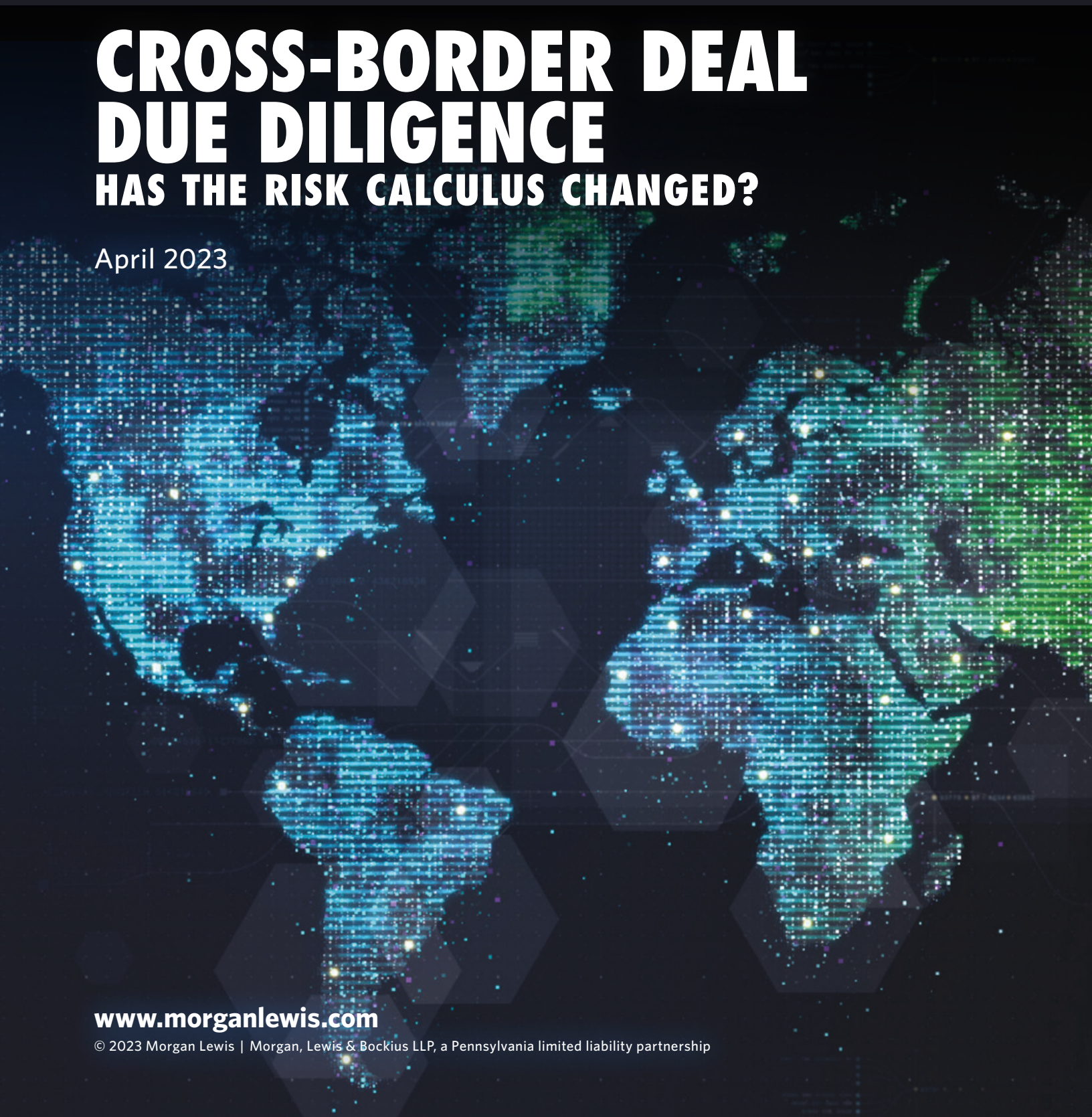
Morgan Lewis

REPORT

CROSS-BORDER DEAL DUE DILIGENCE

HAS THE RISK CALCULUS CHANGED?

April 2023



www.morganlewis.com

CROSS-BORDER DEAL DUE DILIGENCE: HAS THE RISK CALCULUS CHANGED?

Investors and targets generally view cross-border transactions from a risk-based perspective. That calculus applies not only to the manner in which an investment is made, but also to the level of diligence conducted, the timing for closing the deal, and the regulatory filings that need to, or should, be made to close the transaction effectively. This risk-based approach has been a baseline for how diligence has been and continues to be conducted for cross-border transactions.

In September 2022, however, that calculus may have been brought to the forefront as part of the Department of Justice's (DOJ) overall policy emphasis on corporate compliance. Deputy Attorney General Lisa Monaco, followed by Assistant Attorney General for the Criminal Division Kenneth Polite, and Principal Associate Deputy Attorney General Marshall Miller seemed to raise the bar by highlighting DOJ's focus on post-acquisition remediation when violations or noncompliance were identified during the diligence process.[1] Miller's comments from his September 20, 2022 keynote speech at the Global Investigations Review conference provide insight into how DOJ views post-acquisition remediation and appropriate diligence levels:

> Acquiring companies should be rewarded – rather than penalized – when they engage in careful pre-acquisition diligence and post-acquisition integration to detect and remediate misconduct at the acquired company's business…[W]e will not treat as recidivist any company with a proven track record of compliance that acquires a company with a history of compliance problems *as long as those problems are promptly and properly addressed in the context of the acquisition.* (emphasis added)[2]

In March 2023, DOJ reiterated the importance of corporate compliance overall, while highlighting how detailed inquiries into a company's compliance efforts should be part of the diligence process in mergers, acquisitions and other investments.[3] While not a new concept, as Monaco established the baseline with her first presentation on September 15, 2022, DOJ's strong emphasis on these points[4] suggests that

---

[1] *See, e.g.,* Memorandum: Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group, US Department of Justice (September 15, 2022); Deputy Attorney General Lisa Monaco Delivers Remarks on Corporate Criminal Enforcement, US Department of Justice (September 15, 2022, New York); Assistant Attorney General Kenneth A. Polite Delivers Remarks at the University of Texas Law School (September 16, 2022, Dallas, Texas); Principal Associate Deputy Attorney General Marshall Miller Delivers Live Keynote Address at the Global Investigations Review Conference (September 16, 2022, New York); Assistant Attorney General Kenneth A. Polite Delivers Remarks on Revisions to the Criminal Division's Corporate Enforcement Policy (January 17, 2023, Washington, DC).

[2] Principal Associate Deputy Attorney General Marshall Miller Delivers Live Keynote Address at Global Investigations Review, at p. 2 (September 20, 2022, New York).

[3] "Evaluation of Corporate Compliance Programs," US Department of Justice, Criminal Division (March 2023), at pp. 8-9.

[4] Others within DOJ supported and reinforced Monaco's statements, noting that prompt remedial as well as "careful pre-acquisition diligence and post-acquisition integration" are crucial to mitigating any damage to US interests. Justice as well as other agencies view these steps as essential to the remediation of "problems [that] are promptly and properly addressed in the context of the acquisition." "Principal

investors and targets reexamine the manner in which diligence is conducted, the areas where enhanced diligence may be needed, and the value that representations in lieu of diligence may or may not have as part of the reasonable efforts exercised during the diligence period. While due diligence remains a risk-based process that varies depending upon the circumstances of each investment, DOJ's pronouncements appear to indicate an increasing interest in the approach to ensure that unexpected or prolonged delays do not affect national security or other US government interests.

DOJ, however, does not stand alone in its focus on pre-investment diligence. Beginning with the Trump administration and continuing through the Biden administration, the executive branch has identified key areas of concern directly affecting the industrial base and US government access to resources, technologies, and products essential to the evaluation of risks associated with changes in US ownership, control, or influence. Executive Order 14083, which directed the Committee on Foreign Investment in the United States (CFIUS) to evaluate specific areas such as the supply chain, past acquisition or investment history, the impact of investments on the United States' future lead in key technologies, and sector, industry, or technology consolidations, formed the basis for reminding parties where national security sensitivities may arise.

Coupled with swift and impactful expansions of export controls by the US Department of Commerce, changes in the focus of the International Traffic in Arms Regulations, and explosive growth in the use of sanctions based on the Ukraine conflict, investors now face a risk calculus that is no longer predicated solely on military, defense, or intelligence sectors. To paraphrase President Biden when discussing other executive orders and commenting on the 100-day supply chain review he ordered under EO 14017,[5] national security now covers not only traditional defense, military, and intelligence objectives, but also corruption, healthcare, biotechnology, telecommunications, public welfare, financial well-being, and climate change. In a sense, no sector of the US economy falls outside the scope of national security interests, and if everything is considered within the scope of national security, then identifying the true national security issues becomes more complex and difficult to discern.

This view has been adopted through other governments' approaches to foreign direct investment reviews (FDI) and export controls.[6] Since 2018, over 30 other governments have either expanded or enhanced their existing FDI national security review processes or established new frameworks to evaluate these issues. The same has occurred with export controls, the most recent iteration of which can be seen in the October 7, 2022 announcement by the Department of Commerce of stringent new export controls on advanced semiconductor and supercomputing technologies and products.

Although DOJ has consistently been responsible for the enforcement of criminal violations of US export laws, DOJ has played less of a visible role in the CFIUS process until the last two or three years, during which it has taken the lead on a larger number of cases under CFIUS reviews, participated in the enforcement of breaches of mitigation agreements, and provided detailed input to the CFIUS on

---

Associate Deputy Attorney General Marshall Miller Delivers Live Keynote Address at Global Investigations Review," (New York, September 20, 2022), at p. 2.

[5] America's Supply Chains.

[6] Since 2018, over 20 countries have enhanced, expanded, or established FDI regimes to evaluate cross-border investments. The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) expressly directed the president to increase outreach to other countries to multilaterize FDI reviews. The results of that outreach have resulted in FDI regimes or enhancements in Japan, the United Kingdom, the European Union, Italy, France, China, Russia, Germany, Canada, India, and Australia, as well as other countries.

counterintelligence and national security concerns through both the FBI and other offices within DOJ. Concerns regarding personal information, data aggregation, and the power of information more generally have placed DOJ at the forefront of CFIUS reviews, in some instances overshadowing the US Department of Defense.

Given this mix, what do these public statements and changes mean for investment due diligence? What changes may be needed to the diligence process to both protect investors and targets, while not unnecessarily impeding the pace of investment? One thing is clear: maintaining the status quo of using template language, relying on representations or certifications, and conducting post-closing "clean up" carry new risks for investors. Within this environment, it would be prudent for investors and US targets preparing for investment to update their diligence approach—whether checklists, questions, document collection, or deal documents. In that vein, this Report suggests that the US government has signaled a key interest in at least the following areas, each of which is crucial to an understanding of the value of the investment being made and the back-end risks an investor inherits post-closing.

AREAS OF US GOVERNMENT INTEREST

The US government has maintained an interest in certain national security issues for over 40 years. Export controls have been a mainstay of diligence requests in order to determine whether a company supports or supplies US government agencies with national security missions. For example, diligence questions routinely ask whether a US company is International Traffic in Arms Regulations (ITAR) registered or manufactures ITAR-controlled products or technology, not only to manage a foreign investor's assessment of the likely interest the CFIUS may have in a deal, but also to determine notification obligations under ITAR 122.4 and whether existing export licenses may transfer once the US company is foreign owned.

The same degree of inquiry, however, did not consistently apply to dual-use export controls under the Export Administration Regulations (EAR). The EAR, long viewed as the more flexible regime and the one where fewer controls applied, generally received a more cursory review during diligence. Since registration or any form of notification similar to the ITAR is not required, many investors comfortably relied upon export classification representations by US companies to evaluate any national security concerns. US companies also relied more heavily on the broader classifications that apply under the EAR, especially EAR99, a basket category that covers a range of wholly unrelated products/technology, such as visualization software that replicates 3D scenes for training and simulation, ballistic computer circuit boards (34 MM x 23mm x 4 mm: 2 grams), cloud-delivered event-simulation and visualization training tools, information about the positioning of mounts for mine-hunting sonars, and gun mounts.

EAR99 classifications, however, do not include any technical descriptions but simply represent a catch-all designation to identify items, technology, or software that are not otherwise enumerated on the Commerce Control List (CCL). Given the variety of items that can be considered EAR99, obtaining a response during diligence that a company or organization manufactures, develops, designs, or otherwise produces EAR99 items provides little substance upon which to gauge the importance of the classification. In addition, considering the EAR99 classification as an indication by the Department of Commerce that the items, technology, or software have little criticality to national security interests would fail to take into account how many of these items may play a direct or indirect role in facilitating or enhancing national security objectives.

These examples highlight, in part, why due diligence updates in at least the following areas would be beneficial to the parties and to the evaluation of the risks associated with any regulatory interest in the deal:

- Export controls including critical and emerging technologies
- Supply chain
- Investor's relationships (direct or indirect) with China
- Cybersecurity
- Access to data
- Sanctions compliance
- Foreign investor compliance with US laws and regulations

Given these areas of US and foreign government interest and the shifting geostrategic situation not only with China but also with Russia, Europe, and other countries, parties should consider including additional questions as part of the diligence process to delve more deeply into how these interests can affect government concerns. Addressing regulatory issues early in the deal process helps manage, minimize, or mitigate the potential for deal disruption based on regulatory reviews.

ADDITIONAL QUESTIONS TO CONSIDER

As part of the diligence process, parties that seek to minimize or more accurately assess the national security risks in cross-border investments should consider updating at least the following areas and collecting underlying documentation to support the responses prior to closing a deal[7]:

Export-Controlled Technologies and Related Items

- Technology applications:
    - What applications currently exist for the products/technology produced by the US company and the investor?
    - What applications may be developed?
    - What funding currently supports the developing applications?
    - What funding supported prior applications that were embedded into current products?
    - Is the technology considered emerging—and under what definition?
    - Is the technology considered disruptive—and by whose definition?[8]
    - Is the technology foundational—both as a legacy technology and as the basis for expanding applications in the emerging or disruptive realms?
- Multilateral technology controls:

[7] The areas of interest represent a select group of areas where the US government has expressed concern. The list is not designed to be comprehensive or to provide legal advice. It is focused on some of the key areas where additional information would be beneficial to the parties.

[8] On February 16, 2023, the Departments of Justice and Commerce jointly announced the creation of the Disruptive Technology Strike Force to enforce US laws that are designed to protect US advanced technologies from illegal acquisition by "adversaries." "Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force" (Office of Public Affairs, Department of Justice) (February 16, 2023).

    - What public studies—whether from the United States or abroad—identify specific technologies of concern or interest?
    - What other governments maintain an interest in the same technologies as the United States?
    - Are there multilateral export controls already in place?
    - What jurisdictions require licenses, and which permit the use of exceptions, open general licenses, or exemptions?
    - What countries apply unilateral controls to any products or technology? For example, the Netherlands and Japan maintain leads in semiconductor manufacturing equipment, but do they also impose more restrictive licensing on transfers to other countries?
- "Made in China 2025" and other similar policies that reflect a civil to military or military to civil transfer of technologies:
    - How may technology be used?
    - Was the technology originally developed with an agnostic purpose?
    - Who participated in the development and what ties did the party have to government agencies with responsibility for implementing technology policies?
    - What US government funding was obtained and for what purpose?
- Whether "foreign adversaries" may use technology in a manner detrimental to US interests:
    - "Detrimental to US interests" should be viewed in terms of US government objectives rather than conclusory statements that indicate "it is low-level technology" or "it is available from foreign sources."
    - Consider the avenues by which the technology may be accessed—in essence, is the detriment to US interests direct or indirect.
- Consider the reliability of the export classifications provided and obtain underlying documentation for any classification, whether Department of Commerce classifications, Commodity Jurisdiction determinations, or self-classifications provided by the company.
    - When evaluating self-classifications, consider the "source." Was the classification prepared and provided by someone technically knowledgeable, trained in export controls and in coordination with resources who understands the legal significance of the classification?
    - If the company obtained a commodity classification automated tracking system (CCATS) or a commodity jurisdiction (CJ), request the underlying submissions, not just the decision.
- Consider how "critical technologies" are defined—for example, the establishment of the Office of Critical Technologies as part of the Office of the President or CFIUS or through EO 14083.
- The tie between intellectual property (IP), export controls, and "controlled unclassified information" (CUI):
    - What company IP is also export controlled?
    - What transfers of IP have occurred that implicate both export controls and CUI?
    - What authorizations exist or have been used to transfer IP?

- What tracing mechanisms exist—outside of contract terms—to assess where IP is shared?

Supply Chain

- The global nature of supply chains and the risks associated with allowing other parties or countries to leverage that global activity creates the need for a more in-depth understanding of supply chains. Thus, identifying the supply chain, both vertically and horizontally, becomes essential to national security analyses.
- First, second, and third tier supply chain identification is no longer adequate. Consider addressing more than the top suppliers and deeper than the third tier.
- Understand who within the supply chain is a sole source and from what country or countries. This takes into account the concept of indigenous capabilities, "friend-shoring," and "offshoring."
- Understand who within the supply chain is a sole qualified source and from what country or countries. Distinctions exist from a quality and competence perspective between a sole source and a sole qualified source.
- Although NAICS codes are no longer foundational to a CFIUS analysis, they may be evaluated as part of EO 14083's direction to consider consolidations within industry sectors.
- Understand what company business includes Defense Priorities and Allocations System (DPAS) ratings, whether directly through rated orders or indirectly through mandatory flow-down provisions.
- Evaluate the consequences to the supply chain by choke points (i.e., one country provides the majority of the supply), leverage (i.e., one customer is responsible for the majority of purchases) or competitors (i.e., multiple companies vie for the same limited suppliers and resources).

Purchaser/Investor Relationship with China

- Recent geostrategic and geopolitical circumstances highlight the importance of the Far East region on national security issues. Congress and the executive branch have focused on China and Hong Kong by implementing policies that change the manner in which the US government views the risks associated with dealing in these regions. Thus, understanding the impact of the increased focus on China and Hong Kong is an area where additional diligence becomes key.
- US government policies consider China as the "pacing challenge for the United States" and the "near peer" or "peer competitor" to the United States. This places China in a unique position of being viewed as a country with leverage across technologies and industries.
- With that leverage, areas for further diligence include:
    - How long has the foreign purchaser/investor had relationships in China
    - What kind of relationships are they (e.g., joint ventures, research and development centers, marketing agreements, or baseline supply chain agreements)?
    - What Chinese law requirements apply to the relationships?
    - Have those legal requirements been enforced and how?
    - What parties were involved (e.g., universities, research institutes, distributors, state-owned enterprises, state-directed enterprises, government laboratories, or university professors or students)?

- Are any of the parties now sanctioned? If so, at what point during the relationship were sanctions imposed? Did the company make any changes to the relationship based on those sanctions? If so, what changes?
- What export licenses were obtained for the transfer of any technology from the United States to China? If no licenses were obtained, what authorizations were used? Did the authorizations change over the course of the relationship? If so, how?
- Was any of the technology routed through third parties? For example, did the US company enter into an agreement with a third party which then forwarded the technology to China?
- Were Chinese funds used to make the investment (e.g., Chinese banks or Chinese venture capital funds)? Were the funders screened and, if so, with what results?

Cybersecurity

- What cybersecurity programs does the purchaser/investor have? What laws control the cybersecurity program?
- What notices has the investor provided to government agencies, whether US or non-US, regarding cybersecurity incidents?
- Does the investor utilize software applications or communications mechanisms to raise national security concerns?
- What cybersecurity programs does the US business have?
- How many cybersecurity breaches has the foreign purchaser/investor experienced?
    - How many have been reported?
    - To which government agency (US or foreign) were they reported?
    - How were they remediated?
    - Do vulnerabilities remain? If so, on what timeline will they be remediated?
- Did the vulnerabilities and cybersecurity breaches result in the loss of data considered critical to US national security or other interests? If so, what specific data? For how long did the breach continue?

Access to Data

- Data – personal, technical, or financial/business
    - What data does the US business possess?
    - How is it protected?
    - Who has access?
    - How can access be terminated?
    - How many breaches have occurred?
    - To whom were they reported?
    - How were they remediated?
- What data access is the foreign purchaser/investor requesting?
- How is data generally protected?

- What additional considerations apply to the foreign purchaser/investor's cyber requirements (e.g., privacy)?

Sanctions Compliance

- How does the foreign purchaser/investor comply with US sanctions?
- Does the foreign purchaser/investor have a sanctions compliance program?
- Does the foreign purchaser/investor conduct business inconsistent with US sanctions' objectives?
- Is the foreign purchaser/investor subject to blocking or other home country statutes that impede compliance with US sanctions programs?
- How does the foreign purchaser/investor interpret US sanctions statutes from a compliance perspective?
- Does the foreign purchaser/investor's home country abide by multilateral sanctions programs (e.g., programs or policies agreed to at the United Nations)? If so, which ones? If not, why not?
- Has the foreign purchaser/investor's home country government made public statements contrary to US sanctions policies or passed laws and regulations that create conflict with US sanctions compliance?
- Is the foreign purchaser's/investor's home country part of the multilateral sanctions engagement for the Ukraine conflict?

Foreign Investor's Compliance Posture Under US Laws and Regulations

- Compliance with US laws and regulations is an indication of reliability, which can be important to clearing a CFIUS transaction.
- FIRRMA expressly requires consideration of a foreign purchaser/investor's compliance with certain US laws and regulations, such as export control and sanctions laws. Given this objective, what does compliance mean for the investor/purchaser? Is this type of inquiry a first foray into the use of the CFIUS process to potentially change foreign investor/purchaser behavior that may be inconsistent with US laws and regulations?
- Parties that experience difficulties or challenges with compliance may face increased scrutiny during a CFIUS review and may find their transactions subject to mitigation to address the view that the foreign purchaser/investor may be unable to handle compliance requirements as part of the CFIUS clearance.
- Particular challenges arise with the Office of Foreign Assets Control (OFAC) and the ITAR, where the agencies have expressly extended jurisdiction to foreign parties for violating the OFAC regulations and the ITAR. Recent public statements by the European Commission indicate that "the EU does not recognize the extra-territorial application of third country sanctions and considers it contrary to international law." (citing COM/2021/32 final)
    - Reconcile compliance obligations.
    - Consider the impact of foreign investor's/purchaser's compliance with US laws as a rebuttable indication that mitigation measures may be part of any FDI review.

Updating information collection during the diligence process can place investors and US companies in a more favorable position when deciding whether national security issues exist. Investment due diligence is an organic process that changes as external conditions shift. Whether those conditions include trade tensions, sanctions, transparency regarding ultimate beneficial ownership or new government alignments, transaction diligence processes provide a front-line view into areas of greatest risk.

CONTACTS

If you have any questions or would like more information on the issues discussed in this report, please contact any of the following:

Author		
Giovanna M. Cinelli	+1.202.739.5619	giovanna.cinelli@morganlewis.com
Washington, DC		
Kenneth J. Nunnenkamp	+1.202.739.5618	kenneth.nunnenkamp@morganlewis.com
David Plotinsky	+1.202.739.5742	david.plotinsky@morganlewis.com
Ulises R. Pin	+1.202.373.6664	ulises.pin@morganlewis.com
Heather C. Sears	+1.202.739.5246	heather.sears@morganlewis.com
Katelyn M. Hilferty	+1.202.739.5674	katelyn.hilferty@morganlewis.com
Christian Kozlowski	+1.202.739.5677	christian.kozlowski@morganlewis.com
Eli Rymland-Kelly	+1.202.739.5657	eli.rymland-kelly@morganlewis.com
Ivon Guo	+1.202.739.5163	ivon.guo@morganlewis.com
Boston		
Carl A. Valenstein	+1.617.341.7501	carl.valenstein@morganlewis.com
Houston		
Casey Weaver	+1.713.890.5409	casey.weaver@morganlewis.com
Brussels		
Christina Renner	+32.2.507.7524	christina.renner@morganlewis.com
Frankfurt		
Dr. Michael Masling	+49.69.714.00.753	michael.masling@morganlewis.com
London		
Joanna Christoforou	+44.20.3201.5688	joanna.christoforou@morganlewis.com

ABOUT US

Morgan Lewis is recognized for exceptional client service, legal innovation, and commitment to its communities. Our global depth reaches across North America, Asia, Europe, and the Middle East with the collaboration of more than 2,200 lawyers and specialists who provide elite legal services across industry sectors for multinational corporations to startups around the world. For more information about us, please visit www.morganlewis.com.