RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **LAW-W04**

Treating CFIUS: Funding and Exiting When Feds Step In to "Enhance Security"

Joshua Gruenspecht
Partner
Wilson Sonsini Goodrich & Rosati

Ken Mendelson CISSP, CIPP-US
Senior Managing Director
Guidepost Solutions LLC

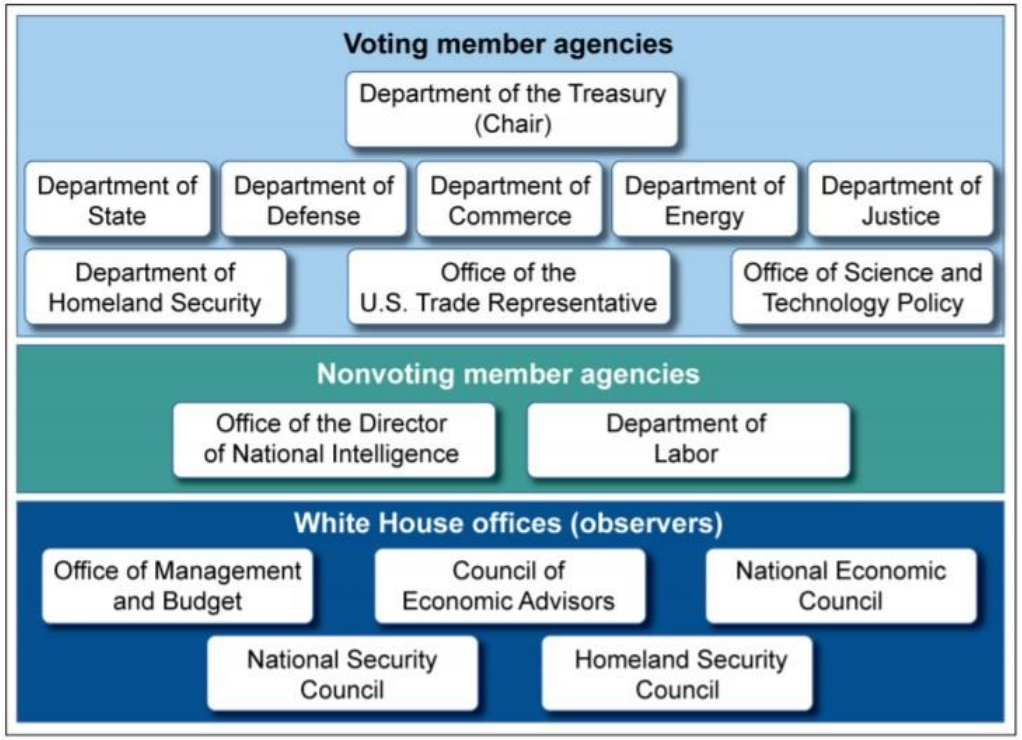
RSAConference2020

Introduction: Catching CFIUS

1. What It Is
2. What It Does
3. What It Could Mean For Cybersecurity Enterprises

CFIUS IS…

A Treasury Department-led interagency committee that evaluates the national security implications of transactions involving Foreign Direct Investment ("FDI") in U.S. companies.



Source: GAO analysis of agency documents. | GAO-18-249

What CFIUS Does (i.e., Potential Outcomes)

CFIUS Approves Investment or Acquisition

CFIUS Asks POTUS to Block/Unwind Investment or Acquisition

CFIUS Requires Parties to Mitigate National Security Concern(s) in Order to Approve Deal

Obligatory Horror Stories (CFIUS Has Real Impact)

What These CFIUS Changes Mean for Your Business

What we'll cover today:

- Background on CFIUS – both what it has been and how Congress has redirected it
- New rules and the impact they may have on cybersecurity-oriented companies – both in seeking investment and in exiting a business
- How CFIUS thinks about security problems and how they address them
- Summary and suggestions regarding how you should think about CFIUS problems – and the *opportunities* for companies that offer cyber security solutions – going forward

RSAConference2020

CFIUS Overview and Changes Under FIRRMA*

**Foreign Investment Risk Review Modernization Act of 2018*

CFIUS' Evolving IMPACT on Investing

Then: M&A Focus

- Emphasis on "FOCI" and potential foreign ownership "structure"
- Actions affected deal-close timing, could force post-close divestment
- Never limited to "defense" companies, but with limited resources, CFIUS had to pick its battles (even then, cybersecurity was an area of interest)
- Was a *voluntary* process (unless CFIUS singled out a deal)

Now: Concerned about foreign investments in U.S. technology companies and access to data

- Now includes many non-controlling investments (even though "control" is already broad at CFIUS)
- Mandate to specifically investigate foreign access to various technologies and large data sets across a wide range of industries and applications:
    - From cybersecurity to gene editing tools to autonomous vehicle tech to online advertising and beyond
- **For some transactions filing is now Mandatory**

More Background -- Pre-FIRRMA CFIUS Jurisdiction

A CFIUS "covered transaction" formerly was one that could result in:

- A "**foreign person**"
  - A non-U.S. national or non-U.S. entity, or an entity over which control can be exercised by a non-U.S. national or entity
- Acquiring "**control**"
  - Power to affect decision making with respect to important matters
  - 10%+ equity, or a board seat, or a veto right, or other rights that could affect decision making = possible control
- Over a "**U.S. business**"
  - Any entity engaged in commerce within the U.S.
  - A foreign person can also be a U.S. business

Filings had been voluntary unless specifically compelled by CFIUS

- Voluntarily filing with CFIUS = safe harbor against a post-closing compelled review

CFIUS is Changing: New Law + Newer Rules

FIRRMA broadened CFIUS's authorities; it has been partially effective for over a year but is now for the first time fully operational under rules that took effect on February 13, 2020

- Failure to file with CFIUS – especially a "mandatory" filing under the new FIRRMA rules – can result in forced divestiture, substantial civil penalties, and/or lawsuits between the parties

FIRRMA represents the most significant change in CFIUS in 20 years

- Broadens CFIUS' jurisdiction over various specific areas of CFIUS interest
- Creates mandatory filing obligations
- Grants CFIUS new resources, and emphasizes monitoring and enforcement
- Changes certain aspects of CFIUS procedure (e.g., creates an expedited process)

Going forward, CFIUS risk should be assessed for ANY foreign investment into a U.S. business

- Foreign investments can include investments made by a U.S. fund with foreign limited partners or a fund with foreign general partners
- Such investments may also include certain joint ventures in which a U.S. business participates

RSAConference2020

The New FIRRMA Rules and What They Mean When Seeking Foreign Investment (or an Exit)

CFIUS Jurisdiction Under the New Rules

CFIUS can still reach any investment that grants "control" to a "foreign person" over any "U.S. business"

In addition, it can now reach non-controlling investments into "TID businesses":

- Produce, build or test critical **technologies** (the "T")
- Own, operate, manufacture or service critical **infrastructure** (the "I")
- Maintain or collect, directly or indirectly, sensitive (or large amounts of) U.S. person **data** (the "D")

Now, in order to avoid CFIUS jurisdiction, a foreign investment into a TID business must avoid not just "control" but all of these "triggering rights":

- A board seat, observer seat or nomination rights
- Access to "material non-public technical information" (e.g., through a license to the technology)
- Involvement in substantive decision-making about the business's sensitive operations or technologies (e.g., through a commercial agreement)

Who is a "TID Business"?

All three parts of the "TID business" definition implicate cybersecurity service and product providers:

- **"Critical technology"** defined by reference to six U.S. government lists (primarily export controls)
  - *Many cybersecurity providers' products will be classified as 5D002 software – a "critical technology"*
- **"Critical infrastructure"** defined according to an eight-page appendix
  - E.g., satellite systems that provide services directly or indirectly to the Department of Defense, IP networks with access to others through settlement-free peering, major power/water utilities, etc.
  - *Analysis of a U.S. business's relationship to critical infrastructure will be highly fact-specific, but those who provide cybersecurity services to critical infrastructure may themselves be "critical infrastructure"*
- **"Sensitive personal data"** defined as falling into any one of many distinct categories
  - Individuals' genetic information is sensitive personal data when held by any U.S. business
  - Several other categories (financial data, geolocation data, health data, electronic communications, etc.) qualify if the underlying business either (i) holds or intends to hold many records or (ii) targets U.S. government customers
  - *Cybersecurity service providers with access to, e.g., electronic communications data may have sensitive data*

Required Filings for Critical Technologies

Five-part conjunctive test to determine whether there is a "critical technology" filing requirement; this is largely unchanged from the previous "pilot program" rules:

1. Is there a U.S. business?
2. Is there a foreign person (a foreign natural person, foreign entity, foreign government, or U.S. entity under control of any foreign person)?
3. Will the investor receive control or other triggering rights?
4. Does the target deal in "critical technologies"
   - Defined by reference to six U.S. government lists, particularly export control lists, such as the Commerce Control List
   - The list of critical technologies will expand with "emerging" and "foundational" technologies
   - Special rule for 5D002 technologies
5. Does the target use its technology in, or design it for use in, any of 27 designated industries?
   - CFIUS is likely to alter this fifth prong in the near future

Required Filings for Other TID Businesses

The government "substantial interest" test is the latest addition to the relatively narrow set of transactions for which filings are mandatory; a four-part conjunctive test would include:

1. Is there a U.S. business?
2. Is there a foreign person (a foreign natural person, foreign entity, foreign government, or U.S. entity under control of any foreign person) with a "substantial interest"?
   - i.e., one in which a foreign government has a 49% or greater interest (direct or indirect) in the foreign investor
3. Will the investor receive control or other triggering rights along with a "substantial interest"?
   - i.e., the foreign person will obtain a 25% or greater interest (direct or indirect) in the U.S. business
4. Is the target a "TID business"
   - As defined above

Broader CFIUS Reach on an Elective Basis

CFIUS can choose to review control transactions into any U.S. business and investments that grant "triggering rights" into TID businesses, and now has more resources with which to do so:

- CFIUS can block the transaction, impose conditions, or force divestment post-closing
- Transactions facing severe CFIUS headwinds can create legal disputes between the parties
- Only obtaining CFIUS clearance before closing insulates the transaction from post-closing adverse action

However, its reach extends to tens or hundreds of thousands of investments; CFIUS is interested in only some

Whether to make a filing or take the risk of post-closing adverse action depends on many factors, including:

- Identity and history of the foreign person
- Details regarding the U.S. business (e.g., potential relevance to U.S. security)
- Timing and cost considerations
- CFIUS enforcement practices
- Parties' risk tolerance and allocation of CFIUS risk in transaction documents

Even More FIRRMA

There are many additional aspects of FIRRMA that we won't cover here in depth but should acknowledge:

- Changes in CFIUS procedures
- Expanded coverage of real estate transactions
- "Excepted investor" status for certain UK, Canadian, and Australian investors
    - Difficult to qualify for various reasons
- Possible filing fee going forward
- International coordination on similar foreign investment regimes overseas
- And many, many more changes…

The likely overall result: more CFIUS cases

- Which in turn will likely mean more CFIUS security measures…

RSAConference2020

How CFIUS Thinks About Security

The Structure and Function of a National Security Agreement ("NSA"):

When CFIUS determines that a transaction requires intervention to protect sensitive assets, technology, or data from a foreign investor or parent, it has the option to establish a risk mitigation agreement

- Such agreements are private, secret agreements between the U.S. government and the companies that are party to the investment transaction

There are generally two forms of mitigation agreements:

- The national security agreement (NSA)
- The letter of agreement or letter of assurance (LOA)
- Both forms often are collectively referred to as "NSAs"
- These are secret (i.e., non-public) documents

Agreements look like standard commercial letters or agreements

Breach of these agreements carries severe penalties…

The Terms of an NSA

NSAs are intended to put in place mechanisms to ensure the security of sensitive aspects of the company in question; categories may include:

- Physical and logical controls re: access to data
- Governance controls (limited Board presence, limited visitation/communication with company, limited decision-making)
- Oversight mechanisms (i.e., third party monitors and/or audits)

Typical issues addressed in NSAs (though CFIUS has full discretion to require whatever it feels is necessary):

- Compliance with U.S. surveillance laws permitting access to certain forms of data
- ***Establishing/maintaining cybersecurity best practices***
- Limiting operations "offshoring"
- Restricting the types of vendors or products that may be used

Some sample NSA terms impacting cybersecurity appear after the end of this deck in the course materials

CFIUS Interest in Cybersecurity = Opportunity

NSAs can incorporate specific requirements to improve cybersecurity posture. Examples of NSA requirements include:

- Physical and logical access controls related to specified data types
- Developing a cybersecurity plan consistent with NIST CSF
- Hiring dedicated security staff
- Adopting comprehensive information security policies and procedures
- Requiring employee screening/visitor logging

Auditing, Monitoring and Oversight

- **Required third-party monitoring and/or auditing of compliance with NSA terms and additional USG requests.**

Summary: In most cases, CFIUS will require companies do those steps they should be taking anyway (i.e., because it's simply the right thing to do – from a business perspective)

RSAConference2020

Key Takeaways and Applications

The Key Question: CFIUS Enforcement

CFIUS is standing up a new enforcement division whose mission, in part, will be to find unfiled transactions

- Failure to make a mandatory filing may carry penalties up to the value of the transaction – on the investor, the company, or both
- For either mandatory or voluntary filings, if CFIUS intervenes post-closing, the negative consequences can include the expense of unwinding a transaction or accepting burdensome conditions and the valuation hit that may come from a rapid CFIUS-mandated divestiture

CFIUS has not yet made clear how it plans to effectuate its new, broadened jurisdiction on the voluntary side

- If CFIUS uses its new enforcement arm to take a more aggressive stance on bringing in unfiled transactions subject to its new jurisdiction, filings with CFIUS may need to expand significantly to accommodate those risks
- On the other hand, if CFIUS does not actively enforce its newly expanded jurisdiction, the ultimate impact of the expanded coverage of TID businesses (and real estate) in the new rules may be of limited practical import

Practical Summary of the Changes to CFIUS

1. The new CFIUS rules are now fully operational and will impact how cybersecurity product sellers and service providers seek investment and engage in other transactions
2. Mandatory filings and enforcement will be two key drivers of CFIUS risk
3. However, CFIUS also presents an opportunity to service providers

Apply What You've Learned

- Recognize the potential national security concerns with respect to foreign investment
- Reach out to counsel early when considering a JV, investment, or other deal involving a foreign counterparty
- Plan for mitigation: Can sensitive information be segregated and controlled to address national security concerns?
- Consider the potential utility of your own product or service in assisting the U.S. government in reviewing foreign investor activity in other companies

RSAConference2020

Thanks

Joshua Gruenspecht
Partner
Wilson Sonsini
jgruenspecht@wsgr.com
(202) 973-8817

Ken Mendelson, CISSP, CIPP
Senior Managing Director
Guidepost Solutions LLC
kmendelson@guidepostsolutions.com
(202) 499-4329

Supplemental Materials – Sample NSA Terms

Listed below are examples of various requirements CFIUS agencies have placed on transaction parties as conditions for obtaining CFIUS' approval of the transaction. The actual requirements imposed will vary based upon the nature of the transaction and the specific national security concerns implicated by the deal. This list is for illustration purposes only and is not exhaustive.

Sample NSA Terms: Cybersecurity Policies and Practices

Physical and logical access:

- Designating secure facilities for certain company operations
- Drafting and enforcing a CFIUS-approved information security plan to protect U.S. government designated classified and sensitive information
- Establishing CFIUS-approved employee screening measures
- Designating an employee to serve as the in-house lead for enforcement of the NSA terms
- Limiting permitted offshoring of corporate activities
- Limiting foreign person access to domestic equipment and operations

Supplemental Materials – Sample NSA Terms

Equipment and service provider limitations:

- Providing information to CFIUS on company networks and vendors
- Granting CFIUS the right to review and approve providers of key equipment and related services
- Requiring the removal or replacement of selected deployed equipment or vendors of services

Reporting:

- Provide advance notice and opportunity for review/approval of changes in key personnel or security incidents
- Provide an annual report to CFIUS discussing changes in services offered or locations from which they are offered, security practices, or updated policies and procedures

Auditing and oversight:

- Establishing an in-house compliance team, which may include, e.g.:
  - Point of contact for law enforcement
  - Point of contact on security issues
- Requiring a third-party audit and/or monitor for security and/or NSA compliance
- Permitting CFIUS visitation and inspection rights