Economic Statecraft: How the Emerging Front in National Security Impacts Cross-Border Firms

July 22, 2025

In a global environment where "[e]conomic security is national security," the rise of protectionist regulatory regimes and industrial policy is threatening to bring decades of global free trade to a close. In this article, the Debevoise National Security team (i) examines how the evolving political landscape and the proliferation of national security regulatory regimes are dismantling the global free trade consensus, and (ii) provides recommendations for global firms to successfully navigate this increasingly fragmented landscape.

European and U.S. investment restrictions, global economic sanctions, data localization regulations, supply chain regulations, and enhanced criminal and civil enforcement policies are blurring the historical lines between economic security and national security, with the U.S. government and others likely to expand their use of national security tools to advance economic objectives. We discuss each of these areas below.

European Investment Restrictions

There is renewed interest in the European Union ("EU") in fostering EU and national "champions" to strengthen European economic independence and counterbalance U.S. and Chinese influence. This effort aligns with ongoing concerns about protecting domestic economic security by minimizing the leakage of strategically important technologies and know-how across the EU. In support of these goals, the European Commission ("Commission") is looking to further tighten and control the review of inbound investment and is considering introducing outbound investment screening.

European Outbound Investment Restrictions

In January 2025, the Commission issued a Recommendation to Member States to gather information and data on outbound investments made by EU investors in third countries going back to January 1, 2021. Member States are encouraged to do so including by establishing an "adequate system for review that may provide for voluntary provision of information on transactions." Transactions in focus relate to specific sensitive sectors,

namely semiconductors, artificial intelligence and quantum technologies. This Recommendation is only a data collection exercise and not legally binding, but the Commission has asked Member States for a progress update by July 15, 2025 and a final report by June 30, 2026 on their implementation. Although not imminent, the Recommendation is seen as a preparatory step to ultimately introduce a common EU-wide outbound investment assessment mechanism.

European Inbound Investment Restrictions

At the same time, the Commission is planning to tighten its bloc-wide regulation of inward foreign direct investments ("FDI"). Unlike merger control, FDI screening in the EU lacks a centralized "one-stop-shop" mechanism and remains largely the responsibility of Member States to police at their discretion. However, the EU FDI Screening Regulation, which came into force in October 2020, has created a cooperation mechanism for all Member States and strongly encouraged the adoption of national regimes with a basic level of harmonization. As a result, 24 of the 27 EU Member States now screen FDI, with many continuously working to enhance the robustness of their regimes to protect sensitive sectors. The trend of heightened FDI regulation at a national level has also been galvanized by the recent electoral success of anti-globalization and protectionist governments in several Member States, blurring the divide between national security concerns and economic nationalism. To date, only Croatia, Cyprus and Greece have yet to implement a national screening mechanism.

Yet, in the absence of further harmonization, the rules of Member States' FDI regimes vary significantly, making assessment and notification cumbersome. The EU's most recent proposals therefore seek to address this and other existing shortcomings, as well as to make national FDI review mandatory. Among other measures, the proposals look to (i) introduce a uniform minimum standard for the critical sectors that fall within the sectorial scope of the EU FDI Screening Regulation, and (ii) extend the EU FDI Screening Regulation to cover indirect foreign investments (i.e., acquisitions by EU companies with a non-EU parent), thereby closing a significant loophole. The effect would be increased harmonization with additional transactions in scope. The proposals are currently navigating the EU's legislative process and are currently expected to become effective before the end of 2025.

Meanwhile in the UK, statistics show that the number of screened FDI transactions has remained relatively consistent in 2024 compared to prior years. It is noteworthy, though, that the number of transactions considered to be a risk to national security dropped by 40% over the same period. There is some expectation that this trend will continue, particularly considering the new Labour government's pro-growth agenda. The new government has also demonstrated a willingness to court investment from China. That may result in a gradual departure from the UK's previously hawkish

approach to Chinese investment, particularly in low-risk sectors. This would be in direct contrast to the EU and its Member States, which have continued to be skeptical of Chinese investment. For example, in July 2024 the German government prevented the acquisition of a Volkswagen subsidiary by a Chinese state-owned company, citing national security concerns about dual use technologies.

It is worth emphasizing that while FDI screening regimes tend to cast a wide net, leading to a large number of transactions triggering notification, only a minority of deals are subjected to a prolonged, in-depth review and an even smaller proportion is ultimately prohibited or abandoned. However, there has been an uptick in the number of transactions that result in behavioral remedies, such as commitments to retain domestic production and ensure continued investment in the business. As a result, the key challenge for most dealmakers is to ensure timely approvals while navigating an ever-growing web of national security review regimes that trigger at much lower ownership levels than merger control and that are more predisposed toward intervention.

U.S. Investment Restrictions

U.S. foreign investment policy has traditionally been centered on the regulation of inbound investment through the Committee on Foreign Investment in the United States ("CFIUS"), which reviews certain foreign investment in the U.S. for national security risks. Over the past several presidential administrations, this longstanding model on foreign investment policy has evolved significantly. Now, CFIUS's review of inbound investment as currently authorized is not considered enough to protect U.S. economic and national security interests.

Recent policy developments reflect an effort to expand CFIUS's role and establish a complementary outbound investment screening regime to address risks beyond the scope of traditional inbound reviews. These developments are expected to continue under the Trump Administration, particularly after release of the February 2025 presidential memorandum on foreign investment, titled the America First Investment Policy. Per the memorandum, the overarching themes of the Trump Administration's foreign investment policy are that "[e]conomic security is national security" and that "investment at all costs is not always in the national interest." In particular, the policy emphasizes national security threats from "foreign adversaries," principally the People's Republic of China ("PRC"). The policy calls out threats such as PRC efforts to use inbound U.S. investments to acquire critical technology, obtain intellectual property, and gain leverage in strategic industries, as well as exploiting outbound U.S. investments in Chinese companies to strengthen military and intelligence capabilities. The U.S.

government's intended response to such threats largely informs both inbound and outbound investment restrictions.

CFIUS and U.S. Inbound Investment Restrictions

Through its review of inbound investment, CFIUS has long been the primary U.S. federal government vehicle to address national security risks related to foreign investment. Accordingly, it is no surprise that certain objectives of the America First Investment Policy either explicitly or implicitly involve CFIUS, whether through seeking to expand CFIUS's authority or by realigning CFIUS's discretionary priorities. The specific policy measures likely to affect CFIUS include:

- Implementing proportional restrictions on foreign investors that are to ease in proportion to a foreign investor's verifiable distance and independence from foreign adversaries or other threat actors.

- Establishing an expedited "fast-track" review process for investment in advanced technology businesses and other important areas from allied and partner sources that are not themselves partnering with foreign adversaries; the Treasury Department has stated via a May 8, 2025 press release that this "fast-track" process will involve CFIUS collecting information on investors through an online portal in advance of a CFIUS filing.

- Restricting PRC-affiliated investors from investing in strategic sectors like technology, critical infrastructure, healthcare, agriculture, energy, and raw materials, and restricting all foreign adversaries from access to U.S. talent and operations in sensitive technologies, especially artificial intelligence.

- Protecting strategic real estate, such as farmland and property near sensitive facilities.

- Expanding CFIUS review to address "greenfield" investments (as in, companies created in the U.S. by foreign parents) and a greater number of "emerging and foundational" technologies.

- Ceasing the use of complex and open-ended mitigation agreements for investors from foreign adversary countries and generally ensuring that mitigation agreements consist of concrete actions that companies can complete within a specific period of time.

- Welcoming passive investments from all foreign investors, with passivity generally including non-controlling stakes with no voting, board, or governance rights, and no

influence over or non-public access to technical or proprietary U.S. business information.

While the actual implementation of the America First Investment Policy is ongoing with much yet to be seen, many of its goals align with efforts that CFIUS has already been undertaking. For instance, CFIUS has already implemented a laser-like focus on the PRC and PRC-affiliated investors. Since the first Trump Administration and continuing through the Biden Administration, CFIUS has heavily scrutinized foreign investors for PRC ties, including through gathering extensive information on investors that do not have overt or obvious connections to the PRC or PRC-affiliated investors. These efforts include requesting information about non-U.S. limited partners in private equity fund structures, even when such limited partners are passive or hold low levels of equity interest. CFIUS has sought information including limited partner identities and governance and transaction rights, with CFIUS requiring the sharing of such information even when it is subject to confidentiality protection. Such information requests are likely to continue in order to provide CFIUS with information it needs to determine which foreign investors are affiliated with the PRC.

Beyond its focus on the PRC, other elements of the America First Investment Policy align with recent CFIUS priorities. After gaining authority via statute to review certain real estate transactions, CFIUS expanded its real estate review jurisdiction by adding to its list of sensitive real estate locations in both 2023 and 2024. These efforts are likely to continue in light of the policy goal to protect strategic real estate. Additionally, CFIUS's regulations do allow some exceptions for investors from certain allied countries, as well as offer guidance on how passive investments can be outside of CFIUS jurisdiction, but these rules may be expanded or enhanced in light of the Trump Administration's stated policy objectives to offer a more favorable review process for allied country investors and welcome passive investments from all investors.

However, the America First Investment Policy does signal changes to other CFIUS practices and procedures. Specifically, a major area to watch is CFIUS's use and implementation of mitigation agreements. With the stated goal of avoiding complex mitigation agreements for investors that are from foreign adversary countries, it appears CFIUS may start blocking transactions by such investors instead of allowing them to go forward with expansive mitigation measures. Further, CFIUS has been requiring onerous mitigation for transactions in certain sensitive industries, even when the foreign investor is from an allied country, giving rise to seemingly perpetual compliance obligations. That practice may soon change given the policy goal to ensure that mitigation agreements have concrete actions with specific timelines for completion.

The future for other areas of CFIUS focus is less certain. For example, in recent years, CFIUS has enhanced its capabilities and internal resources necessary to research and

investigate foreign investment, including the creation of a "non-notified" team to inquire about transactions not affirmatively filed with CFIUS. In December 2024, new regulations became effective that further strengthened CFIUS's compliance and enforcement authorities, enabling it to collect detailed information, mitigate the national security risks of transactions, and penalize parties that violate CFIUS rules or obligations. It remains to be seen how these enhanced powers will be applied going forward. One possibility is that CFIUS will intensify its enforcement posture primarily toward PRC-affiliated investors, while adopting a more measured approach toward others. Alternatively, CFIUS may continue using these tools broadly to ensure that any foreign investment presenting a national security risk—whether PRC-related or not—is subject to review and potential mitigation. Further, other policy goals of the America First Investment Policy, such as expanding CFIUS review to cover greenfield investments, would likely require legislative action. These measures are even less certain than executive action and may take more time to be implemented.

While there is uncertainty about precisely how CFIUS may change under newly stated U.S. foreign investment policy goals, the CFIUS trendlines suggest a spectrum of CFIUS scrutiny depending on the nationality of a foreign investor. On one end of the spectrum, investors from U.S.-allied countries can expect the same or a softened approach regarding inbound investment restrictions from CFIUS, while on the other end of the spectrum, investors from or affiliated with foreign adversary countries—especially the PRC—can expect even more heightened CFIUS scrutiny and restrictions on their investments. Global investors will want to take stock of where both they, and other investors with which they are affiliated, fall on that spectrum and prepare for CFIUS scrutiny of U.S. inbound investment accordingly.

Regulation of Advanced Technologies: Export Controls and Outbound Investment

Historically, U.S. national security concerns regarding advanced technologies have been addressed primarily through U.S. export controls.

For example, during the first Trump Administration several Chinese companies, including major telecommunications and semiconductor companies, were added to the Entity List of the U.S. Commerce Department's Bureau of Industry and Security. This designation restricted the provision of most U.S. goods and technology to these companies and was accompanied by efforts to secure similar restrictions from allied countries. These efforts were expanded under the Biden Administration, which imposed even broader export controls on semiconductor technologies. The aim was to prevent China, Russia, and other geopolitical adversaries from acquiring and developing sensitive technologies. However, these policies have contributed to a breakdown in international consensus around multilateral export control frameworks, such as the

Wassenaar Arrangement. As a result, the global export control framework—particularly for advanced technologies like semiconductors, quantum information and certain AI developments—is fragmenting into Western and rest-of-the-world camps, with cross-border and multinational companies facing new and growing regulatory barriers to global commerce, including research and development efforts.

Despite the significant expansion of export controls over the last several years, U.S. national security authorities concluded that additional measures were needed to address risks posed by outbound U.S. investment in sensitive technologies. In response, President Biden established a new and novel outbound investment regime targeting the PRC. The policy aims to deny PRC-related businesses any "ancillary benefits" that flow from U.S. investment in their companies. The new U.S. restrictions impose notification and prohibition requirements on certain investments by U.S. persons in PRC-related companies that develop or produce items related to semiconductors and microelectronics, quantum information or certain AI systems. To be clear, these outbound investment controls do not mirror the CFIUS review model. Rather than requiring prior government approval, they establish a compliance regime more akin to export controls or sanctions. U.S. investors are subject to compliance obligations across their global operations, with responsibilities extending to "controlled foreign entities" of U.S. companies. Investors are also expected to implement appropriate due diligence processes to ensure compliance with the new framework.

This focus on technology-related national security restrictions continues to be a primary national security goal of the Trump Administration. The issuance of the America First Investment Policy already has signaled the possible imposition of new or expanded outbound investment restrictions targeting other areas of concern related to the PRC's military-industrial sector, including biotechnology, hypersonics, aerospace, advanced manufacturing, directed energy, and other areas related to China's alleged Military-Civil Fusion development strategy, as well as potential discontinuation of certain existing exclusions, such as acquisitions of publicly traded securities.

Meanwhile, legislative efforts also aim to expand U.S. outbound investment restrictions. In March 2025, bipartisan legislation introduced in the U.S. House of Representatives would, among other measures, expand U.S. outbound investment restrictions under a similar but distinct regulatory regime that would include controls on additional technologies, including hypersonics.

As the new outbound investment restrictions have only recently been made effective, it remains to be seen how U.S. authorities may monitor and enforce compliance. However, there is a strong bipartisan policy consensus supporting the new regime and a clear aim by both the Trump Administration and U.S. lawmakers to expand these restrictions. Accordingly, U.S. export controls and outbound investment restrictions

will continue to have significant regulatory implications for cross-border business activity and wide impacts on global investment by both U.S. and non-U.S. firms.

Sanctions

U.S. Sanctions

Sanctions have historically been one of the primary tools for the U.S. government to advance U.S. national security and foreign policy objectives. During the first Trump Administration, sanctions were employed aggressively, including to reimpose "maximum pressure" on Iran and cut off Iranian oil revenues, impose sweeping sanctions against the regime of Venezuela's Nicolás Maduro, and restrict transactions in publicly traded securities of certain Chinese companies identified as a threat to U.S. national security interests. The new Trump Administration appears to be picking up where it left off, embracing a similar use of sanctions to achieve an array of national security goals. For example, on his first day in office, President Trump issued an executive order declaring a national emergency regarding threats posed by international cartels and authorizing the imposition of sanctions under the International Emergency Economic Powers Act ("IEEPA") on international cartel organizations.

Many of the sanctions priorities under the first Trump Administration appear to be focuses of the new administration. On February 4, 2025, President Trump issued a National Security Presidential Memorandum reinstating the "maximum pressure" campaign against Iran, to disrupt Iran's oil trade, with a particular focus on exports of Iranian crude oil to China. The Trump Administration has already issued multiple rounds of sanctions targeting Iran's shadow fleet of vessels carrying its oil exports, other entities facilitating Iranian oil shipments, and Chinese "teapot" refineries purchasing or facilitating the delivery of Iranian oil (although the scope of future U.S. sanctions on Iran may depend on the outcome of ongoing talks addressing Iran's nuclear program). With respect to China, President Trump's America First Investment Policy directs U.S. agencies to "use all necessary legal instruments to further deter U.S. persons from investing in the PRC's military-industrial sector," including through use of blocking sanctions or non-blocking sanctions targeting certain securities transactions related to identified Chinese military companies. In the case of Venezuela, the Trump Administration has taken a harder stance on the Maduro regime by revoking previous sanctions licenses authorizing various multinational oil and gas companies to operate in Venezuela.

For many firms, U.S. sanctions on Russia present significant uncertainty. In the confirmation hearings for both Secretary of State Marco Rubio and Secretary of the Treasury Scott Bessent, the potential for both lifting and, conversely, ratcheting up U.S.

sanctions on Russia was mentioned in the context of ending the war in Ukraine. In February 2025, Attorney General Pam Bondi disbanded the U.S. Department of Justice's Task Force KleptoCapture, which was created under the Biden Administration to enforce U.S. sanctions on Russian oligarchs. Subsequently, in March 2025, news reports suggested that the U.S. State and Treasury Departments were directed to prepare proposals for easing sanctions on certain Russian entities and individuals as part of potential negotiations with Russia. These actions suggested a potential openness by the U.S. government to easing sanctions on Russia, but more recently President Trump has expressed frustration with Russia and the lack of progress on ending the war in Ukraine. Meaningful clarity is yet to emerge on U.S. sanctions policy toward Russia going forward or potential implications for firms' business activities.

The new administration has adopted novel interpretations of existing sanctions authorities in furtherance of national security aims. Notably, President Trump is the first president to use IEEPA as authority to impose tariffs, with recent tariffs intended to address the "national emergency posed by the large and persistent [U.S.] trade deficits." Further, on March 24, 2025, President Trump issued an executive order authorizing so-called "secondary tariffs," also under IEEPA, on countries importing Venezuelan oil in response to the national security and foreign policy threats posed by the Maduro regime. President Trump has subsequently threatened to impose similar secondary tariffs on countries buying oil from Iran and Russia. These new uses of existing sanctions authorities enable the administration to take action rapidly, which means firms must remain alert and ready to respond quickly to new developments. In April 2025, the first legal challenges to the President's use of IEEPA to impose tariffs were filed and bipartisan legislation was introduced to limit the President's ability to unilaterally impose tariffs without congressional approval, but the outcome of these efforts remains to be seen.

In addition to the potential use of secondary tariffs, the Trump Administration may seek to further sanctions objectives through regulatory changes related to financial institutions' anti-money laundering ("AML") obligations. The February 4, 2025, National Security Presidential Memorandum directs the Treasury Department to "evaluate beneficial ownership thresholds to ensure sanctions deny Iran all possible illicit revenue" and to consider whether financial institutions should adopt a "know your customer's customer" standard for certain transactions to prevent evasion of Iran sanctions. Lowering beneficial ownership thresholds or expanding the mandated scope of customer due diligence could significantly impact financial institutions' AML policies, procedures and controls.

Under the new administration, there also have been early signs of a departure from the close coordination that existed in recent years between the U.S. and its allies on sanctions measures. For example, on the three-year anniversary of Russia's invasion of

Ukraine in February 2025, for the first time, the U.S. did not join the EU and United Kingdom in releasing a new package of sanctions on Russia. This divergence in sanctions approach was also evident in the Trump Administration's recent imposition of sanctions targeting the International Criminal Court, which drew wide condemnation from Western allies and sparked discussions on the invocation of the EU blocking statute to enable EU firms to resist conflicts created by U.S. sanctions. This may portend future divergence between the sanctions regimes of the U.S. and its allies and greater potential sanctions exposure and compliance burden for companies operating across these jurisdictions.

While the precise contours and focuses of U.S. sanctions under the Trump Administration are still emerging, it is evident that the robust use of sanctions by U.S. authorities to further U.S. national security and foreign policy aims will continue. In addition, authorities may seek enforcement of sanctions objectives through economic measures and changes in related regulatory areas.

European Union Sanctions: Dawn of EU "Secondary Sanctions"

Traditionally, EU trade and economic sanctions have been narrower in both scope and application than their U.S. counterparts. It was generally assumed that unless a transaction involved an EU entity or was taking place within the EU, EU sanctions compliance did not need to be considered. That assumption is no longer valid. Since the start of Russia's invasion of Ukraine in 2022, the EU has significantly evolved its approach to designing and implementing its sanctions regimes. These developments mean that EU sanctions increasingly take a U.S.-style approach to extraterritoriality and can impact cross-border trade throughout the world, even in circumstances where there may be no immediate connection to the EU.

The EU's increasingly assertive approach to sanctions policy is best illustrated by its new "best efforts" obligation. EU companies are now required to take proactive "best efforts" to ensure that their owned or controlled subsidiaries—regardless of location—do not take actions that would undermine EU sanctions targeting Russia and Belarus. While the United States has for a long time applied a similar principle under its Cuba and Iran sanctions regimes, this has not been extended to its Russia and Belarus regimes. Importantly, this "best efforts" obligation will bite whenever EU entities are included in a corporate structure. For example, a U.S.-headquartered company that structures its Middle East and Africa operations under an EU holding entity will find that all of its subsidiaries in this region are required to comply with EU sanctions (at least relating to Russia and Belarus).

The EU can also impose asset freezes against persons that it deems are "significantly frustrating" EU sanctions against Russia. This has already been used to sanction entities

in Hong Kong, Israel, and China identified as supplying sensitive products targeted by EU trade sanctions to Russia. Critically, this listing ground looks similar to U.S. secondary sanctions, which allow the United States to impose blocking sanctions on entities that undertake business with U.S. sanctions targets, in that it achieves a very similar goal: dissuading companies outside EU sanctions jurisdiction from undertaking activities prohibited for EU persons under EU sanctions and thereby promoting voluntary global compliance with EU sanctions. Although application of this asset freeze designation ground requires unanimous consent from all EU Member States and is therefore likely to be used sparingly, it nonetheless demonstrates a new commitment to pushing EU sanctions beyond EU borders.

Finally, the EU is starting to mandate certain sanctions-related contractual language for EU exporters under a principle commonly referred to as the "No Russia" clause requirement. Under this requirement, an EU exporter is mandated to include a contractual obligation to prevent re-export to Russia whenever sending certain sensitive categories of sensitive goods to non-EU buyers (with limited exceptions for "partner nations," such as the United States, the United Kingdom and Japan). Although at first blush this appears to be a relatively minor technical requirement, the net effect is that non-EU buyers are required to contractually bind themselves to complying with EU sanctions (at least in relation to Russia) whenever buying certain products being exported from the EU. The impact of this development is amplified by the fact that the EU's model "No Russia" clause (which, while not binding, is being followed by EU parties) obliges buyers of EU products to themselves take "best efforts" to prevent their own customers from allowing the relevant products to be sent to Russia, effectively creating a chain of contractual EU sanctions compliance obligations following the relevant product.

These developments mean that EU sanctions are increasingly relevant when conducting cross-border trade, even where no EU entity is involved in a transaction. International businesses should ensure that they have mapped their potential exposure to these new extraterritorial EU sanctions compliance obligations. Fortunately, at present these risks will only apply in relation to business touching on Russia and Belarus, although these measures may well form a template for future EU sanctions policy.

Data Access Restrictions

On December 27, 2024, the U.S. Department of Justice ("DOJ") issued the "Final Rule on Preventing Access to Sensitive Data" ("Bulk Data Rule") to implement the February 28, 2024 Executive Order on Preventing Access to U.S. Sensitive Personal Data and the United States Government-Related Data by Countries of Concern or Covered Persons.

The Bulk Data Rule established a national security-based export control regime to restrict the transfer of bulk sensitive personal and government-related data to foreign adversaries deemed threats to U.S. national security. The Bulk Data Rule has significant implications for global companies that do business or have operational footprints in China and Hong Kong, which are identified as countries of concern.

Legislative frameworks and regulatory requirements prior to the Bulk Data Rule failed to fully address these potential vulnerabilities. Specifically, existing laws, such as the Protecting Americans' Data from Foreign Adversaries Act of 2024, CFIUS authorities, and earlier executive orders focus on transaction-specific reviews or sector-specific controls but lack broad restrictions on data transactions. The Bulk Data Rule fills this gap by restricting certain sensitive bulk data transactions with countries of concern and covered persons, establishing a new regulatory regime implemented by DOJ's National Security Division ("NSD") to issue licenses for such transfers, provide advisory opinions, and enforce specific security mitigation requirements and exemptions.

Substantively, the Bulk Data Rule targets access—broadly defined—by "covered persons" to either government-related data or "bulk U.S. sensitive personal data." The latter encompasses a wide array of information about U.S. persons, including financial transaction data, IP addresses, advertising IDs, and mental or physical health information. Importantly, these categories are covered regardless of encryption or anonymization, significantly broadening the traditional scope of "personally identifiable information."

The Bulk Data Rule provides bulk thresholds (such as 100,000 covered personal identifiers) that, when met as between a U.S. person providing access to covered persons over any 12-month span, may be a "covered transaction." Covered transactions have four flavors—data brokerage, employment agreement, vendor agreement, and investment agreements. Data brokerage is defined broadly and is prohibited, full stop. The remaining agreement types may proceed provided compliance requirements are met—which include the implementation of CISA's security requirements that, in turn, include data-level measures that are "sufficient to fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable." In other words, even for restricted transactions to proceed, access by the covered person cannot be to identifiable personal data, which in practice may act as an effective prohibition where the covered person cannot carry out a vendor or employment agreement without access to linkable personal data.

Additionally, the Bulk Data Rule mandates contractual safeguards in cross-border arrangements involving data brokerage. Data brokerage transactions involving foreign persons are prohibited unless those parties are contractually bound not to forward the

data to covered persons—extending due diligence and contractual obligations beyond direct access arrangements.

The Bulk Data Rule became effective on April 8, 2025, with additional provisions taking effect on October 8, 2025. Clients should be aware that non-compliance carries significant civil and criminal penalties and should ensure prompt review of data-sharing practices, vendor agreements, and foreign partner obligations to mitigate enforcement risks.

On April 11, 2025, shortly after the first effective date of the Bulk Data Rule, the DOJ issued a suite of three policy and guidance documents to facilitate compliance with what the DOJ now refers to as the "Data Security Program." The suite of policy and guidance documents consists of: (1) an Implementation and Enforcement Policy; (2) a Compliance Guide; and (3) a set of frequently asked questions ("FAQs"). Notably, DOJ indicated in the Implementation and Enforcement Policy that it "will not prioritize civil enforcement actions against any person for violations of the Data Security Program that occur from April 8 through July 8, 2025, so long as the person is engaging in good faith efforts to comply with or come into compliance with the Data Security Program during that time." Organizations should use the Implementation and Enforcement Policy's 90-day "good faith" safe harbor to continue understanding their data flows and work on their existing compliance efforts, including continued risk assessments and compliance buildout, as applicable.

Supply Chain

ICTS Rule

The United States has increasingly exercised its regulatory authorities to safeguard supply chain security. One of the key national security tools expected to be used by the Trump Administration is the Department of Commerce's information and communications technology and services ("ICTS") supply chain regulations. These ICTS regulations have been developed over the past several years following Executive Order No. 13873, issued on May 15, 2019 during the first Trump Administration. These regulations were designed to strengthen efforts to prevent foreign adversaries, including China and Russia, from exploiting vulnerabilities in the U.S. ICTS supply chain.

Final implementing regulations were issued by the Commerce Department on December 6, 2024. Codified in Title 15 of the Code of Federal Regulations, Part 791, the rule prohibits certain transactions involving ICTS that are "designed, developed, manufactured, or supplied by persons, owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries," whenever the Secretary of Commerce,

in consultation with other federal officials, determines that such a transaction, or a class of transactions, poses an undue or unacceptable national security risk.

The rule defines ICTS transactions broadly. The definition encompasses technology integral to critical infrastructure, data hosting, computing, or storage connected software applications (including for use in autonomous vehicles), certain network or communications systems such as mobile networks, wireless local area networks, and satellite operations, and emerging or sensitive technologies, including AI, quantum computing, clean energy generation, drones, and robotics.

The U.S. government has already begun enforcing on these authorities. On June 20, 2024, the U.S. Commerce Department's Bureau of Industry and Security ("BIS") issued its first final determination under the ITCS rule, targeting Kaspersky Lab Inc., the U.S. subsidiary of a Russia-based antivirus software and cybersecurity company, and its affiliates, subsidiaries and parent companies. The determination prohibits Kaspersky from providing certain antivirus products and services in the United States or to U.S. persons wherever located. It also prohibits, in the United States or to U.S. persons, the resale of Kaspersky cybersecurity or antivirus software, its integration into other products and services, or its licensing for purposes of resale or integration into other products or services.

On January 14, 2025, BIS issued a final rule prohibiting certain transactions involving the import or sale of connected vehicles and certain related hardware and software with a nexus to the PRC or Russia. Specifically, the rule prohibits (1) the import of vehicle connectivity systems ("VCS") hardware, (2) the import or sale of connected vehicles that incorporate VCS and automated driving system software for model year 2027 and later; and (3) the import or sale of certain connected vehicles by PRC or Russian manufacturers in the United States for model year 2027 and later. BIS has also issued an advanced notice of proposed rulemaking targeting technology and software used in unmanned aircraft systems ("UAS") and seeking comments regarding the impact of foreign adversaries on the UAS supply chain and how the U.S. Commerce Department can mitigate those risks.

Going forward, the BIS Office of ICTS has identified several technology sectors that pose the most significant ICTS national security risks and are therefore expected to be the focus of regulatory scrutiny and enforcement. These include:

- Satellite access points
- Mobile network hardware
- Advanced and networked sensors

- Energy generation and storage
- Autonomous systems and robotics
- Semiconductors and microprocessors
- Infrastructure as a service
- Advanced cloud services
- Network security and operations
- Artificial intelligence
- Space technologies and systems
- Advanced computing
- Data privacy and cybersecurity
- Positioning, navigation and timing
- Quantum information technologies

The Executive Director of BIS's Office of ICTS has announced that the office will conclude several ongoing investigations and publish final determinations impacting these industries in the near future.

1260H List of Chinese Military Companies

Section 1260H of the 2021 National Defense Authorization Act requires the U.S. Department of Defense ("DOD") to publish annually a list of "Chinese military companies" that DOD determines are operating directly or indirectly in the United States (the "1260H List"). "Chinese military companies" are defined to include, among other things, entities that engage in providing commercial services, manufacturing, producing, or exporting, and:

- are directly or indirectly owned, controlled, or beneficially owned by, or acting as an agent of or on behalf of the People's Liberation Army ("PLA") or any organization under the Central Military Commission ("CMC") of the Chinese Communist Party, the State-Owned Assets Supervision and Administration Commission of the State

Council, or the State Administration of Sciences, Technology, and Industry for National Defense (among other Chinese governmental entities);

- are identified as a military-civil fusion contributor to the Chinese defense industrial base; or

- have a wholly owned subsidiary or affiliate, or parent company (if owning the entity with greater than 50 percent of equity control), that is a "Chinese Military Company."

DOD has since issued several rounds of 1260H List designations, including in January 2025, and designees have included a range of companies that span a wide range of industries, such as telecommunications, aerospace, automotive, electronics, semiconductors, and other ICTS sectors. Although designations on the 1260H List currently have no legal effect, that will soon change. Effective June 30, 2026, DOD generally will be prohibited from entering into, renewing, or extending a contract for goods, services or technology with any entity designated on the 1260H List or entities that they control, as well as from contracting with any company (including its subsidiaries or parent company) that engages with individuals or entities involved in lobbying activities on behalf of a 1260H designee.

Effective June 30, 2027, DOD will also be prohibited from purchasing end products or services produced or developed by an entity on the Section 1260H List indirectly through third parties. Being listed may also negatively affect a company's reputation in international markets, particularly in the United States, and can foreshadow the U.S. government's intent to add the entity to other restrictive lists, such as BIS' Entity List, which would result in additional U.S. export restrictions against the entity.

Enforcement

National security has become one of the most closely monitored areas for government enforcement activity. This national security landscape is constantly evolving, shaped by geopolitical tensions, shifting administrations and priorities, and technological advancements. While post-9/11 investigations and criminal prosecutions primarily targeted counterterrorism and focused on al-Qaeda and ISIS, in recent years DOJ has shifted its focus to economic "Great Powers" competition more reminiscent of the Cold War than the War on Terror. Under the Biden Administration, DOJ sought to focus on foreign influence operations, covering a wide range of activities. DOJ's Fraud Section actively investigated corporate violations of the Foreign Corrupt Practices Act ("FCPA"), particularly cases involving money laundering and bribery of foreign officials.

Similarly, NSD enforces the Foreign Agents Registration Act ("FARA"), which requires individuals, companies, and organizations receiving foreign funding to disclose their activities to prevent improper foreign influence over political activities in the United States.

As concerns over Iran, Russia, and China grew, and particularly after Russia's invasion of Ukraine, preventing the transfer of advanced technology to foreign adversaries became a top DOJ priority. In response, DOJ launched Task Force KleptoCapture and the Disruptive Technology Strike Force to combat these threats. The Corporate Enforcement Unit was also created to strengthen enforcement of sanctions and export controls. These initiatives elevated sanctions and export control violations from regulatory matters overseen by the Commerce and Treasury Departments to core national security threats, placing them on par with counterterrorism and counterintelligence.

Attorney General Pam Bondi has redirected DOJ resources to focus on drug cartels and transnational criminal organizations, leading to the disbanding of Task Force KleptoCapture, the Disruptive Technology Strike Force, and the Corporate Enforcement Unit. The FARA Unit has been instructed to prioritize traditional espionage threats, including foreign influence operations within the United States. Meanwhile, the Fraud Section's FCPA Unit has been directed to focus on cartel-related cases, and U.S. Attorney's Offices now have independent authority to prosecute national security violations, a responsibility that previously required Main Justice approval.

To bolster enforcement against transnational crime, the State Department designated eight drug cartels, including the Sinaloa Cartel and Mara Salvatrucha ("MS-13"), as Foreign Terrorist Organizations ("FTOs"). This designation expands legal tools for law enforcement and intelligence agencies, allowing them to prosecute cartel members under anti-terrorism statutes, seize assets, and impose financial sanctions to disrupt cartel operations. This, coupled with DOJ's reallocation of resources, signals an expectation of heightened enforcement.

Despite this shift, the Trump Administration has maintained and expanded certain economic security measures, particularly targeting China and Iran. CFIUS remains a key mechanism for blocking foreign acquisitions of critical American technology, while export controls on semiconductors and AI have been tightened to curb Beijing's access to sensitive technology. Instead of imposing blanket bans on Chinese-owned platforms like TikTok, the administration has pursued forced divestitures, requiring companies to transfer ownership to U.S.-approved buyers. These measures suggest that the administration continues to leverage economic tools to counter strategic rivals, even as DOJ enforcement priorities shift toward organized crime and domestic security concerns.

As the geopolitical landscape evolves, so too will the methods and targets of national security enforcement, shaping how the U.S. government navigates the complex interplay between security, foreign commerce, and international relations. Given these changes, businesses should reassess their compliance programs, conduct risk assessments of supply chains and vendors, and evaluate compliance programs to ensure alignment with evolving enforcement priorities.

Key Takeaways

In today's national security-driven regulatory environment, success in cross-border transactions hinges not only on financial acumen but also on anticipatory risk management, structural agility, and sustained regulatory intelligence. The accelerating convergence of economic and security interests across jurisdictions means even traditionally low-risk transactions now may warrant deliberate scrutiny. Firms must position themselves to act early, adapt quickly, and institutionalize compliance capacity.

The following strategies offer a practical roadmap for managing regulatory complexity:

Engage Early on Regulatory Risk

National security regulations—whether related to FDI, export controls, sanctions, or data access—are critical to transaction viability. Early engagement with in-house or external counsel enables tailored assessments across jurisdictions, sectors, and structures. With over two dozen EU Member States operating fragmented FDI regimes, and the expanding scope of the U.S. CFIUS process (e.g., into real estate and greenfield investments), even minority, passive or non-obvious investments may trigger scrutiny. Proactive evaluation helps identify filing triggers, mitigate risks, and design a filing strategy to avoid unnecessary transaction delays.

Structure Transactions with Regulatory Objectives in Mind

Global investors must assess how deal terms—voting rights, governance, board access, information rights—affect regulatory jurisdiction and scrutiny. Under the *America First Investment Policy*, a transaction's proximity to PRC entities, sensitive sectors, or national security infrastructure can significantly elevate risk. Allied-country investors may benefit from expedited "fast-track" treatment, while transactions involving adversary-linked investors face greater hurdles or outright restrictions. Transaction documents should reflect these realities through closing conditions, mitigation flexibility, and rights of withdrawal.

Scrutinize Fund and LP Composition

Investor identity is a critical diligence item. For funds operating in sensitive sectors or geographies, understanding the jurisdictions to which LPs are connected is essential. This is particularly important under the CFIUS framework and in jurisdictions that increasingly require disclosure of passive foreign LPs in private equity structures. Investors should implement LP screening protocols and adopt governance policies that anticipate disclosure requirements relating to beneficial ownership and the personal data of controlling persons. These measures also support broader diligence efforts under sanctions, data access, and ICTS regimes, where connections to foreign adversaries or other targeted persons are receiving heightened scrutiny.

Institutionalize Internal Compliance Capacity

National security regimes are increasingly document-intensive, requiring granular disclosures such as passport data, date of birth, residence, and nationality of key individuals. Investors should build internal systems to manage these requirements efficiently where possible, including standardized disclosures, pre-cleared filing materials, and template provisions for regulatory cooperation. Firms should also consider developing centralized policies to address DOJ bulk data rules, EU sanctions "best efforts" clauses, and ICTS supplier screening—particularly as compliance, disclosure, and monitoring obligations deepen under new regimes.

Strengthen and Expand Due Diligence Protocols

Cross-border investors and firms engaged in cross-border activity should implement standing risk assessment frameworks across core regulatory areas. Diligence checklists and deal review processes should be updated to include exposure to outbound investment restrictions, ICTS suppliers, DOJ data rules, cartel/TCO-related enforcement, and EU "No Russia" clauses. Due diligence must also assess vendor relationships, data flows, technology classifications, and beneficiary disclosures that could trigger review or post-close obligations. These reviews should be applied across all phases of the transaction lifecycle and refreshed regularly to reflect shifting priorities.

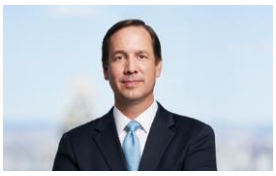
Plan for Divergent Compliance Obligations

Finally, the growing divergence between U.S. and EU regimes—on sanctions, FDI reviews, data governance, and outbound investment—demands careful cross-jurisdictional compliance strategies. Compliance with U.S. sanctions or BIS requirements does not ensure compliance with EU frameworks, particularly where EU entities or supply chains introduce EU jurisdiction. Firms must assess global structures for overlapping exposure, prepare for contradictory regulatory demands, and embed mechanisms for identifying and managing cross-border regulatory tension.

Debevoise & Plimpton continues to monitor national security developments and is ready to assist clients in navigating this shifting landscape—whether in assessing transaction risk, shaping policy-informed fund strategies, or responding to emerging regulations.

* * *

Please do not hesitate to contact us with any questions.



Carter Burwell
Partner, Washington, D.C.
+1 202 383 8149
cburwell@debevoise.com

Rick Sofield
Partner, Washington, D.C.
+ 1 202 383 8054
rcsofield@debevoise.com

Konstantin Bureiko
Counsel, London
+44 20 7786 5484
kbureiko@debevoise.com

Robert T. Dura
Counsel, Washington, D.C.
+1 202 383 8247
rdura@debevoise.com

Anne-Mette Heemsoth
Counsel, London
+44 20 7786 5521
amheemsoth@debevoise.com

Aseel M. Rabie
Counsel, Washington, D.C.
+1 202 383 8162
arabie@debevoise.com

Johanna N. Skrzypczyk
Counsel, New York
+1 212 909 6291
jnskrzypczyk@debevoise.com

Emily Kennedy
Associate, Washington, D.C.
+1 202 383 8112
eakenned@debevoise.com

Gabriel A. Kohan
Associate, Washington, D.C.
+1 202 383 8036
gakohan@debevoise.com

John M. Satira
Associate, Washington, D.C.
+1 202 383 8108
jmsatira@debevoise.com