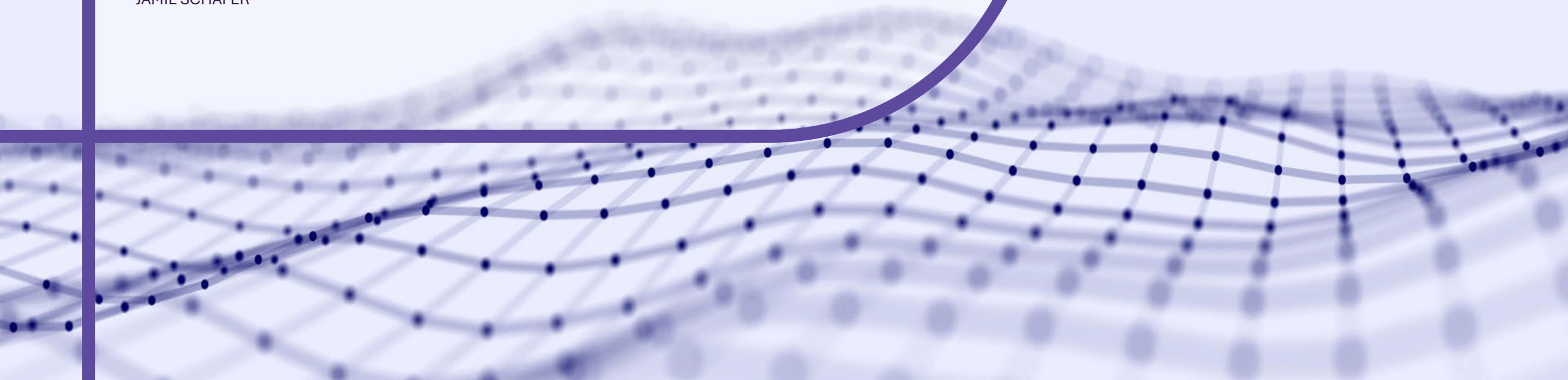
Perkins Coie

THE COMPLIANCE COLLECTIVE

Navigating U.S. Restrictions on Business Transactions with Russia, China and Other "Countries of Concern"

SEPTEMBER 19, 2025

PRESENTED BY: DAVID AARON, MIKE HOUSE, RICHARD OEHLER AND JAMIE SCHAFER



The Compliance Collective

This webinar is a part of our monthly webinar series, “The Compliance Collective.”

The webinar series is hosted by a team of cross-disciplinary Perkins Coie lawyers who provide a monthly overview and discussion forum on a critical hot topic in ethics and compliance. Each topic provides a look at emerging issues and offers creative solutions to potential compliance problems.

The webinar is hosted every third Thursday at the same time each month: 10:00 a.m. PT/12:00 p.m. CT/1:00 p.m. ET.

Sign up on our website to receive invitations to our future webinars!

Agenda

Overview: Regulatory, Enforcement and Political Trends
New Data Sharing Restrictions
Foreign Investments (CFIUS)
Anticipated U.S. Investment Restrictions
Key Compliance Takeaways

David Aaron
SENIOR COUNSEL | WASHINGTON, D.C.
Privacy & Data Security
DAaron@perkinscoie.com
+1.202.654.1723

Mike House
PARTNER | WASHINGTON, D.C.
International Transactions & Trade
MHouse@perkinscoie.com
+1.202.654.6288

Richard Oehler
PARTNER | SEATTLE
Government Contracts
ROehler@perkinscoie.com
+1.206.359.8419

Jamie Schafer
PARTNER | WASHINGTON, D.C.
White Collar & Investigations
JSchafer@perkinscoie.com
+1.202.661.5863

Overview

Overview: Regulatory, Enforcement and Political Trends

Observations

- We are at an inflection point in our application of U.S. regulatory and enforcement power to achieve foreign policy and national security ends
- Impacts reverberate around the world and place the U.S. under significant scrutiny
- Increasingly blurry lines between national security and economic policy

Political Trends

- Significant swings in foreign policy and national security priorities create deep market uncertainty (e.g., Russia, Iran, Cuba)
- However, many priorities will shift but not disappear (e.g., China)

Overview: Regulatory, Enforcement and Political Trends

Regulatory Landscape

- Drinking from a fire hose since 2022

- Abundance of new—and uniquely complex—AML, anti-corruption and economic sanctions rules aimed at stripping adversaries of wealth and shutting them out of U.S. markets or positions in which they could harm U.S. interests

- Focusing on strategic priorities, such as:
  - technologies like AI and quantum computing
  - social media platforms that collect enormous amounts of public data
  - access to U.S. infrastructure
  - Critical U.S. supply chains

- Other examples:
  - Corporate Transparency Act
  - CHIPS Act
  - Uyghur Forced Labor Prevention Act
  - Real Estate Rule

Overview: Regulatory, Enforcement and Political Trends

Enforcement Landscape

- Department of Justice: “Sanctions are the new FCPA”
  - DOJ will take on unprecedented regulatory role—including licensing and guidance—for certain new restrictions
- Reshuffling and addition of resources at DOJ National Security Division (NSD) and Money Laundering and Asset Recovery Section (MLARS)
- Vast increases in resources for other enforcement agencies (e.g., OFAC, FinCEN, BIS)
- Unprecedented interagency and intergovernmental coordination
- New indictments regarding sanctions, export control and other violations of law driven by U.S. foreign policy agenda announced every day

Overview: Regulatory, Enforcement and Political Trends

Perkins Coie

Risk Areas for Foreign Intervention Targeted by New and Emerging Laws and Regulations

- Access to U.S. markets (sanctions)
- Access to U.S. products/technology (export controls)
- Ownership of U.S. businesses by foreign persons (CFIUS)
- U.S. investment in foreign technologies/technology development (new investment restrictions, aka "reverse CFIUS")
- Access to U.S. data (U.S. data transfer restrictions)

New Data Transfer Restrictions

Data Transfer Restrictions

AUTHORITIES

- Executive Order 14117/IEEPA: Bulk Data Transactions & DOJ ANPRM
- Protecting Americans' Data from Foreign Adversaries Act (PADFA): Data Brokers

KEY CONCEPTS

- Data Brokers/"Data Brokerage"
- Other Data Transactions
- Countries of Concern
- Compliance vs. Enforcement
- Third-Party Service Providers

PADFA: Narrow Scope, Enforcement Emphasis

Perkins Coie

Applies only to "data brokers"

- entity that sells, transfers, discloses or otherwise makes available "data of United States individuals that the entity did not collect directly from such individuals to another entity that is not acting as a service provider"

Data broker may not:

- Sell, transfer, disclose, make available, etc.
- Personally identifiable
- Sensitive data
- of a U.S. Individual
- to any entity "controlled by a foreign adversary"

Enforcement:

- FTC: unfair/deceptive practice
- Maximum civil penalty per violation: $51,744

EO 14117 & ANPRM: Broad Sweep, Compliance Emphasis

Perkins Coie

Not currently in effect: EO issued, regulations pending

Covered transactions: any of the following with a "covered person" and involving "covered data"

- Data brokerage
  - sale of, licensing of, access to or similar commercial transactions involving the transfer of data from any person (the provider) to any other person (the recipient), where the *recipient* did not collect or process the data directly from the individuals
- Employment agreements
- Vendor agreements
- Investment agreements

Covered person:

- entity owned by, controlled by or subject to the jurisdiction or direction of CoC;
- foreign person who is an employee or contractor of such an entity or of CoC;
- foreign person who is primarily resident in CoC; or
- any person designated by AG

EO 14117 & ANPRM: Covered Data

"Bulk" sensitive data of U.S. Persons (or certain USG data, whether or not bulk)

Sensitive data:

- Personal identifiers
  - Gov't ID, account #s, device identifiers, network-based identifiers, ad IDs, etc.
- Personal financial data
- Personal health data
- Precise geolocation data
- Biometric identifiers
- Human genomic data

Bulk: Depends on type of data

- 100 to 1,000 (genomic data)
- 100 to 10,000 (biometrics, geolocation)
- 1,000 to 1,000,000 (health, financial)
- 10,000 to 1,000,000 (personal identifiers)

Applies equally to encrypted and/or anonymized data

EO 14117 & ANPRM Cont'd

Perkins Coie

Prohibited with CoC/Covered Person

- Data brokerage transactions involving bulk sensitive U.S. person data
- Bulk human genomic data

Restricted with CoC/Covered Person

- Vendor, employment & investment agreements that
- Transfer/provide access by CoC/Covered Person to bulk sensitive U.S. person data

Exceptions

- Intra-entity transactions incident to business operations
- Transactions required by U.S. law

Security Controls

CFIUS

What Is CFIUS?

- Committee on Foreign Investment in the United States (CFIUS)
- Interagency committee chaired by the U.S. Department of Treasury
- CFIUS is authorized to review certain transactions involving foreign investment in the U.S. in order to determine the effect of such transactions on the national security of the U.S.

What Are CFIUS-Covered Transactions?

- Any acquisition of a U.S. business by a foreign person
- Any controlling investment in a U.S. business by a foreign person
- Certain non-controlling minority investments in a U.S. business if the foreign investor has any of the following rights:
    - Access to material, nonpublic technical info of the U.S. business
    - Membership or observer rights on the board of directors (or equivalent) of the U.S. business or the right to nominate an individual to such a position

TID U.S. Business

- And the U.S. business is a TID U.S. business

- "T" stands for Critical Technologies, which generally includes products or technology subject to U.S. export controls

- "I" stands for Critical Infrastructure, which includes a U.S. business that performs certain functions regarding certain critical infrastructure systems and assets

- "D" stands for Sensitive Personal Data
  - Sensitive Personal Data includes certain categories of identifiable data where the U.S. business has data on more than one million individuals or intends to maintain or collect such data on greater than one million individuals as part of its products or services

TID U.S. Business (Cont'd)

- Here are the Sensitive Personal Data that are the most likely to arise:

    - Financial data that could be used to analyze an individual's financial distress or hardship
    - Data relating to the physical, mental, or psychological health condition of an individual
    - Nonpublic electronic communications, including email, messaging, or chat communications, between or among users of a U.S. business's products or services if a primary purpose of such product or service is to facilitate third-party user communications
    - Geolocation data collected using positioning systems, cell phone towers, or Wi-Fi access points, such as via a mobile application, vehicle GPS, other onboard mapping tool or wearable electronic device

CFIUS and China

- CFIUS has been vigorously reviewing Chinese investments for the past 10 years
- Critical Technology – CFIUS will examine carefully investments in U.S. businesses that are involved in Critical Technology
- CFIUS may require that the parties enter into a National Security Agreement (NSA) pursuant to which the parties agree that the Chinese investor will have no access to Critical Technology or limited access to such technology
- CFIUS will monitor compliance with the terms of the NSA

CFIUS and China

- Sensitive Personal Data has become extremely important to CFIUS
- CFIUS will ask many questions regarding the handling of such data by the U.S. business, particularly when the foreign investor is from China
- CFIUS frequently will ask the parties to enter into an NSA where the parties will agree that the Chinese investor will have little or no access to such data
- CFIUS will monitor compliance with the terms of the NSA and can bring an enforcement action if the parties are not complying with the NSA

Non-Notified Transactions

- If the parties to a CFIUS-covered transaction do not file with CFIUS, CFIUS has a continuing right to review the transaction post-closing and take appropriate action
- These transactions are known as non-notified transactions
- CFIUS has a significant staff that looks for non-notified transactions, and many of those transactions involve Chinese investment
- CFIUS can ask the parties to provide information and may request that they file a Notice with CFIUS

Anticipated U.S. Investment Restrictions

Proposed Treasury Regulation on Certain Outbound Foreign Investments by U.S. Persons

- June 2024: Treasury Department issues Proposed Rule establishing **new outbound investment control regime covering sensitive and national security technologies**
- Implementation of President's **Executive Order 14105** (Aug. 2023): "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern"
- Proposed Rule would, for first time, **impose significant prohibitions or notification requirements on certain outbound U.S. investments to China** (including Hong Kong and Macau) in technology sectors relevant to military, intelligence, surveillance or cyber capabilities
- Proposed Rule **places burden directly on U.S. persons** to determine the new rule's applicability to contemplated transactions—including a "knowledge" standard requiring due diligence in connection with compliance
- Treasury received public comments on Proposed Rule through August 4, 2024, and is now working on Final Rule

“U.S. Person” and “Covered Foreign Person”

- **“U.S. Person”**
  - Any U.S. citizen, lawful permanent resident or entity organized under U.S. law
  - Any person in the U.S.
  - Also applies to certain transactions undertaken by **non-U.S. persons controlled by a U.S. person**
  - U.S. persons may not **“knowingly”** direct a transaction prohibited if undertaken by a U.S. person

- **“Covered Foreign Person”**
  - Person of a **“country of concern”** (currently only **China**, including Hong Kong and Macau) that engages in **“covered activities”**
  - Person that holds an interest in **and** receives more than 50% of its revenue, net income, capital expenditure or operating expenses from the **above-defined person** (even if it is not itself a person of a country of concern or engaged in covered activities)
  - Person of a country of concern (China) that **participates in a joint venture with a U.S. person** if such joint venture is engaged in “covered activities”

- **“Person”** of country of concern includes: (1) individual citizen or permanent resident; (2) entity organized under the laws of, or headquartered in, incorporated in or with a principal place of business in, a country of concern; (3) the government of a country of concern; and (4) any entity that is majority-owned or majority-controlled (directly or indirectly) by any of the foregoing

“Covered Transaction”

- Limited to those transactions subject to **prohibition or notification requirements** under the Proposed Rule—i.e., transactions involving “**covered activities**”

- Types of “covered transactions” by U.S. persons can include:
  - Acquisition of an equity interest or contingent equity interest in covered foreign person
  - Provision of certain debt financing
  - Conversion of a contingent equity interest or convertible debt
  - Greenfield investment or other corporate expansions involving covered foreign person
  - Entrance into a joint venture (regardless of location) that will undertake a covered activity
  - Limited partner investment into a non-U.S. person fund investing in a covered foreign person

- Certain types of transactions are **exempted**, including investments in publicly traded securities or mutual funds, certain limited partner investments in funds, outright acquisitions of covered foreign persons and certain intercompany transactions

“Covered Activities”

(1) Semiconductors and Microelectronics

Prohibited: Electronic design automation software for the design of integrated circuits or advanced packaging; certain fabrication and advanced packaging equipment; certain advanced ICs subject to U.S. export controls; certain logic, NAND, DRAM, gallium, graphene or carbon nanotube ICs; advanced packaging techniques; and development, installation, sale or production of certain supercomputers.
Mandatory Notification: Any covered transactions related to the design, fabrication or packaging of any integrated circuits not otherwise covered by the prohibited transaction definition.

(2) Quantum Information Technologies

Prohibited: Development of quantum computers or production of critical components for quantum computers; development or production of certain quantum sensing platforms; and development or production of certain quantum network and quantum communication systems.
Mandatory Notification: None (all defined transactions are prohibited).

(3) Certain Artificial Intelligence Systems

Prohibited: Any AI system designed or intended for military, government intelligence or mass surveillance end uses; any AI system trained using a specified quantity of computing power or computing power using primarily biological sequence data.
Mandatory Notification: Any AI system, not otherwise prohibited, designed for government intelligence, mass surveillance or military end use; or for cyber security applications, digital forensics tools, penetration-testing tools or robotic systems; or trained over a certain threshold of computing power.

Additional Restrictions and Considerations

- Covered transactions are **prohibited** (even if otherwise only subject to mandatory notification) where the covered foreign person is listed on BIS's Entity or Military End-Users Lists, OFAC's SDN List or certain other Treasury, State and Commerce prohibited entity and end-user lists.

- **Knowledge Standard – Onus Is on the U.S. Person:**
  - U.S. persons are obligated to determine whether the given transaction is prohibited, permissible but subject to notification, or not covered by the rule.
  - Proposed Rule defines "knowledge" or "know" to include **facts or circumstances a person was aware had a high probability of occurring or had reason to know.**
  - U.S. person that has **failed to conduct a "reasonable and diligent inquiry"** prior to entering the transaction may be assessed to have had "reason to know."
  - Proposed Rule requires U.S. persons to take "all reasonable steps" to prohibit and prevent its controlled foreign entities from engaging in a transaction that would be prohibited if engaged in by a U.S. person.

- Unlike other U.S. export controls and sanctions regimes, under Proposed Rule, there is **no license process** and **no advance case-by-case review** to obtain prior authorization for transaction.

- Given the broad knowledge standard and no pre-clearance process, **vigilant due diligence by U.S. persons and their foreign subsidiaries is critical.**

Anticipated U.S. Outbound Investment Restrictions: Takeaways

- Outright prohibition or mandatory notification requirement for certain outbound "covered transactions" involving "covered foreign persons"—definitional scope of these terms is critical for U.S. business

- Distinction between "prohibited" and "notifiable" transactions based on defined national security technologies and products: semiconductors and microelectronics; quantum information technologies; artificial intelligence (AI) systems

- Violations subject to civil and criminal penalties under the International Emergency Economic Powers Act (IEEPA) and potential divestment of any prohibited transaction

Key Compliance Takeaways

Key Compliance Takeaways

- Risk assessment as to exposure to “countries of concern” as well as countries subject to applicable sanctions
- Stay abreast of shifting landscape: engage with knowledgeable in-house resources or outside counsel to receive updates and assist in navigating rules as they evolve
- Build “countries of concern” into risk-based controls requirements for new third-party relationships and transactions
- Consider other risk factors as well:
  - Critical nature of any enterprise targeted for foreign ownership
  - Involvement of U.S. person data
  - Implications for development of critical technologies
  - Implications for U.S. access to critical supply chains/resources
- Make contingency plans—e.g., robust termination clauses; exit strategies; UBO monitoring; restrictions on foreign access/control
- Adopt written compliance policies
- Train relevant personnel

