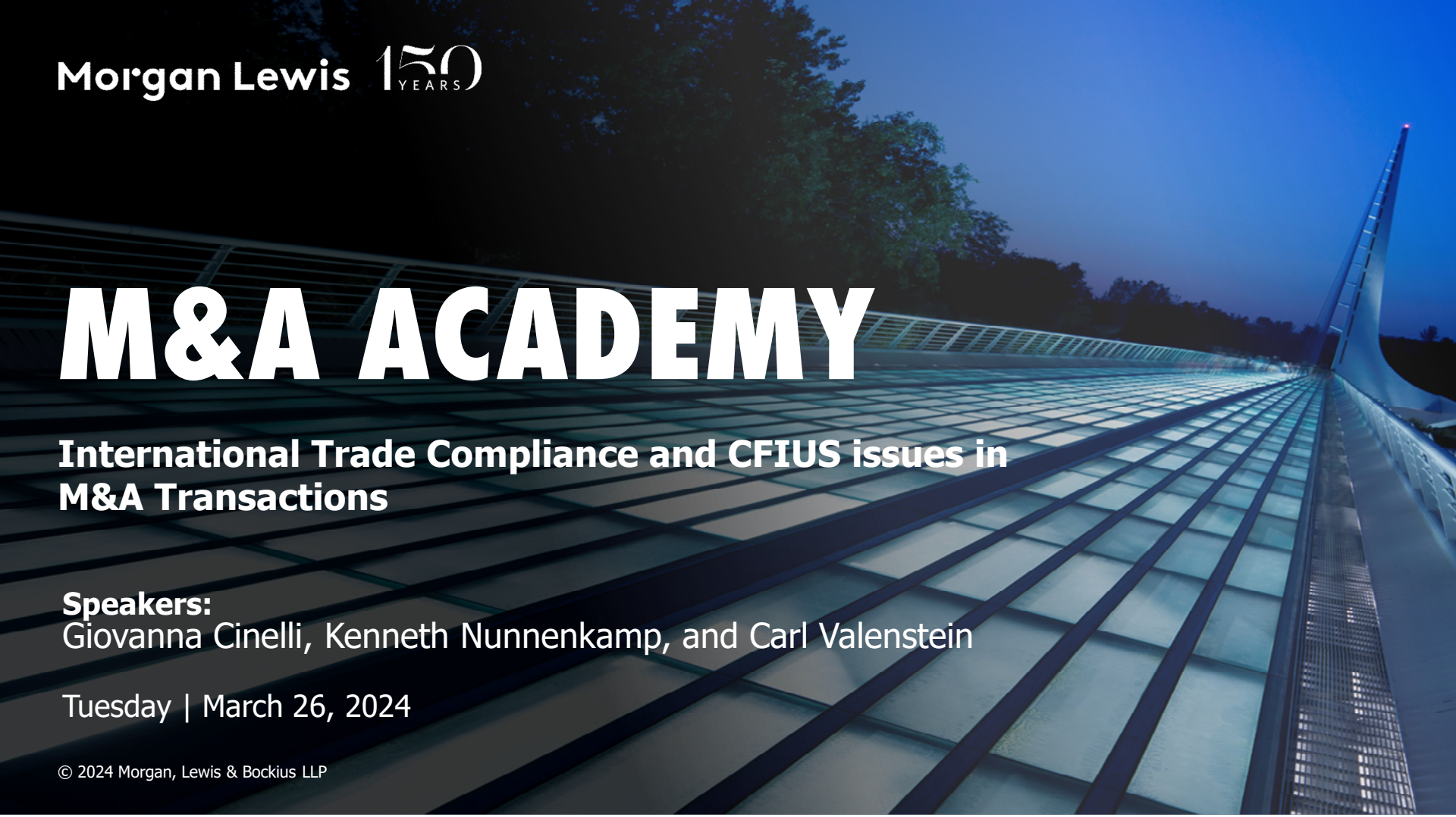


Morgan Lewis 150 YEARS

M&A ACADEMY

International Trade Compliance and CFIUS issues in M&A Transactions

Speakers:
Giovanna Cinelli, Kenneth Nunnenkamp, and Carl Valenstein

Tuesday | March 26, 2024

Introduction

1. Conducting Risk-Based International Compliance Due Diligence in M&A Transactions
2. Clearing M&A Transactions with CFIUS

Conducting Risk-Based International Compliance Due Diligence in M&A Transactions

Key International Compliance Risk Areas and Associated Liabilities

Guidance and Case Law on Successor Liability

Practical Approaches to Conducting Risk-Based International Compliance Due Diligence

Key Diligence Questions

Use of International Compliance Due Diligence

Need for Specialized Contractual Provisions

Considerations for Sellers

Considerations for Buyers

Key International Compliance Risk Areas and Associated Liabilities

Anti-Corruption (FCPA and UK Bribery Act, as well as applicable local anti-corruption laws) - liabilities can include criminal and civil fines, jail time for individuals, debarment, deferred prosecution agreements or consent decrees, follow-on civil litigation.

Sanctions Laws (US, UK and EU) - liabilities can include criminal and civil fines, jail time for individuals, debarment, deferred prosecution agreements or consent decrees.

Export and Re-Export Laws (US, UK and EU) - liabilities can include criminal and civil fines, jail time for individuals, denial of export privileges, deferred prosecution agreements or consent decrees.

Key International Compliance Risk Areas and Associated Liabilities

Anti-Boycott Laws (US) – liabilities can include criminal and civil fines and loss of tax benefits.

Customs/Import Compliance and Trade Actions/Remedies – liabilities can include increased duties, penalties and forfeitures, exclusion of products from the United States, follow on civil litigation, including FCA claims.

National Security (CFIUS/FOCI/NISPOM) – liabilities can include blocked transactions, loss of government contracts, debarment, suspension of exporting and other privileges, criminal and civil fines as well as intangible penalties, such as mitigation agreements or other proscriptions.

Note that additional areas could include privacy and international tax.

Successor Liability

- In certain areas of international compliance, including the FCPA, sanctions and export and import controls there is clear precedent establishing the liability of the buyer for misconduct of the target company occurring before the closing under the theory of successor liability.
- In the FCPA area, DOJ/SEC have provided specific guidance in the joint 2020 FCPA Guide (Second Edition) how to minimize successor liability.
- In the trade area, the Department of Commerce began asserting successor liability in 2002 in the *Sigma Aldrich* case.
- The Department of State has a long history of imposing strict successor liability on companies who purchase entities that committed violations prior to the acquisition. *See Consent Agreement with L-3/Goodrich; Consent Agreement with General Motors/General Dynamics; Consent Agreement with L-3/Titan; Consent Agreement with Meggitt USA, Inc.; Consent Agreement with Multi-Gen Paradigm*
- In the customs areas, successor liability was found in the following cases: *Shields Rubber Corp* (1989), *Ataka America* (1993), *Adaptive Microsystems* (2013) and *CTS Holding* (2015).

Recent DOJ Guidance on Corporate Compliance in M&A Transactions

DOJ Criminal Division; Evaluation of Corporate Compliance Programs (2023)

- A well-designed compliance program should include comprehensive due diligence of any acquisition targets, as well as a process for timely and orderly integration of the acquired entity into existing compliance program structures and internal controls.
- Pre-M&A due diligence, where possible, enables the acquiring company to evaluate more accurately each target's value and negotiate for the costs of any corruption or misconduct to be borne by the target. Flawed or incomplete pre- or post-acquisition due diligence and integration can allow misconduct to continue at the target company, causing resulting harm to a business's profitability and reputation and risking civil and criminal liability.
- The extent to which a company subjects its acquisition targets to appropriate scrutiny is indicative of whether its compliance program is, as implemented, able to effectively enforce its internal controls and remediate misconduct at all levels of the organization.

Recent DOJ Guidance on Corporate Compliance in M&A Transactions

DOJ Criminal Division; Evaluation of Corporate Compliance Programs (2023)

- Due Diligence Process – Was the company able to complete pre-acquisition due diligence and, if not, why not?
- Integration in the M&A Process – How has the compliance function been integrated into the merger, acquisition, and integration process?
- Process Connecting Due Diligence to Implementation – What has been the company's process for tracking and remediating misconduct or misconduct risks identified during the due diligence process?

Safe Harbor Policy

- Under the DOJ's "Safe Harbor Policy", if an acquiring company makes a good faith effort to self-disclose previously unknown criminal misconduct by the target company within six months of closing a transaction, the acquirer will generally receive a presumption of a criminal prosecution declination.

- Disclosing companies must also fully cooperate with any ensuing investigation by the government; and fully remediate the disclosed conduct within one year of the closing date of the transaction, including any restitution and disgorgement.

- Although the Safe Harbor Policy thus presents companies with a carrot to encourage VSD, the stick is that DOJ will be comfortable with harsher repercussions if companies fail to disclose, and misconduct is later discovered by the government.

DOJ/SEC Guidance – FCPA

- The DOJ also suggests that parties use the Opinion Release procedure for M&A transactions. While Justice has issued several opinion releases in the M&A context, this process can be time consuming and may, according to the DOJ, contain more stringent requirements that may be necessary in all circumstances.
- It is important to emphasize that while, by following the above advice, you may be able to avoid or minimize successor liability for the acquiring company, you will not avoid the liability for any past FCPA violations of the target company being acquired, and such liability can materially adversely affect the value of the proposed investment.

Risk-Based Due Diligence

- There is very little guidance on what level of risk-based international compliance due diligence is required for a particular target and the scope of due diligence will depend upon the amount of time and resources you have available and the particular international compliance risks associated with the target.
- There is a fundamental difference between responding to a governmental enforcement action or pursuing an internal investigation, on the one hand, and performing M&A due diligence on the other.
- While the client or deal team will want you to estimate potential exposure it is very difficult to do that accurately because of the wide range of potential monetary and non-monetary liabilities and long -5 year-statute of limitations. It is particularly challenging when the target has limited compliance programs in place and may have unknown violations.

Risk-Based Due Diligence

- Government enforcement cases and internal investigations focus on discovered conduct that may be a violation. Internal investigations may require intensive document review and analysis, electronic mail collection, and witness interviews. Depending upon the subject matter, this process may take many months and even years, especially if the Government is concerned that the conduct at issue has jeopardized an important national security or foreign policy interest.
- In contrast, risk-based international compliance due diligence attempts to identify the international compliance risk areas of a target in a relatively short period of time – often with limited access to critical documents and personnel.

Risk-Based Due Diligence

The risk assessment should focus on the following:

- The nature of the target's business and reputation in the market.
- The industry and the countries in which the target operates.
- The extent to which the target is exposed to certain international compliance risk areas and how it approaches compliance in these areas.
- The extent to which the target utilizes third parties in dealing with customers and regulators.
- The extent to which the target interacts with government officials or has government customers.
- The strength of the target's existing compliance program and internal controls.

Practical Approaches

Choose your team wisely: The international compliance due diligence team should include those subject matter experts (SME) best suited to address the specific issues involved in a transaction. These include transaction and regulatory counsel with experience in the field, as well as in-house personnel from the legal, finance and compliance departments. Some cases may benefit from third party consultants with a specific expertise tailored to the risks at issue. Each team varies somewhat and a cookie cutter approach generally increases the costs of the transaction.

Understand what you need to investigate or review and the timeline: Determine the amount of time, scope of international compliance due diligence and allocation of responsibilities. Transactional lawyers focus on the high-level areas of risk given the target's business model and international operations; regulatory counsel provides laser focused input on the areas where greatest or most consistent risk exists; the in-house compliance department can supplement the assessment provided by outside counsel or SMEs; and the finance department focuses on books and records and accounting controls, including any material weaknesses in internal controls.

Practical Approaches

Understand what can be obtained through the data room: Because information concerning international compliance issues is rarely included in publicly available materials or in a data room, it is critical to create a separate work stream to conduct international compliance due diligence. Often a supplemental international compliance questionnaire is submitted followed by one or more interviews of the target's compliance and business personnel to understand the international compliance risks and to focus on areas for further inquiry.

Address violations or noncompliance up front and in the deal documents: If enforcement cases or internal investigations are discovered or disclosed, it may be necessary to bring in outside counsel skilled in the legal issues involved (*i.e.*, an SME) to assess the potential impact on the target and its business/value pursuant to a common interest agreement to prevent waiver of the privilege.

Practical Approaches

Understand the risks and where additional diligence is needed: One of the biggest challenges in conducting due diligence is determining when a desk-top review or interview of target personnel may be insufficient and when certain potentially high-risk transactions should be audited in more detail. This kind of audit can be very time consuming and international compliance issues are often difficult to detect without a full investigation.

Practical Approaches

Prepare to deal with foreign affiliates or subsidiaries: Most transactions involve international activities or parties. Your transaction may involve a target's foreign subsidiaries, foreign suppliers or vendors or foreign consultants and customers. Uncovering potential violations in any of these situations where foreign parties may be involved presents an additional challenge. Privacy requirements, the extraterritorial effect of US laws and regulations as well as interpretative consistency may hamper the diligence process.

Note that, to the extent there is a limited opportunity to conduct pre-acquisition international compliance due diligence, it is essential to conduct more in-depth post-acquisition international compliance due diligence to eliminate ongoing compliance problems. Also critical is the integration of the acquired company into the acquiring company's international compliance program.

Use Of Due Diligence

Once the risk-based international compliance due diligence is concluded, you need to assess the effect of what you have found on the overall transaction. Options include:

(a) proceeding as planned or renegotiating to account for risks,

(b) delaying closing until further due diligence is done or active cases/investigations are resolved and then reassessing or renegotiating, or

(c) walking away.

Use Of Due Diligence

Questions to consider include:

1. How much of the target's revenue stream/business model could be affected?
2. How many key employees, intermediaries, or customers may be affected or need to be retrained or terminated?
3. Is the target's business model/culture so different that it will be difficult to integrate it into your compliance program without the business being materially affected?
4. How much uncertainty is there concerning whether you have had sufficient time to assess compliance risks or to resolve known compliance issues and quantify associated costs and liability?
5. Can identified risks be addressed through contractual provisions or revaluation? Or are they so serious that they should be resolved prior to closing?

Need for Specialized Contract Provisions

- It is market practice to include specialized FCPA and other international compliance representations and warranties in transactional documents and not to rely on general compliance with laws representations and warranties, which are often qualified with no material adverse effect language.
- These specialized representations and warranties serve two purposes; first, to force disclosure of compliance issues and, second, in private company transactions where representations and warranties survive the closing, to set up special indemnities, which may be secured by special escrows.

Considerations for Sellers

Sellers should consider the following with respect to international compliance issues:

1. Prepare due diligence for buyers by doing a self-assessment of ongoing compliance issues, including hotline complaints, internal investigations, or external enforcement cases.
2. Prepare any required disclosure information and determine at what time and in what manner to disclose it to buyers.
3. Be prepared for a discussion with buyers concerning the potential materiality of international compliance issues in terms of purchase price adjustments in public deals where representations, warranties and indemnities do not survive the closing or special escrows in private deals where they do.
4. Be prepared for a requirement by buyers that the international compliance issues be disclosed to enforcement authorities as a condition of closing.

Considerations for Buyers

Buyers should consider the following with respect to international compliance issues:

1. Prepare due diligence plan and allow for adequate time where possible; do not let the sellers delay disclosure until the 11th hour.
2. Adjust the due diligence plan and resources depending upon what is learned.
3. Discuss with sellers and buyers' own counsel potential materiality of international compliance issues and level of uncertainty.
4. Consider international compliance representation and warranty insurance products.
5. Consider adequacy of proposed special escrows in private deals where issues have been identified.
6. Consider whether forcing disclosure to enforcement authorities will lead to timely resolution of international compliance issues before closing.
7. Prepare pre-acquisition the post-acquisition international compliance integration plan.
8. If the target is a public company, consider SEC disclosure obligations and potential issues relating to material weaknesses in internal controls.

Clearing M&A Transactions with CFIUS - Introduction

- The United States has a long history of reviewing cross-border investment (FDI) to assess the national security implications of these types of transactions. With more than 20,000 to 40,000 cross-border investments a year, most transactions, however, occur outside the purview of US government review.
- The United States maintains a robust review process, managed by the Committee on Foreign Investment in the United States (CFIUS), which evaluates the national security impact of cross-border investments at any level.
- Congress amended the CFIUS process in 1988, 1993, 2007, and 2018. In each iteration, Congress further consolidated the Committee's authorities, expanded its jurisdiction and identified the factors that matter to the US Government member agencies of CFIUS from a national security perspective.
- CFIUS' jurisdiction has been enhanced by Executive Order 14083 – which outlined additional factors relevant to any CFIUS national security analysis.

Clearing M&A Transactions with CFIUS - Introduction

- In 2018, Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA) which updated CFIUS and added a mandatory process to CFIUS' review
- FIRRMA also directed the President to engage in multilateral discussions to encourage other countries to establish or enhance national security reviews of cross-border investments.
- FIRRMA and the regulations created a cascading effect–as CFIUS issued its regulations, developed its policies and interpretations, restructured its offices and increased its resources, other countries changed their FDI review processes as well.
- This cascading effect has resulted in new or enhanced national security review regimes in Japan, Australia, the United Kingdom, the European Union, Germany, France, Italy, India, New Zealand, Spain, China and Russia.
- In concert with CFIUS, these regimes help protect national security interests of the United States and its allies and partners.

Background

- Longstanding review by the United States of cross-border investments for national security implications
  - Originally established in 1975
  - Focused on "classic" national security issues
  - Conducted on an ad hoc basis
  - Predicated on US Government's perceived equities in the military, defense and intelligence areas
  - Primarily focused on domestic issues
  - Limited multilateral approach
  - Focused on large acquisitions and divestitures
  - Limited to no review of minority investments unless specific national security equities existed

Foreign Direct Investment (FDI) Timeline – US and Global

- 1949 – Foreign Exchange and Foreign Trade Act (Japan)
- 1961 – Foreign Trade and Payments Act (Germany)
- 1966 – French Foreign Investment Regime (France)
- 1975 – Executive Order (EO) 11858 establishing CFIUS as an ad hoc committee
- 1975 – Foreign Acquisitions and Takeovers Act (Australia)
- 1985 – The Investment Canada Act (Canada)
- 1988 – Exon-Florio Amendment (Exon-Florio) to the Defense Production Act
- 1993 – Byrd Amendment to Exon-Florio to expand CFIUS review of sovereign wealth fund investments

FDI Timeline – US and Global

- 1999 – Federal Law on Foreign Investments (Russia)
- 2005 – Overseas Investment Amendment Act (New Zealand)
- 2007 – Foreign Investment and National Security Act (FINSA)
- 2012 – Italian Foreign Investment Regime ("Golden Power" Regime) (Italy)
- 2015 – Foreign Acquisitions and Takeovers Fees Impositions Act (Australia update)
- 2018 – Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)
- 2020 – Foreign Direct Investment Regulation (European Union)
- 2020 – Foreign Investment Law of the People's Republic of China (China)
- 2022 – National Security and Investment Act (United Kingdom)
- 2022 – President Biden Executive Order 14083 directing CFIUS to review certain factors

Current Environment

- Changing interests from 1975 to the present
  - Importance of critical and emerging technologies
  - Supply chain vulnerabilities
  - New national security concerns – *i.e.*, healthcare, public welfare, telecommunications
  - New financial considerations – *i.e.*, types of investors and manner of investment
  - New geopolitical and geostrategic factors – *i.e.*, the role of China, elimination of redundancies, loss of manufacturing capabilities, renewed focus on the value of self-sufficiencies
  - Focus on multilateral FDI reviews
  - Focus has expanded to outbound investment reviews as well – with President Biden issuing Executive Order 14105 – which established a framework for outbound investments destined for countries of concern, currently China, Hong Kong and Macau
  - Outbound investments were originally considered in the FIRRMA rewrite but eventually were table in favor of allowing US export controls to manage any outbound transfers or investments

Trends

- CFIUS and FDI trends from 2018 through the present
  - The "truth" about Chinese investment in the US and abroad
  - Enhanced participation by new players – *e.g.*, the Office of Science and Technology Policy
  - Actions by the Chinese Government that affect FDI
  - US Congressional inquiries and their impact
  - More US Executive Action – *e.g.:*
    - New emerging technology designations by the Department of Commerce
    - Expanded use of sanctions lists to limit interaction with parties of concern
    - New executive orders on areas of interest – *i.e.*, biotechnology and biomanufacturing
    - New CFIUS enforcement guidelines – *i.e.*, guidelines on penalties and enforcement
    - Executive Order 14083

Elements of CFIUS

- Members
- Process
  - Regulations
  - Jurisdiction
    - Control versus minority investments
    - Factors that establish mandatory jurisdiction
  - Filings
  - Timeline
  - Substantive Review
  - Mitigation

Baseline CFIUS Requirements

- CFIUS Jurisdiction generally requires
  - A foreign investor
  - A "US business" – whether or not a "TID Business" (technology, infrastructure or data)
  - A national security equity as determined by the US Government agencies with an interest in the transaction

Permanent Members

- Department of the Treasury (chair)
- Department of Justice
- Department of Homeland Security
- Department of Commerce
- Department of Defense
- Department of State
- Department of Energy
- Office of the U.S. Trade Representative
- Office of Science & Technology Policy

Members Based on Specific Activities or Transactions

- Office of the Director of National Intelligence, nonvoting member
- Department of Agriculture
- Department of Labor
- Department of Interior
- Any other agency with equities in the transaction

Jurisdiction

- US Regulations – developed and managed by Treasury as the staff chair of CFIUS

  - 31 C.F.R. Part 801 Determination and Temporary Provisions Pertaining to a Pilot Program To Review Certain Transactions Involving Foreign Persons and Critical Technologies (October 2018)
  - 31 C.F.R. Part 802 Provisions Pertaining to Certain Transactions by Foreign Persons Involving Real Estate in the United States (January 2020)
  - 31 C.F.R. Parts 800 & 801 Provisions Pertaining to Certain Investments in the United States by Foreign Persons (January 2020)
  - 31 C.F.R. Parts 800 & 802 Definition of "Principal Place of Business"; Filing Fees for Notices of Certain Investments in the United States by Foreign Persons and Certain Transactions by Foreign Persons Involving Real Estate in the United States (Final Rule – July 2020)
  - 31 C.F.R. Part 800 Provisions Pertaining to Certain Investments in the United States by Foreign Persons (Final Rule – September 2020)
  - 31 C.F.R. Parts 800 & 802 Definitions of Excepted Foreign State and Excepted Real Estate Foreign State (Final Rule – January 2022)

Jurisdiction

- Guidance to CFIUS on factors relevant to national security reviews
- EO 14083 – "Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States" (September 15, 2022)
  - Directs the Committee to consider specific factors and memorializes key areas of concern
  - Key areas of CFIUS concern under the EO:
    - Supply chain
    - Aggregate investments or industry consolidations
    - Relationships with third parties (of concern)
    - Expanded industry sectors of interest
    - Focus on "foreign adversaries" and "countries of special concern"
    - "Future" US technological leadership and advancements
    - Aggregate investment posture from a technology or industry sector or corporate perspective

Jurisdiction

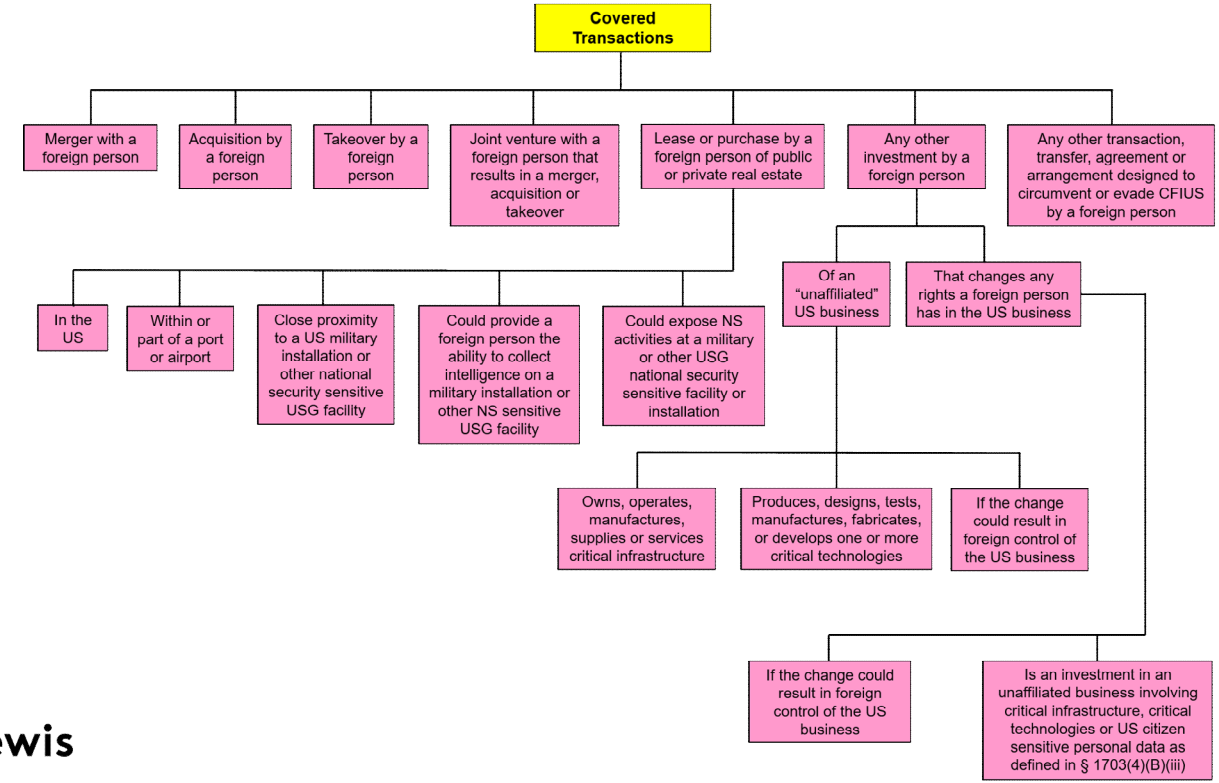
- Executive Order 14083
  - Expressly identifies sectors of interest (in addition to those mentioned in EO 14017 (America's Supply Chain) – *e.g.*:
    - Microelectronics
    - Artificial intelligence
    - Biotechnology
    - Biomanufacturing
    - Quantum computing
    - Advanced clean energy
    - Critical materials
    - Elements of the agricultural industrial base
    - Climate adaptation technologies

Timeline for Review

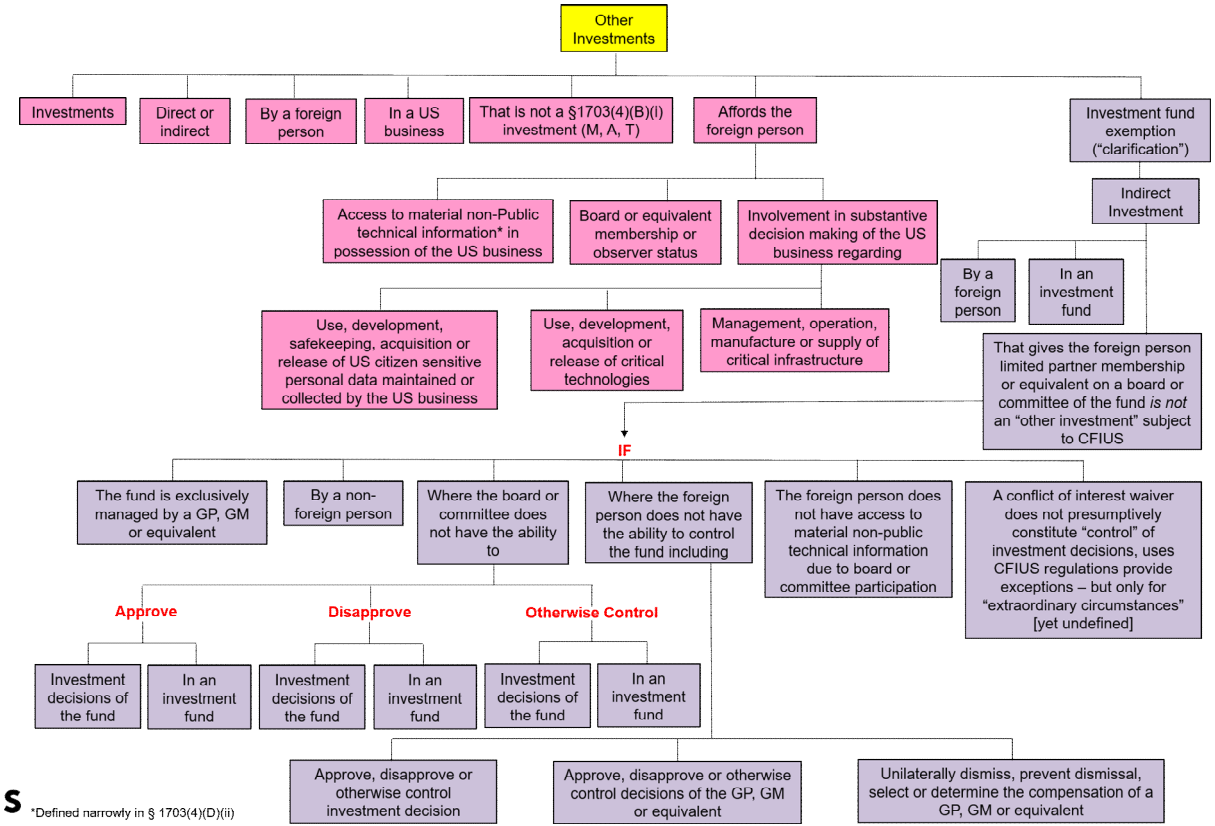
- Overall formal timeline – up to 120 calendar days – by statute – plus an additional 10 calendar day review for CFIUS evaluation of a "draft" filing
  - Submit draft filing – 10 calendar days
  - CFIUS advises whether the draft filing is complete
  - File the formal filing – approximately 2 to 7 calendar days to issue the "Day 1" letter that starts the formal time period for review
  - 45 calendar day review period (initial review)
  - 45 calendar day investigation review period (second review)
  - 15 calendar day extension for complex cases (discretionary)
  - 15 calendar day review by the President

Covered Transactions

FIRRMA § 1703(4)(A) AND (B)



Other Investments



*Defined narrowly in § 1703(4)(D)(ii)

US TID Business

- CFIUS may review cross-border investments in a US business – as defined in the regulations
- FIRRMA identifies a subset of "US business" where specific mandatory requirements apply – a "US TID Business" which involves
  - Technology
  - Critical infrastructure
  - Data
- Each element of a US TID Business is tied to specific requirements
- Relevant determination because CFIUS requires a filing if an investor is acquiring or otherwise funding or investing in a US TID Business

US TID Business

- Critical Technology
  - Covers existing and emerging technologies deemed "critical" to US interests
  - Broadly defined in some circumstances
  - Defined by US export control laws and regulations
    - Export Administration Regulations – where the controls are based on national security
    - International Traffic in Arms Regulations
    - Department of Energy/NNSA and Nuclear Regulatory Commission Regulations
    - Regulations governing biologics, toxins, and certain drugs
  - Leave the determination of what export classifications apply to the parties, unless a US Government agency decides to classify the technology in addition to the parties' representations regarding the controls that apply

US TID Business

- Critical Infrastructure
  - Defined in the regulations by location, activity and purpose – *e.g.*, a particular type of facility (for example, energy), conducting certain types of activities (for example, nuclear or standard electricity), providing output to particular consumers (for example, commercial customers or a military base or a hospital)
  - Regulations include datapoints for identification of the location, activity and purpose (Appendix A)
  - General raise national security concerns when it affects telecommunications, energy, transportation support, etc.

US TID Business

- Data includes personal information about US persons
  - Identifiable
  - Not in the aggregate or if aggregated, capable of being disaggregated
  - Related to US persons
- Includes but is not limited to any data points that may be used to identify a specific person – for example, name, date of birth, Social Security Number, driver's license numbers, passport numbers, military identifications, social media accounts, financial information (*e.g.*, banking, credit cards, loans), tracked preferences, location (*e.g.*, as tracked through geolocation services), health related data
- Also includes companies that collect a certain amount of this type of data for US individuals when that data exceeds either 1,000,000 individuals per year or, in select circumstances that impact genomic or biologic data, may be 100,000 or more
- Covers businesses that, for example, conduct clinical trials, biopharma development, nano-biotech research and development, hospital data manager, biotechnology development, data storage that houses this type of data

Factors that Affect the Review Period

- Inadequate filing
  - Incomplete information
  - Inaccurate information
  - Responses that do not answer the question asked
  - Incomplete attachments or supporting documentation
- Sensitive parties
- Sensitive countries or foreign governments – *e.g.*, countries of concern
- Extensive US Government engagement – *e.g.*, classified contracts, key supplier
- Export classifications – *e.g.*, accurate, consistent and current

Jurisdiction

- "Control" transactions versus minority investments
- Control is defined and interpreted broadly by CFIUS as the power, whether exercised or not, to determine, direct or decide important matters affecting an entity. Control can be present even in minority investments.
- Fact specific
  - "Control" investments remain covered the same as pre-FIRRMA
    - No set percentage of ownership required to meet "control" test – *e.g.*, no presumptive "10% rule" exists
    - Established by a combination of factors – *e*.g., percentage ownership, board or other operational rights, access to technology or other critical assets, "interrelated" or "coordinated" investors (*e.g.*, individuals from the same family each own 2%, so an aggregate evaluation is conducted)
    - A 'totality of circumstances' test – *e.g.*, situations exist where a 2% ownership with other factors qualifies as "control" and where a 45% ownership without other factors may not

Jurisdiction

- Control transactions may be subject to voluntary or mandatory filings
- Depends upon specific factors – *e.g.,*
  - Deal structure
  - Rights obtained by the foreign investor – both direct and indirect (whether exercised or not)
  - Timing of rights – *e.g.*, current, expected, tied to milestones
  - Home country or primary country of operations of the foreign investor
  - Whether the investor is a foreign government entity (direct or indirect)
  - Foreign investor's past investment history

Mandatory versus Voluntary Filings

- Factors that establish mandatory filing jurisdiction
  - Generally applies to minority investments and to investments in TID businesses (whether control or minority)
  - Are not tied to a specific percentage of investment – *e.g.*, not 5% or 10% or some other number
  - Would be subject to mandatory filing if the minority investor obtained any one of the following rights:
    - A board or observer seat (status defined by the responsibilities of the position, not the title) – for example, funds that make investments may have advisory committees that maintain the same type of rights and responsibilities as board members or board observers
    - Access to nonpublic technical information (generally defined by US export laws)
    - Any involvement in the day-to-day operations of the US business

Filings

- Mandatory
  - Completed electronically
  - No requirement for filing of personal identifier information (PII)
  - Are generally not filed for "pre-review" before filing
  - Involve minority investments or TID businesses
  - 30 calendar review period
  - May result in one of several outcomes:
    - Clearance
    - Clearance with mitigation measures
    - Rejection (for any specified reason)
    - No determination – either no request for a further filing or no determination
    - Finding of no covered transaction
    - Request to submit a full joint voluntary notice

Filings

- Voluntary filing
  - Same type of criteria matter to CFIUS for voluntary filings as for mandatory filings – *e.g.*, critical technologies, parties, countries of concern, engagement with the US Government, supply chain placement, cyber issues, specific industry sectors, relationships with China
  - Same time period for review except that CFIUS has the initial 10 calendar day pre-formal filing period to review a draft submission – 10 + 45 + 45 + 15 + 15
  - Requires the submission of PII, except if filed as a declaration
  - May be filed as a declaration or a full joint voluntary notice
  - Requires, in some cases, more extensive attachments and representations
  - Same potential outcomes, except the request for a more fulsome joint filing

Substantive Review

- Key factors CFIUS considers
  - Critical or emerging technologies
  - Supply chain
  - Defense industrial base resiliency
  - Indirect supply to the US Government or allied/partner governments
  - Expanded view of national security – now includes public welfare, healthcare, and corruption
  - Cybersecurity
  - "Building block" products or technology
  - Relationships with the People's Republic of China (China)
  - Government engagement
  - Multilateral jurisdiction

Mitigation

- Mitigation allows CFIUS to approve an investment because national security issues may be addressed through specific measures – *i.e.,* foreign ownership, control and influence (FOCI)
- Mitigation measures are generally reflected through the parties' execution of a national security agreement or mitigation agreement
- CFIUS retains discretion to develop and require mitigation measures as a condition of investment approval
- Is managed by Treasury and the "co-lead" agency with equities in the industry sector, technology or national security issues associated with the foreign investor
- Mitigation measures depend upon the type of assets involved – *e.g.*, real estate versus technology versus government contracts

Mitigation Measures

- Common mitigation measures include but are not limited to:
  - Restrictions on physical access to the acquired US business
  - Restricted access to US business technology
    - No access to US business IT systems
    - No participation on committees or as advisors on technology-focused aspects of the US business
    - No access to any export-controlled product, technology, software, materials or equipment absent appropriate authorization
  - Certain investor parties prohibited from any board or observer seats or from any operational issues – *i.e.,* only citizens from particular countries may hold these positions
  - Monitors overseeing foreign person activities
  - Notice requirements prior to any foreign person visit to the facility
  - US Government (co-lead agency or Treasury) participation in certain mitigated activities – *e.g.*, US Government agency may sit in on technology development meetings
  - Prohibitions on exiting certain US business areas absent notice and lead times to accommodate US interests

Due Diligence Focus

- Export Controls
- Supply Chain
- Investor's relationships (direct or indirect) with China
- Cybersecurity
- Access to Data
- Sanctions Compliance
- Foreign Investor Compliance with US Laws and Regulations
- Direct and indirect impact on the US industrial base – both defense and commercial
- Economic considerations related to supply resiliency

Export-Controlled Technologies and Related Items

- Technology applications
- Multilateral technology controls
- Made in China 2025 – the manner in which technology may be used
- Whether 'foreign adversaries' may use technology in a manner detrimental to US interests
- Updating US and multilateral technology lists
- Consideration of how 'critical technologies' are defined – *see, e.g.*, the establishment of the Office of Critical Technologies as part of the Office of the President and the 3rd iteration of the Critical and Emerging Technologies List
- The tie between intellectual property, export controls and 'controlled unclassified information"

Supply Chain

- Identifying the supply chain
  - For the US business
  - For the foreign purchaser/investor
- 1st, 2nd and 3rd tier supply chain identification is no longer adequate
- Understanding who within the supply chain is a **sole source** and from what country(ies)
- Understanding who within the supply chain is a **sole qualified source** and from what country(ies)
- Defense Priorities and Allocations System (DPAS) ratings and Title III designations of critical or strategic items (to include products or technology/software)
- Understanding the threat to the supply chain faced by the US business and the foreign purchaser/investor

Purchaser/Investor Relationship with China

- Increased focus by CFIUS
  - How long has the foreign purchaser/investor had relationships in China?
  - What kind of relationships – *e.g.*, joint ventures, research and development centers, marketing agreements, baseline supply chain agreements, etc.?
  - What Chinese law requirements applied to the relationships?
  - What parties were involved – *e.g.*, universities, research institutes, distributors, state-owned enterprises, state-directed enterprises, government laboratories, university professors or students, etc.?
  - What export licenses were obtained for the transfer of any technology from the United States to China?
  - Was any of the technology routed through third parties – *e.g.*, did the US company enter into an agreement with a third party who then forwarded the technology to China?
  - Were Chinese funds used to make the investment – *e.g.*, Chinese banks, Chinese venture capital funds, etc.?
  - Has China utilized its anti-foreign sanctions laws, state secrets, or intelligence laws in relation to the business conduct of the US company – i.e., has the company been designated by the Chinese government on any lists

Cybersecurity

- What cybersecurity programs does the foreign purchaser/investor have?
- What cybersecurity programs does the US business have?
- How many cyber 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?
  - Did the vulnerabilities and cyber breaches result in the loss of data considered critical to US National Security or other interests?

Access to Data

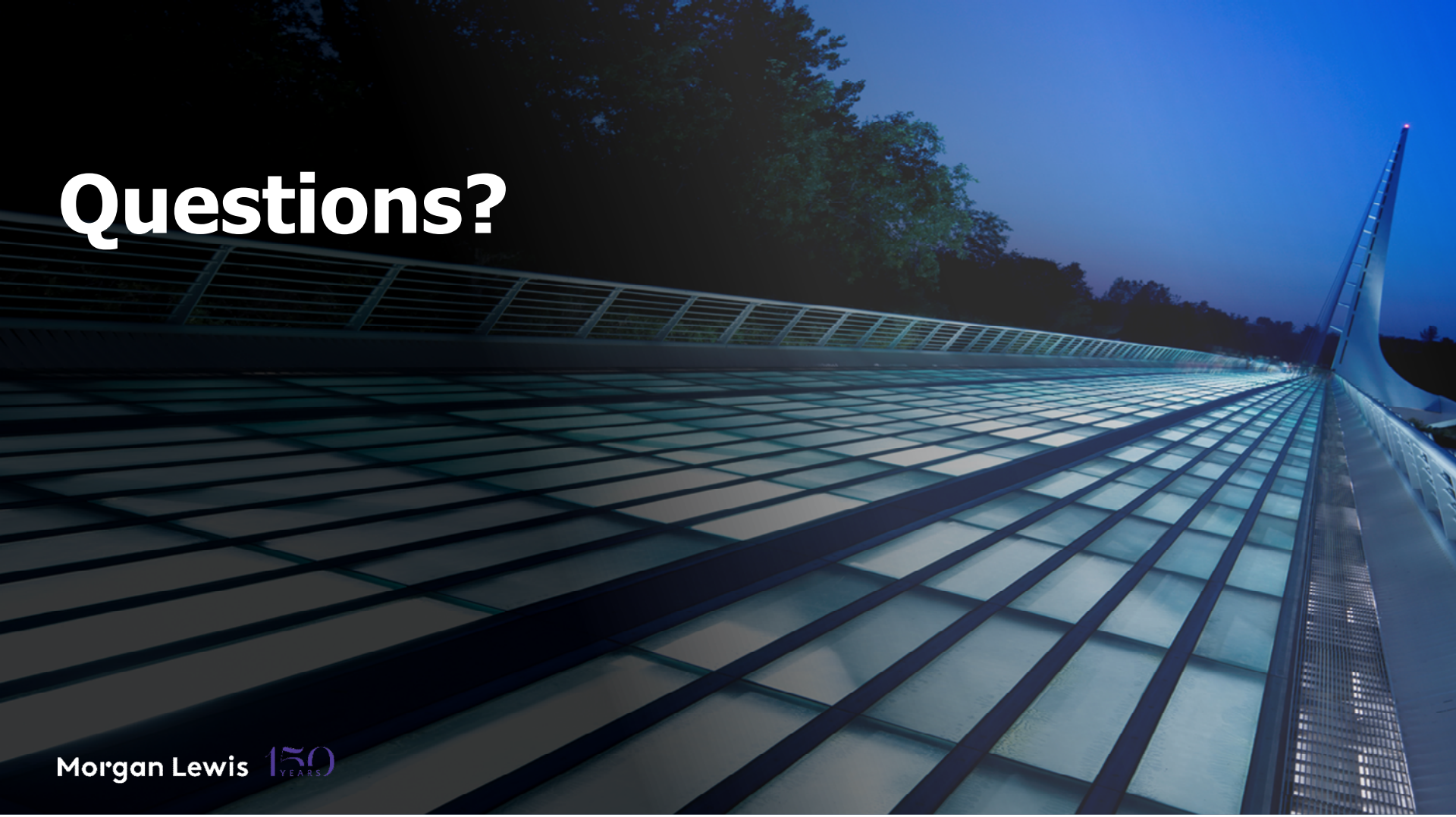
- Data – personal, technical or financial/business
  - What data does the US business possess?
    - How is it protected?
    - Who has access?
    - How can access be terminated?
    - How many breaches have occurred?
    - To whom were they reported?
    - How were they remediated?
  - What data access is the foreign purchaser/investor requesting?
    - How is data generally protected?
    - What additional considerations apply to the foreign purchaser/investor's cyber requirements – *i.e.*, privacy?

Sanctions Compliance

- Compliance with US sanctions or other US laws such as export controls
  - How does the foreign purchaser/investor comply with US sanctions?
  - Does the foreign purchaser/investor have a sanctions compliance program?
  - 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 CAATSA from a compliance perspective?
  - Does the foreign purchaser/investor home country abide by multilateral sanctions programs – *i.e.*, programs or policies agreed to at the United Nations?
  - 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?

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
- Parties who 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
- Challenges arise with OFAC and the International Traffic in Arms Regulations ("ITAR"), where the agencies have expressly extended jurisdiction to foreign parties for violating these regulations. Similar jurisdictional extensions have applied within the last 3 years as the Biden Administration has imposed additional export restrictions on China, specifically, in the semiconductor and semiconductor equipment industries


Questions?
Morgan Lewis
150 YEARS

Biography

Giovanna M. Cinelli
Washington, D.C.
+1.202.739.5619
giovanna.cinelli@morganlewis.com

Giovanna M. Cinelli is the leader of the Firm's international trade and national security practice. As a practitioner for more than 35 years, she counsels clients across industries, including the defense, finance, software, research and development, and high-technology sectors. Giovanna advises on a broad range of issues affecting national security and export controls, including CFIUS, cross-border due diligence, complex export compliance matters, and export enforcement, both classified and unclassified. She sits on 3 federal advisory committees at State, Commerce and Defense and has been considered a subject matter expert by Congress, think tanks and the US Government. She has testified in Congress and before the US-China Economic and Security Review Commission on export controls, CFIUS, diligence requirements, and enforcement matters.

Biography

Kenneth Nunnenkamp
Washington, D.C.
+1.202.739.5618
knunnenkamp@morganlewis.com

Ken Nunnenkamp represents clients in international trade and national security matters before United States federal courts and government agencies, including the US departments of State, Commerce, Homeland Security, Defense, and Treasury. His practice involves internal investigations and disclosures, including voluntary disclosures and responding to government demands, as well as federal court defense against government actions. He also advises on compliance counseling and training, transactional due diligence–including both domestic and cross-border transactions–and statutory submissions to US government agencies.

Biography

Carl A. Valenstein
Boston
+1.617.341.7501
carl.valenstein@morganlewis.com

Carl Valenstein focuses his practice on domestic and international corporate and securities matters, mergers and acquisitions, project development, and transactional finance. He counsels extensively in the life science, telecom/electronics, and maritime industries, and he has worked broadly in Latin America, the Caribbean, Europe, Africa, Asia and the Middle East.

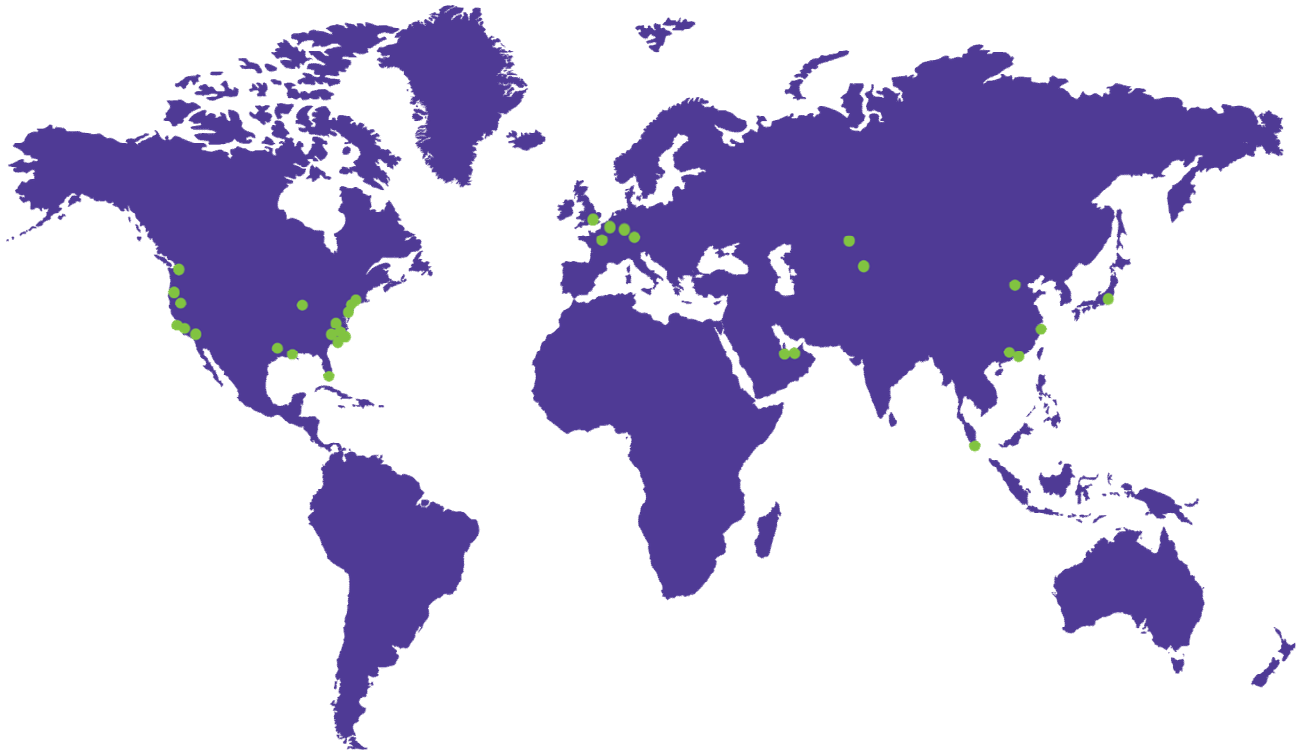
Carl advises clients on international risk management, including compliance with the foreign investment review process (Exon-Florio/CFIUS), export control and sanctions, anti-money laundering, anti-boycott, and anticorruption (FCPA) laws and regulations. He also advises on internal investigations, enforcement cases, and dispute resolution proceedings relating to his transactional and regulatory practice.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Astana
Beijing
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong
Houston
London
Los Angeles
Miami
Munich
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
Shanghai
Shenzhen
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis 150 YEARS

THANK YOU