign investor" criterion.** A filing obligation can arise even where neither the buyer nor the ultimate owners are from outside the EU, EEA or Switzerland. It may be enough for a non-EU/EEA/Swiss person or entity to sit anywhere in the acquisition chain.
- **Voting rights aggregation.** Even where no single investor meets the relevant voting rights threshold, voting rights may need to be aggregated with those of other investors.
- **Broad interpretation of sensitive sectors.** The sectors covered by the ICA extend beyond those expressly listed in its annex, which is non-exhaustive, and also captures upstream and downstream activities. Security services, for instance, fall within scope despite not being listed. Finance captures core activities such as payment services and electronic trading platforms as well as gambling, while Traffic and Transport extends to motor vehicles and cable cars.

Notably for dealmakers, asset deals can trigger a filing obligation just as share acquisitions can. Approval is required when a foreign investor acquires substantial assets of an Austrian company. The BMWET interprets "substantial" broadly: customer lists, inventory, marketing authorizations or employee transfer obligations may be sufficient to bring an asset deal within scope.

> Transactions are attracting particular scrutiny where investors are based in countries whose laws require, or may require, disclosure of sensitive information relevant to Austria's security or public order.

Austrian FDI review process

The Austrian screening process has two main phases, preceded by an EU cooperation mechanism, often referred to as "Phase 0." During this stage, the European Commission and other Member States may comment or raise questions. The length of Phase 0 depends on whether any such input is received.

Once the EU cooperation mechanism is complete, Phase I begins. Within one month, the BMWET will either clear the transaction, having concluded that there is no "reasonable suspicion" of a threat to security or public order, or initiate an in-depth Phase II review.

Before opening Phase II, the BMWET must convene the Investment Control Committee. This advisory body provides a non-binding recommendation, but its views carry considerable weight in the review process.

If Phase II is opened, the BMWET is subject to a hard two-month deadline, which is not suspended by information requests. At the end of the process, it may approve the transaction unconditionally, approve it subject to conditions or prohibit it.

A strict standstill obligation applies throughout both phases. Closing before clearance constitutes a criminal offence. Investors should therefore build the relevant timelines into transaction planning, deal documentation and long-stop date negotiations from the outset.

Heightened scrutiny in practice

According to the most recent activity reports for 2022 and 2023, 68-79% of cases were cleared in Phase I, conditional approvals accounted for 5.5-7.5% and no prohibitions were issued.

The position has since shifted with a clear uptick in both prohibitions and voluntary withdrawals by investors anticipating a negative outcome. Transactions are attracting particular scrutiny where investors are based in countries whose laws require, or may require, disclosure of sensitive information relevant to Austria's security or public order. Targets of particular strategic importance are also receiving closer attention.

This stricter approach to intervention is being mirrored at EU level. Those still at the proposal stake, the Industrial Accelerator Act (IAA), if enacted, would signal a significant shift beyond traditional FDI screening. It would target investors from countries without an EU free trade agreement, particularly those with dominant global manufacturing capacity in certain sectors, such as China.

Rather than focusing only on whether a transaction threatens security and public order, the IAA would make market access conditional on technology transfer, the sharing of know-how and intellectual property, and local value creation commitments.

Managing Phase II proceedings

The two-month Phase II deadline can be challenging, particularly in complex cases where a prohibition or conditional approval is under consideration. With no statutory mechanism to extend the timeframe, the BMWET typically investigates intensively, engages with other ministries and federal provinces and issues targeted information requests to the parties.

Given the limited time available, investors must be proactive. This may include regularly requesting access to the file, addressing concerns raised by the members of the Investment Control Committee or the BMWET, responding in detail and promptly to information

> Rather than focusing only on whether a transaction threatens security and public order, the IAA would make market access conditional on technology transfer, the sharing of know-how and intellectual property, and local value creation commitments.

requests and seeking to resolve any doubts about potential threats to security or public order.

Most conditions imposed by the BMWET have related to security of supply. These include commitments to maintain a local presence, to continue supplying certain customers or to sustain agreed supply levels. Patent protection is another common focus, particularly where the transfer of patents could affect the continued manufacture of essential products. Data security and cybersecurity risks have also been addressed through conditions in a number of cases. Other conditions may include reporting obligations to the BMWET or restrictions on the investor's influence over the target company.

Where conditions are likely, investors should be prepared to engage constructively. The BMWET and the investor will typically discuss the proposed conditions, and investors should seek to ensure that any commitments are proportionate, targeted and capable of practical compliance. Conditions are always case-specific and vary considerably.

Purely economic considerations are not sufficient to justify a prohibition or conditional approval. A prohibition should be imposed only as a measure of last resort, where no set of conditions would adequately address the relevant threat. With the right strategy, investors should generally be able to address concerns that might otherwise lead to a prohibition or withdrawal.

Looking ahead

The policy shift at both national and EU levels points towards sustained, and intensified, scrutiny. Investors must therefore continue to prioritize strategic transaction planning. The ability to anticipate evolving policy developments, identify sensitive issues early and manage complex Phase II proceedings effectively will be central to successful deal-making in Austria.

- **FDI risk in Austria requires early and granular assessment.** Investors should analyze ownership structures, voting rights, aggregation rules and asset-level sensitivities at the outset, including for asset deals and indirect exposure.
- **Phase II risk should be built into deal strategy from the start.** Tight statutory deadlines, active information requests and limited flexibility mean investors need a clear plan for engagement, evidence and potential remedies before filing.
- **Enforcement is becoming more interventionist and policy-driven.** Scrutiny is intensifying where transactions involve sensitive sectors, strategic targets or investors from higher-risk jurisdictions, with prohibitions and withdrawals now more common.
- **Transaction outcomes increasingly depend on remedy readiness.** Investors should be prepared to offer targeted, workable commitments on security of supply, governance, data and intellectual property to secure clearance under increasingly stringent review.

With thanks to Freshfields Stephan Denk, Lukas Pomaroli and Marcel Neuhauser for their contributions to this update.

FRESHFIELDS

www.freshfields.com.

June 2026 | DSR0042348

freshfields.com