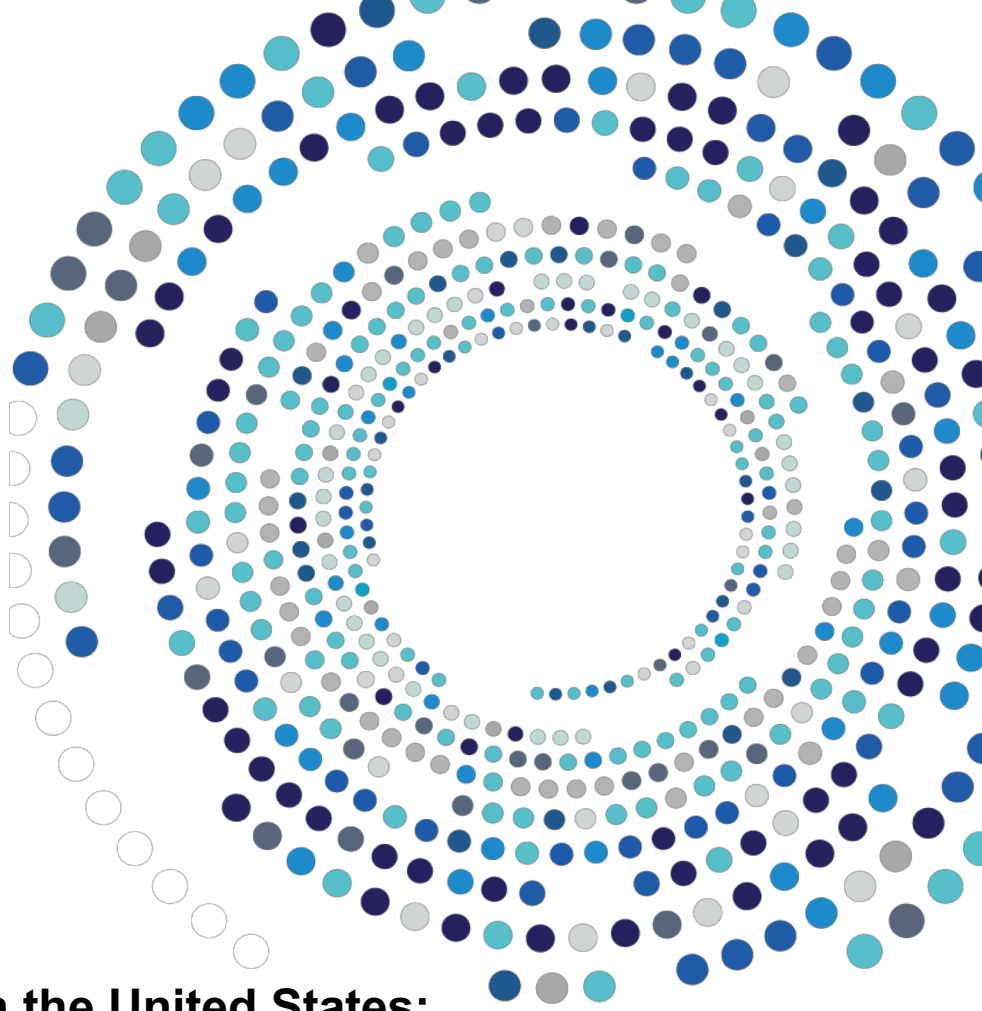

Committee on Foreign Investment in the United States: Background and Recent Developments

Greta Lichtenbaum

March 2019

Evolution of CFIUS

- Created by Executive Order in 1975, in response to wave of investments from the Middle East
- 1980s: Japanese acquisitions of U.S. advanced technology companies (*e.g.,* Fujitsu/Fairchild Semiconductor)
  - 1988: Congress enacts Section 721 of the Defense Production Act of 1950, broadly authorizing the President to block foreign investments on national security grounds
- 2007: Extensive revision of Section 721 after several controversial transactions, including CNOOC's bid for Unocal and Dubai Ports World transaction
- 2018: Responding especially to Chinese M&A activity in tech sector, Congress enacts CFIUS "reform" legislation (FIRRMA)

Committee on Foreign Investment in the United States

- Implements Section 721 by reviewing "covered transactions," assessing national security risks, and resolving identified concerns
- CFIUS may:
  - Clear or block transactions
  - Negotiate agreements to mitigate national security concerns
  - Permit parties to withdraw with no action
  - Refer the case to the President for decision (with its recommendation)
- Decisions are entirely discretionary. President's decisions are generally not subject to judicial review.

Which Transactions are Covered?

- Traditionally CFIUS only reviewed transactions in which a foreign person acquired "control" of an existing U.S. business
  - "Control" may result from minority investments, regardless of % stake
  - Only a few assets may constitute a "business"
- CFIUS jurisdiction now expanded to certain non-controlling investments in U.S. businesses involved in critical technology in certain industries
- JVs are covered where a party contributes a U.S. business
- Changes in ultimate foreign parent of a U.S. business are covered
- For global transactions, only U.S. businesses are covered
- Greenfield investments are not covered; loans generally are not covered
- Convertible instruments: depends on convertibility features
- Long-term leases: depends on facts

CFIUS Membership

- Chaired and administered by the Department of the Treasury
- Other members:
  - Departments of Commerce, Defense, Energy, Homeland Security, Justice, and State; Labor (*ex officio)*
  - Office of the U.S. Trade Representative
  - Office of Science and Technology Policy
  - Director of National Intelligence (also *ex officio*)
  - National Security Council, National Economic Council, Homeland Security Council, Office of Management and Budget, and the Council of Economic Advisors (*Observer status)*
  - Other agencies on an *ad hoc* basis (e.g., HHS for health care industry)

Three-Phase Process

- Statute provides for decision in four stages, within total of 120 calendar days:
  - **First:** Initial 45-day review. Most cases are completed at the end of this stage.
    - *Director of National Intelligence delivers threat assessment at Day 30*
  - **Second:** At end of the initial review stage, CFIUS may initiate a full investigation, lasting up to another 45 days.
    - *Presumption of investigation if case involves government-controlled acquirer or critical infrastructure*
  - **Third:** CFIUS may initiate a one time extension of an investigation for 15 days.
  - **Fourth**: If case remains unresolved, then CFIUS may refer the matter to the President, who has 15 days to act.
    - *CFIUS itself may take action at end of second stage, without referral to the President*

CFIUS Focus: Sensitive Sectors

- Historically, CFIUS was particularly concerned with acquisitions in the defense field
- Broad homeland security concerns are now equally paramount
  - Critical technologies
  - Telecommunications carriers and equipment manufacturers
  - Critical infrastructure, including transportation facilities and utilities
  - Protection of sensitive U.S. citizen data and personally identifiable information ("PII")
- Intense focus on supply chain, cybersecurity vulnerabilities, and "close proximity" to U.S. military facilities
- "Economic security" emerging as distinct concern
  - Preservation of the "National Security Innovation Base" (*e.g.*, semiconductors)
  - Emerging and foundational technologies (*e.g.*, AI, autonomous vehicles, virtual/augmented reality, robotics, IoT)
  - Any business accumulating personal identifying information

CFIUS Analytical Approach

- Threat posed by the investor
  - Nationality, government control, corporate compliance record, *etc*.
- Vulnerability of target
  - Critical infrastructure, defense supplier, sensitive technology, proximity to sensitive assets, *etc*.
  - DNI threat assessment addresses threat plus vulnerability
- National security consequences of foreign control
- If a national security risk exists, how can it be resolved?
  - Existing statutory authorities (*e.g*., export controls)
  - Mitigation agreements
  - Blocking transaction is least-favored option – but often threatened

Mitigation

- National security issues may be addressed through “mitigation agreements”
- Wide range of possible measures:
  - Divestiture of sensitive businesses
  - Structures to isolate foreign influence, creating passive investment position
  - Simple technology control plans and procedures
- Third-party audit requirements
- Appointment of “security directors”
- Mitigation agreements are principally a problem for the investor or acquirer, not the seller

Highlights of FIRRMA – amendments to statute

- New export control focus on “emerging” and “foundational” technologies
- Extends jurisdiction to include non-controlling “other investments” involving critical infrastructure, critical technology, or sensitive personal data of U.S. citizens, and transactions “designed or intended to evade CFIUS review”
- Creates short form “declarations” – mandatory for certain transactions, available to expedite review of straightforward transactions
  - Mandatory if foreign government has a “substantial interest” in foreign person acquiring a “substantial interest” in a U.S. business