

Managing U.S. Export Control Requirements as a Non-U.S. Entity: Understanding and Mitigating Compliance Risks for the Logistics Industry

Tatman R. Savio

Foreign Register Lawyer, Akin Gump Strauss Hauer & Feld LLP (Hong Kong)

September 2, 2015

Agenda

- Overview and Impact of Relevant Law
- Export Controls
- Economic Sanctions
- Penalties and Enforcement – The Costs of Non-compliance
- How to Manage Compliance

Overview and Impact of Relevant Law

Export Controls vs. Economic Sanctions

What's the Difference?

Export Controls – controls on the international movement of goods, software, and technology (collectively, “items”) and sometimes services.

- May be commercial/dual-use or military.
- Typically focused on strategic items, but some controls on embargoed countries can apply to **any** item.
- More than one set of rules may apply to a single transaction (*e.g.*, U.S., EU and Singapore controls).

Economic Sanctions – restrictions on dealings (not necessarily involving items) with other countries, persons or entities based on security or policy concerns.

- Not limited to goods / software / technology.
- Coverage may include financial transactions, commercial agreements, or assistance more broadly.

Why Is Compliance Important?

Global security

- Export controls and sanctions are based on national security and foreign policy considerations.

It's the law

- U.S. export control and sanctions laws have extraterritorial application - for example, to the extent you deal in U.S. origin items, or employ U.S. nationals.

U.S. government aggressively enforces these laws

- Recent enforcement actions targeting freight forwarders

Penalties are severe for non-compliance

- Monetary fines, imprisonment, denial of export privileges, debarment, reputational/commercial impact

Your company requires it – or it will!

- Most companies have a code of conduct and other policies/procedures mandating compliance with all applicable laws generally, and international trade laws specifically.

Your business partners want to see it

- You become a liability for them if you do not have compliance policies and procedures in place.
- Many U.S. and EU companies will steer clear of doing business with you – **no matter how significant the bottom line, the compliance risk is greater.**

Key Questions Every Exporter Must Ask for Every Export

WHAT is being exported?

- Commercial/Dual-Use vs. Military vs. Nuclear
- Tangible vs. Intangibles (tech data, services)
- Classification

WHERE is it being exported?

- Sanctioned countries
- Countries for which license is required

WHO will be receiving the export?

- Denied or Restricted Parties

HOW will it be used? What is the end use?

- Nuclear, missiles, chemical/biological weapons, WMDs

IS authorization required for the export?

- Where is it going?
- What is the item?
- Who is receiving it?
- How will the item be used?

RED FLAGS

- Is the item at risk for diversion?
- Is the customer reluctant to share information on end-use / end-user?

USG's Expectations for Freight Forwarding Community

- Members of the international forwarding community play a key role in ensuring the security of the global supply chain, stemming the flow of illegal exports, and helping to prevent Weapons of Mass Destruction (WMD) and other sensitive goods and technologies from falling into the hands of proliferators and terrorists.
- Forwarding agents have compliance responsibilities even when their actions are dependent upon information or instructions given by those who use their services.
- Agents are responsible for the representations they make in filing export data.
- No person, including an agent, may proceed with any transaction knowing that a violation of the EAR has, is about to, or is intended to occur.

- [BIS Freight Forwarder Guidance](#)

“[A]ll parties that participate in transactions subject to the EAR must comply with the EAR.” – Section 758.3 of the EAR

Export Controls

U.S. Export Control Laws: Why Do U.S. Export Controls Matter in Asia?

- Global Reach:
 - U.S. Export Controls apply both inside and outside of the United States.
 - U.S. Export Controls “follow the item”.
- U.S. Export Controls apply to exports, re-exports, and transfers of:
 - U.S.-origin goods (commodities, software, etc.) and technology
 - Certain goods and technology manufactured or developed outside of the U.S. if:
 - The item or technology incorporates certain levels of U.S.-origin goods and technology;
 - The item is produced from certain U.S.-origin technology.
 - Items physically located in the U.S.
 - Deemed Exports
- **This means that transactions can be subject to U.S. export controls even if no U.S. person or U.S. company is involved in the transaction.**



U.S. Export Control Laws: Export Jurisdiction and Restrictions

- Two **primary** export control regimes:
 - *Military*. International Traffic in Arms Regulations (“ITAR”) administered by the State Department’s Directorate of Defense Trade Controls (“DDTC”) -> U.S. Munitions List (“USML”)
 - *Dual-Use/Commercial*. Export Administration Regulations (“EAR”) administered by the Commerce Department’s Bureau of Industry and Security (“BIS”) -> Commerce Control List (“CCL”)

- Both the ITAR and EAR identify **items** controlled for export and **certain countries** that are subject to embargoes or special controls.
 - ITAR arms embargo includes China and Myanmar, among other countries. Policy of denial for North Korea, Sri Lanka, and Vietnam, among other countries.
 - EAR embargo -> Cuba, Iran, North Korea, Sudan, and Syria.

- Restrictions may also be related to particular designated entities
 - Entity List
 - Denied Persons List
 - Unverified List
 - Nonproliferation Sanctions Lists
 - Debarred List

- Licenses and license exceptions

Economic Sanctions

U.S. Economic Sanctions: Why Do U.S. Economic Sanctions Matter in Asia?

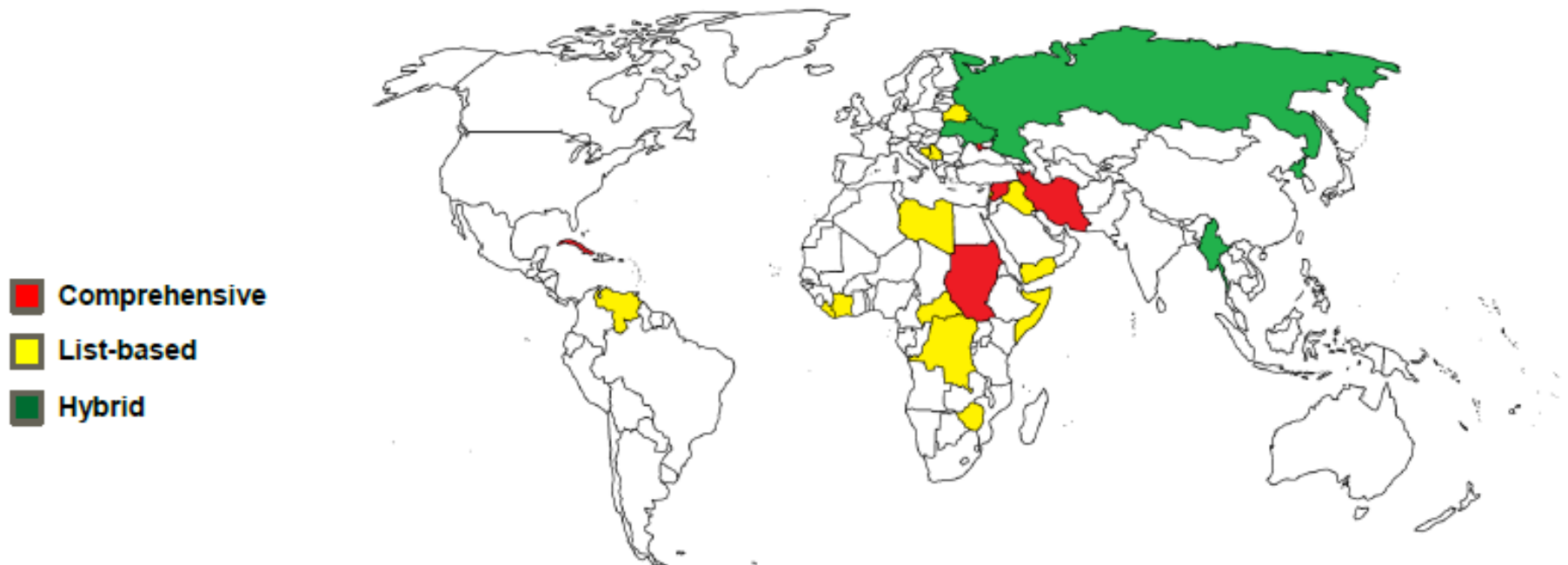
- Global Reach:
 - U.S. Economic Sanctions apply both inside and outside of the United States.
 - U.S. Economic Sanctions “**follow the person**”.
- Overview of jurisdiction
 - Applies to “U.S. persons,” defined to cover:
 - U.S. citizens and permanent residents, *wherever located*;
 - Companies organized under U.S. law (including foreign branches of U.S. companies); and
 - Any person to the extent located in the U.S.
 - U.S. persons may not engage in “**prohibited facilitation**”
 - Under some sanctions programs, jurisdiction extends to non-U.S. companies
 - Non-U.S. persons may not conspire with, aid or abet, or cause the violation of U.S. sanctions laws by a U.S. person
- **This means that transactions undertaken by non-U.S. companies may be subject to U.S. economic sanctions in many instances**

How U.S. Sanctions Programs Work

- **Comprehensive Sanctions Programs (Crimea, Cuba, Iran, Sudan, and Syria)**
 - **U.S. Persons** – With very limited exceptions, U.S. Persons are prohibited from engaging in virtually any unlicensed transaction or dealing with, in, or involving these countries, their governments, or any entity owned or controlled by the governments of these countries
 - **Non-U.S. Persons** – Iran, Cuba, and Syria programs may apply to non-U.S. persons.
- **Limited Sanctions Programs (Burma, North Korea, Russia)**
 - Focused on particular activities involving these countries by U.S. persons, including:
 - Prohibitions on new investment
 - Prohibitions on financial services
 - Prohibitions on export and/or imports
 - Designations of prohibited parties
- **“Targeted sanctions”** on specific individuals and entities with which U.S. persons – and, in certain cases, non-U.S. persons – cannot deal or perform certain transactions. OFAC maintains several lists, including:
 - List of Specially Designated Nationals (“SDN List”)
 - The List of Foreign Financial Institutions Subject to Part 561 (“Part 561 List”)
 - List of Foreign Sanctions Evaders (“FSE List”)
 - Sectoral Sanctions Identifications List (“SSI List”)
- License and License Exceptions

Current U.S. Sanctions Programs

- **Iran**
- **Cuba**
- **Sudan**
- **Syria**
- **Crimea**
- **Burma**
- **North Korea**
- **Russia**
- **Ukraine**
- **Iraq**
- **DRC**
- **CAR**
- **Belarus**
- **Cote d'Ivoire**
- **Lebanon**
- **Liberia**
- **Libya**
- **Somalia**
- **Yemen**
- **Balkans**
- **Zimbabwe**
- **Venezuela**



Penalties and Enforcement

Costs of Non-compliance

- **Costs of non-compliance with U.S. export control and sanctions laws can be significant, even for non-U.S. companies:**
 - **Penalties:** Severe civil and criminal penalties for corporations and individuals
 - **Criminal:** Under ITAR/EAR and most sanctions programs, the maximum fine is \$1 million per transaction and/or up to 20 yrs. in prison
 - **Civil (strict liability):** Under EAR and most sanctions programs, the maximum fine is \$250K per transaction or twice the value of the transaction, whichever is greater. Under ITAR, \$500K per transaction.
 - **Administrative actions:** Asset blocking; denial orders for export related violations; debarment from government contract eligibility; restriction on ability to receive U.S. exports; appointment of a government monitor; license revocation, suspension, or renewal delay
 - **Damage to Reputation:** Consumers and business partners may be reluctant to work with you, or impose additional conditions on contracts
 - **Business Hurdles:** Impact on future license applications
 - **Costs of Investigation:** Significant, regardless of outcome
- **The USG takes enforcement against non-U.S. entities seriously.**



U.S. Enforcement Action Case Study: Aramex Emirates (2014)

- In May 2014, **UAE-based company** Aramex Emirates was charged with causing, aiding, and/or abetting the unlawful export and re-export of U.S.-origin computer monitoring products to Syria
- Aramex Emirates **agreed to receive the two shipments from another freight forwarder in the UAE** and, following receipt of the items, forwarded them from the UAE to Syria
- BIS imposed a **\$125,000** civil penalty
- “[This] settlement shows the *importance of compliance with U.S. law by foreign freight forwarders* handling items subject to U.S. export controls. The items in question could [have been] used by the Syrian government to monitor Internet activity and block pro-democracy websites as part of its brutal crackdown against the Syrian people.”
– **Under Secretary of Commerce Eric Hirschhorn**
- Follow-up to Computerlinks case (2013), in which that company paid \$2.8 million penalty and agreed to compulsory third party audits.



U.S. Enforcement Action Case Study: 3K Aviation Consulting & Logistics (2014)

- In January 2014, BIS issued a Temporary Denial Order (“TDO”) against 3K Aviation Consulting & Logistics (“3K Aviation”) to deny export privileges to prevent an “imminent violation” of the EAR.
- In December 2013, two U.S.-origin General Electric aircraft engines were transported to 3K Aviation, located in Turkey. BIS was notified that 3K Aviation was preparing to immediately re-export the engines to Iran without the required USG authorization
- **Penalties**
 - TDO – 3K Aviation’s export privileges were temporarily denied for a period of 180 days
 - For the duration of this period, 3K Aviation was prohibited from participating in any way in any transaction involving any item exported or to be exported from the U.S. subject to the EAR



U.S. Enforcement Action Case Study: Gatewick LLC (2014)

- In August 2014, **UAE-based company** Gatewick LLC settled allegations by BIS related to the unlawful export of 2,300 motherboards from U.S. to Iran
- Gatewick was the sole booking agent for Mahan Airways, an Iranian airline, and Gatewick entered into an agreement with Seyed Mousavi Trading, an Iranian trading company, to ship items to UAE for later shipment to Iran
- **Allegations**
 - **Conspired with others** to bring about the unlicensed export of items subject to U.S. regulations from the U.S. to Iran, via the UAE
 - **Caused, aided, or abetted the unauthorized export** of goods to Iran
 - Acted contrary to a BIS denial order by **facilitating the acquisition by Mahan Airways, an Iranian airline and a denied person**, of items subject to U.S. regulations
- **Penalties**
 - Civil penalty of **\$40,000**;
 - **2-year denial period** during which Gatewick is prohibited to export any items from US that are subject to the U.S. Export Administration Regulations (followed by 5-year probationary period)



U.S. Enforcement Action Case Study: Kintetsu World Express (U.S.A.), Inc. (2014)

- In September 2014, Kintetsu World Express (U.S.A.), Inc. (“KWE”) settled charges by BIS that it had facilitated the unlawful export of spiral duct machines and related accessories from the United States to a SDN party in China
- Acting as a freight forwarder, KWE arranged for the shipment of the items to China National Precision Machinery Import/Export Corporation (“CPMIEC”)*, a party on the SDN List, and filed an export declaration indicating that the export was designated “NLR” (No License Required)

■ Allegations

- **Caused, aided, or abetted the unauthorized export** of goods to an entity on the SDN List

■ Penalties

- Civil penalty of \$30,000

** CPMIEC appeared on the SDN List because it had supplied Iran’s military and Iranian proliferators with missile-related dual-use items.*



U.S. Enforcement Action Case Study: General Logistics International, Inc. (2015)

- In January 2015, General Logistics International, Inc. (“GLI”) settled charges by BIS related to the unlawful export of scrap steel from the United States to a company on BIS’s Entity List in Pakistan
- Acting on behalf of a Canadian company, GLI arranged for the trucking of scrap steel from the exporter’s location to the port of export, and arranged for the shipping of the steel to People’s Steel Mills in Pakistan. GLI also filed shipping documentation, including an export declaration that indicated the export was designated “NLR” (No License Required)
- **Allegations**
 - Aided or abetted the unauthorized export of goods to an entity on BIS’s Entity List
- **Penalties**
 - Civil penalty of \$90,000



How to Manage Compliance

Identify Your Risk

- Compliance is not one-size fits all
- Think critically about your business model – develop a program to mitigate that risk.
- Start with the questions we flagged at the beginning of the presentation:

WHAT is being exported?

- Commercial/Dual-Use vs. Military vs. Nuclear
- Tangible vs. Intangibles (tech data, services)
- Classification

WHERE is it being exported?

- Sanctioned countries
- Countries for which license is required

WHO will be receiving the export?

- Denied or Restricted Parties

HOW will it be used? What is the end use?

- Nuclear, missiles, chemical/biological weapons, WMDs

IS authorization required for the export?

- Where is it going?
- What is the item?
- Who is receiving it?
- How will the item be used?

RED FLAGS

- Is the item at risk for diversion?
- Is the customer reluctant to share information on end-use / end-user?

Potential Exposure for Freight Forwarders Located Outside the United States

■ Common Business Risks -

- You may provide services to US companies for export/reexport of items
- You may provide services to non-US companies that are exporting/reexporting items subject to the EAR or ITAR
- You may do business with customers or business partners in destinations that are sanctioned by the U.S.
- You may employ U.S. persons who are subject to U.S. sanctions laws
- You may be the foreign subsidiary of a U.S. company
- There may be other U.S. parties that are involved in particular transactions

■ Risks Associated with Doing Business in Singapore

- Singapore is a major transshipment hub for the Asian market.
- While many items may not initially require an export license, exporters need to be aware that two-thirds of items exported to Singapore are re-exported to third countries that may have more stringent licensing requirements that require additional export licenses. See [Export.gov, Doing Business in Singapore](#)

BIS Guidance on Compliance for Freight Forwarders

- Implement a compliance program
 - Key elements – Corporate commitment, risk assessment, written policies/procedures, training, monitoring/auditing, reporting, recordkeeping. See [BIS EMCP guidance](#).
- Conduct screening and diligence; resolve red flags
 - RPLs
 - Embargoed/Sanctioned countries
 - End-use / end-user
 - [“Know Your Customer” guidance](#) and [“Red Flags” indicators](#) – Supp. 1 to Part 732
 - Diversion risk
 - Ten General Prohibitions in Part 736 of the EAR.
- Build compliance partnerships and share compliance strategies with customers.
 - Even if forms like the BIS-711 (Destination Control Statement) and the Letter of Acceptance and License Conditions are not required by the EAR from your overseas business partners, you may wish to require them.
- Ensure recordkeeping compliance
- Voluntary self-disclosure process

Compliance Program Resources

- USG resources on Compliance Programs:
 - BIS provides guidance on an Effective Export Management and Compliance Program [here](#).
 - DDTC provides Compliance Program Guidelines [here](#).

- Pay attention to trends in enforcement – effective way to understand trending risk areas and mitigating factors.

- Settlement Agreements generally outline the scope and nature of a company's violations and provide a roadmap for compliance that is approved by the U.S. government.



Know Your Customer - Red Flags

- Delivery dates are vague, or deliveries are planned for out of the way destinations.
- A freight forwarding firm is listed as the product's final destination.
- The shipping route is abnormal for the product and destination.
- Packaging is inconsistent with the stated method of shipment or destination.
- The customer or purchasing agent is reluctant to offer information about the end-use of the item.
- The product's capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery.
- Item is incompatible with the technical level of the country to which it is being shipped.
- Customer has little or no business background.
- Customer is unfamiliar with the product's performance characteristics but still wants the item.



Compliance Programs: Best Practices and Pitfalls

■ Common Pitfalls:

- Stand-alone policies that are not integrated into business practices;
- Lack of clarity in terms of responsibilities;
- Inadequate training for personnel;
- Lack of written procedures; reliance on single person who handles these issues.

■ Best Practices:

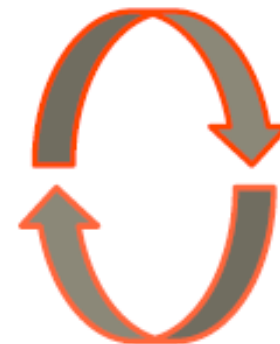
- Integrate export compliance into standard business processes;
- Use automated IT tools, where possible;
- Identify personnel with technical skills, and train them on compliance;
- Tailor training to specific personnel roles, but make sure **everyone is aware of red flags**;
- Conduct on-going assessments to ensure your program meets business needs.

■ Screen, screen, screen!

- Automate, where possible
- Embargoed destinations
- Sensitive items
- All parties to a transaction (e.g., sold-to, ship-to, intermediate consignee, end-user)

What do you do when you've identified an issue?

- Stop potential offending activity
- Investigate potential violations
- Engage in-house/outside counsel at early stage to help oversee the investigation (e.g., collect data, interview those involved, etc.)
- Understand the scope of the issue – one-off problem or systemic issue
- Determine whether a violation has occurred and whether to file a voluntary self-disclosure (“VSD”)
 - Great weight mitigation for export compliance program that results in VSD
 - Over the past several years, on average only 3% of VSDs have resulted in a civil penalty from BIS (July 2015 edition of [Don't Let This Happen to You](#))
- Understand the root cause of the violation – only way to prevent a recurring violation is to understand why it happened
- Implement corrective actions
 - Engage in a continual loop of compliance enhancement



Questions



TATMAN R. SAVIO
tsavio@akingump.com
+852 3694 3015

Thank you!