**National Security, International Trade & Foreign Investment:**

**An Introduction & Discussion of the Future**

***Robert B. Ahdieh***

***K.H. Gyr Professor of Private International Law***

***Emory University School of Law***

**Description:** This program will offer an overview of key areas of overlap between national security and international trade/foreign investment. To begin, we will consider the distinct but related regimes around export controls and foreign sanctions. Foreign investment regulation, including the Exon-Florio Amendment and the Foreign Investment and National Security Act of 2007, will be explored. Both U.S. and U.K. anti-bribery rules, as well as anti-money laundering laws, will be reviewed. Finally, the growing body of cybersecurity regulations will be described. The program will also touch on open questions about the direction of both the law on the books and enforcement practices in these areas, under the Trump Administration.

**Bio:** Robert B. Ahdieh is the K.H. Gyr Professor of Private International Law at Emory University School of Law. A graduate of Princeton University’s Woodrow Wilson School of Public and International Affairs and Yale Law School, Ahdieh served as a law clerk on the U.S. Court of Appeals for the Ninth Circuit before his appointment as a trial attorney in the Civil Division of the U.S. Department of Justice. He has served as a member of the Emory Law School faculty since 2000, and as a visiting professor at universities including Columbia, Georgetown, Illinois, and Princeton. He has also taught overseas, in Canada, China, Germany, Hong Kong, Israel, Norway, Poland, and Singapore. While still in law school, he published what remains the seminal account of Russia’s post-Soviet legal transition. More generally, his scholarship has focused on international trade and finance, and financial regulation broadly.

**OUTLINE**

1. **EXPORT CONTROL REGIME**
2. **Key Legislation/Regulations**
3. Arms Export Control Act (AECA) § 38, 22 U.S.C. § 2778 (2012).
4. Export Administration Act of 1979, 50 U.S.C. app. §§ 2401-2420 (2012).
5. Export Administration Regulations, 15 C.F.R. §§ 730-774 (2003).
6. International Emergency Economic Power Act (IEEPA) §§ 1701-1706, 50 U.S.C. § 99 (2012).
7. **International Traffic in Arms Regulations (ITAR)**
8. Administered by Bureau of Political Military Affairs’ Directorate of Defense Trade Controls (DDTC)
9. Addresses import/export of articles, technology, and services (assistance or training to foreign persons abroad or in U.S.) related to defense
10. Export Defined:
    1. Sending or taking a defense article out of the United States in any manner
    2. Transferring registration, control, or ownership
    3. Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad, or
    4. Performing a defense exportation of a defense article.
11. Includes “technical data”: classified information relating to defense articles, certain software, and information “required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles.”
12. Includes “Re-exports”: Actual shipment or transmission of subject items from one foreign country to another foreign country; or release of subject technology or software to a foreign national outside the U.S.
13. Export license exemptions:
    1. “Official use” and “foreign assistance”: No license required for temporary export of defense articles, technical data, or defense service for official use by U.S. department or agency or for carrying out authorized foreign assistance or sales programs.
    2. Public domain: Technical data that is published and generally publicly available.
    3. Fundamental research: Distinguished from research results restricted for proprietary reason or subject to U.S. government access and dissemination controls.

1. **Export Administration Regulations (EAR)**
2. Concerns “dual-use” items; primarily commercial goods and technology which may have a dual militaristic use.
   1. Encryption software – “May be used to harm U.S. national security;” challenged on First Amendment grounds; Sixth Circuit ruled protected; nonetheless, EAR upheld.
3. Export defined:
   1. Actual shipment or transmission of items out of the United States
   2. Release of technology or software subject to the EAR to a foreign national in the U.S.
      1. Visual inspections of U.S. origin equipment/facilities by foreign nationals
      2. Oral exchanges of information in the U.S. or abroad, or
      3. The application of personal knowledge or technical experience acquired in the U.S. to situations abroad.
4. Includes Re-exports: Similar to ITAR
5. Exceptions: Similar to ITAR
6. **Multilateral Non-Proliferation Regimes**
7. Wassenaar Arrangement (WA)
   1. Restrictions on weaponry and technology with potential for military applications.
   2. 40 member states, *see* Debra Burke, *At the Intersection of Export Control Regulations and Employment Discrimination Law*, 45 Am. Bus. L.J. 565, 568 n.5 (list of member states).
   3. Adopted in 1996 to replace Cold War era regime: Coordinating Committee on Export Controls (Co-Com) (disbanded after collapse of Soviet Union).
   4. Goals:
      1. Regional and international security and stability
      2. Complement and reinforce existing control regimes for WMDs
      3. Combat terrorism through export controls
      4. Promote transparency and greater responsibility in transfer of arms and technology (military and civilian)
8. Export Control and Related Border Security Assistance program
   1. U.S. initiative
   2. Managed by DOS Bureau of International Security and Nonproliferation.
   3. Goal: Improve other countries’ export control systems to meet international standards preventing proliferation of WMD, conventional weapons, and related items.
9. Zangger Committee
   1. 35-nation Nuclear Non-Proliferation Treaty (NPT)
   2. Goal: Harmonize implementation of the NPT requirements to apply International Atomic Energy Agency (IAEA) safeguards to nuclear exports.
   3. Maintains “Trigger List” – a list of equipment and materials exportable only if safeguards are applied to *recipient* facility.
10. Missile Technology Control Regime (MTCR)
    1. 34 countries
    2. Goal: Apply common export policy (MTCR Guidelines) to all key equipment and technology required for missile development, production, and operation.
    3. Particular focus on missiles capable of a minimum 500 kg payload with a minimum 300 km range; “Category I” or “MTCR-class” missiles.
11. Australia Group (AG)
    1. 38 countries
    2. Goal: Prevent member countries from assisting (purposefully or inadvertently) states or terrorists to acquire chemical or biological weapons.
12. **SANCTIONS REGIME**
13. **Key Legislation**
14. Trading with the Enemy Act (TWEA), 50 U.S.C. app §§ 1-44 (2012).
    1. Enacted during World War I to freeze property owned by enemy countries.
    2. Used extensively in World War II and Korean War; basis for North Korean sanctions, and Cuban sanctions after Cuban Missile Crisis.
    3. May be invoked only in wartime; seldom used today
    4. Present sanctions: North Korea and Cuba
15. International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1701 *et seq.* (2012).
    1. Enacted in October 2007
    2. President uses economic powers to regulate and prohibit transactions to address “any unusual and extraordinary threat” from any person or property subject to U.S. jurisdiction.
    3. Office of Foreign Assets Control (OFAC) promulgates implementing regulations.
    4. Present sanctions: Iran, Sudan, Zimbabwe, Burma, Somalia, Syria, the Balkans, and certain individuals within Russia

1. **Office of Foreign Assets Control (OFAC)**
2. Formally created in 1950 during the Korean War; President Truman declared a national emergency and blocked all Chinese and North Korean assets subject to U.S. jurisdiction.
3. Currently administers 29 different sanctions programs.
4. Maintains Specially Designated Nationals (SDN) and Specially Designated Narcotics Traffickers (SDNT) lists.
   * 1. Refers to natural and juridical persons associated with governments targeted for sanctions or with international narcotics trafficking or terrorism.
     2. Assets and accounts of those on the list must be frozen or blocked if in the U.S. *or* held by or in possession, custody, or control of a U.S. person.
     3. U.S. persons are prohibited from dealing with persons on the lists.
     4. No transaction is too small to be blocked or rejected.
     5. Exception: OFAC may issue either a general or specific license.
     6. U.S. commercial banks, their foreign subsidiaries, and foreign banks with U.S. operations must comply with OFAC regulations.
     7. Targeted countries: The Balkans, Belarus, Central African Republic, Cote d’Ivoire, Cuba, Iraq, Democratic Republic of Congo, North Korea, Iran, Liberia, Libya, Sudan, South Sudan, Syria, and Zimbabwe.
     8. Other targets/Related regimes: Terrorism, narcotics traffickers, WMD non-proliferation, transnational criminal organizations, rough diamond control regulations, Ukraine-related sanctions regulations, Yemen-related sanctions, and Magnitsky-related sanctions.
5. **FOREIGN INVESTMENT REGIME**
6. **Key Legislation**
7. Exon-Florio Amendment, 50 U.S.C. app § 2170 (2012).
   1. President authorized to review, modify, or potentially block certain acquisitions, mergers, takeovers, or investments that would give a foreign interest control of a U.S. business, in order to prevent a national security threat.
   2. Amended the Defense Production Act of 1950, 50 U.S.C. App. § 2061 *et seq.* (2012).
8. Foreign Investment and National Security Act of 2007 (FINSA) § 721, 50 U.S.C. App. § 2170 (2012).
   1. Increased CFIUS transaction approval factors from five (Exon-Florio) to twelve.
   2. Expanded definition of national security; does not include national economic security.
9. **Committee on Foreign Investment in the United States (CFIUS)**
10. Established by President Ford in 1975 following the 1972-75 energy crisis, out of fear OPEC countries would take over important sectors of the U.S. economy.
11. Interagency: Departments of Treasury (Chair), Defense, Homeland Security, State, Justice, Commerce, and Energy, and Offices of the U.S. Trade Representative and of Science and Technology.
12. Not authorized to block or divest transactions until Exon-Florio in 1988.
13. Conducts national security review of in-bound foreign investments (mergers, acquisitions, or takeovers) that could result in a foreign control of a U.S. entity.
14. Broad power/scope of review: Charged to defend “national security,” including but not limited to:
    1. Domestic production needed for projected national defense requirements,
    2. The capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, product technology, materials, and other supplies and services, and
    3. The control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the Unites States to meet the requirements of national security.
15. Secrecy: Each review is confidential unless reviewed parties choose to disclose; exempt from judicial review.
16. Negotiation: CFIUS is authorized to negotiate mitigation agreements with the parties to minimize security concerns.
17. **ANTI-BRIBERY REGIME**
    1. **Foreign Corrupt Practices Act of 1977, 15 U.S.C.A §§ 78dd-1 *et seq.* (2012)**
18. Enacted after discovery of corporate misconduct (over $300M in illegal or questionable payments to foreign officials by over 400 corporations).
19. Dual purpose:
    1. Prohibit the bribery of foreign officials
    2. Establish accounting requirements
20. Bribery provisions (15 U.S.C.A. §§ 78dd-1, 78dd-2, 78dd-3, 78ff(c)) apply to issuers, domestic concerns, and foreign nationals or businesses who take any action in furtherance of a corrupt payment while within U.S. territory.
21. Accounting provisions (15 U.S.C.A. § 78m(b)(2) to (7)): Publicly traded companies must keep accurate books and records and sound systems of internal controls.
    1. Primarily enforced by the SEC
    2. DOJ can bring criminal charges of knowing circumvention of internal controls and knowing falsification of books, records, or accounts.
22. 1998 Amendment
    1. Expanded prosecutions to include foreign persons while in U.S. territory
    2. Territorial basis for jurisdiction should be “broadly interpreted”
    3. **United Kingdom Bribery Act 2010**
23. Enacted after discovery of corporate misconduct (BAE Systems spent hundreds of millions in questionable payments to secure foreign defense contracts).
24. Offenses
    1. Active bribery – Offering, promising, or giving of a bribe to any third party
    2. Passive bribery – Requesting, agreeing to receive, or accepting of a bribe
    3. Bribing a foreign official to obtain a real business advantage
    4. Failure of an organization to prevent bribery
25. Enforced by the Serious Fraud Office (SFO)
    1. Broad jurisdiction
    2. Self-reporting and whistleblowing encouraged
26. Differences from FCPA
    1. Includes commercial bribery
    2. Prosecutes the bribe receivers
    3. Criminalizes a company’s failure to prevent bribery
    4. Applies to conduct anywhere in the world; no connection to UK required
27. **ANTI-MONEY LAUNDERING REGIME**
    1. **Key Legislation**
28. Bank Secrecy Act of 1970 (BSA), 31 U.S.C. § 5311 *et seq.* (2012).
    1. Precursor to broader AML efforts
    2. Intended to deter money laundering and use of secret foreign bank accounts
29. Money Laundering Control Act of 1986, 18 U.S.C. §§ 1956-57 (2012).
    1. Part of Anti-Drug Abuse Act of 1986
    2. Created three new criminal offenses for money laundering activities
30. Anti-Drug Abuse Act of 1988, Pub. L. No. 100-690, 102 Stat. 4181. (1988).
    1. Increased civil and criminal sanctions for laundering crimes and BSA violations
    2. Required more precise identification and recording of cash purchases
    3. Required Department of Treasury to negotiate large U.S. currency transaction agreements
    4. Increased criminal sanctions for tax evasion involving criminal activity-related funds
31. Housing and Community Development Act of 1992, Pub. L. No. 102-550, 106 Stat. 3672. (1992).
    1. Allows regulator to close/seize financial institutions for AML violations
    2. Forbids individuals convicted of money laundering from unauthorized participation in federally insured institutions
    3. Established BSA Advisory Group (interdepartmental)
    4. Gave Treasury authority to require financial institutions adopt AML programs
32. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272. (2001).
    1. Amended BSA to require financial institutions to practice enhanced due diligence on high-risk products
    2. Increased due diligence for transactions with non-cooperative countries

* 1. **Money Laundering Crimes**

1. Basic money laundering: Use of funds that a person knows (or has high probability of awareness) are proceeds of unlawful activity.

2. International money laundering: Transfer of criminal proceeds into or outside of the U.S.

3. Money laundering related to an undercover ‘sting’ case; and

4. Knowingly spending more than $10,000 in criminal proceeds

* 1. **Federal Enforcement**

1. DOJ responsible for investigation and prosecution

2. IRS criminal investigation section has investigative jurisdiction over money laundering crimes

3. DEA oversees AML operations in connection with drug trafficking and drug violence

4. ICE responsible for investigating money-laundering activities associated with people moving illicitly across U.S. borders

5. U.S. Postal Service has criminal investigative authority over money laundering offenses

1. **CYBERSECURITY REGULATIONS**
2. **Key Legislation/Regulations**
3. Financial Sector: Gramm-Leach-Bliley Act of 1999 (GBLA), Pub. L. No. 106-102, 113 Stat. 1338 (1999).
   1. Financial institutions required to protect security and confidentiality of customers’ non-public personal information.
4. Chemical Sector: Chemical Facility Anti-Terrorism Standards (CFATS), 6 C.F.R. § 27 (2007).
   1. High-risk chemical facilities required to prepare security vulnerability assessments and implement site security plans.
   2. Must make efforts to deter cyber-sabotage including on-site or remote access to critical process controls.
5. Healthcare/Public Health Sector: Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat 1936 (1996).
   1. Federal government required to create security standards to protect individually identifiable health information.
   2. DHHS authorized to adopt national standards to protect the confidentiality and integrity of electronic protected health information/“ePHI” (HIPAA Security Rule).
6. Energy Sector: Energy Policy Act of 2005, Pub. L. 109-58 (2005).
   1. Authorized North American Electric Reliability Corporation (NERC) to set mandatory standards for the operation of U.S. power systems.
   2. Cybersecurity framework: Protection, deterrence, prevention, limitation, and recovery.
7. Federal Information Security Management Act of 2002 (FISMA), 404 U.S.C. § 3541 (2012).
   1. Government agencies required to ensure system security
8. Executive Order 13636: Improving Critical Infrastructure Cybersecurity, 78 FR 11739 (Feb. 12, 2013).
   1. Aimed to establish specific cybersecurity requirements and standards.

1. **National Institute of Science and Technology**
2. Tasked with establishing a voluntary “cybersecurity framework” companies may adopt.
3. First framework, consisting partly of private-sector best practices, released in February 2014.

**COURSE MATERIALS**

Cecil Hunt, *U.S. Export Controls and Economic Sanctions – An Overview*, SN056 ALI-ABA 193 (May 2008)

Debra Burke, *At the Intersection of Export Control Regulations and Employment Discrimination Law*, 45 Am. Bus. L.J. 565 (2008) (Parts II-IV)

*Anti-Money Laundering and Related Regulatory Regimes: The Separate OFAC Regime*, 1-18 Banking Law Manual § 18.05

*Chapter 12 Acquisition Agreement: Closing Conditions: Regulatory Compliance*, 1-12 M&A Practice Guide § 12.05 (Section 4(b))

Xingxing Li, *National Security Review in Foreign Investments: A Comparative and Critical Assessment on China and U.S. Laws and Practices*, 13 Berkeley Bus. L.J. 255 (2016) (Parts I.A & II)

Greg Golding, *Australia’s Experience with Foreign Direct Investment by State Controlled Entities: A Move Toward Xenophobia or Greater Openness?*, 37 Seattle U.L. Rev. 533 (2014) (Skim Part VI.A)

U.S. Department of Justice & U.S. Securities & Exchange Commission, A Resource Guide to the Foreign Corrupt Practices Act 2-35 (2012)

Richard Grime et al., *The U.K. Bribery Act*, 62-9 CAIL Annual Institute on Oil & Gas Law § 9.04

Bruce Zagaris, *International Trust and Estate Planning: Ethical Issues in Offshore Planning*, SL032 ALI-ABA 199 (August 2005) (Part III)

Lamia Matta et al., *Getting the Deal Through: Anti-Money Laundering: United States*, 2016-1 GTDT: Anti-Money Laundering

Eric A. Fischer, The Expanding Cyber Threat, Congressional Research Service (Jan. 27, 2015) (Statement Before Subcommittee on Research & Technology, Committee on Science, Space, and Technology, U.S. House of Representatives