Export Compliance Insights: China Enforcement Actions

Advanced Topics in Customs Compliance Conference

By: Luis Arandia, Jr. & Clinton Yu, Barnes & Thornburg

Feb. 5, 2025

Presenters from Barnes & Thornburg LLP

Luis Arandia, Jr.
Partner, International Trade Group
Luis.Arandia@btlaw.com
(202) 408-6909

Clinton Yu
Partner, International Trade Group
Clinton.Yu@btlaw.com
(202) 371-6376

BARNES & THORNBURG LLP

Firm Overview

Barnes & Thornburg is a national, full-service law firm. We serve clients worldwide and collaborate smoothly across offices.

Our deep bench of talent means we can easily pull in additional support as needed.

50+	800+	AmLaw 100
practice areas	legal professionals	law firm

International Trade Practice Areas

- Export Controls and Sanctions
- Customs and Imports
- Trade Remedies (AD/CVD)
- CFIUS (national security review of foreign investments)
- Trade Negotiations, Legislation and Policy

BARNES & THORNBURG LLP

Export Controls and Sanctions Experience

Export Controls Capabilities

- Our International Trade team provides comprehensive compliance, licensing, enforcement and policy counsel on export control and sanctions matters to a wide range of clients: early-stage companies, small to medium-sized companies, large multinational corporations, and universities.

ZTE Monitorship (2018-Present)

- Barnes & Thornburg partner Roscoe C. Howard Jr. was appointed by the U.S. Department of Commerce to serve as the Special Compliance Coordinator for Zhongxing Telecommunications Equipment Corporation (ZTE) and its affiliates.
- The largest export control monitorship in U.S. history stems from the historic settlement between the Department of Commerce and ZTE that includes: $1.761 billion fine, a 10-year probationary period, and the installation of the Special Compliance Coordinator to conduct regular and comprehensive compliance supervision by a team answerable to Commerce's Bureau of Industry and Security.
- Luis Arandia and Clinton Yu, serve in various leadership positions within the monitorship.

BARNES & THORNBURG LLP

Today's Topics

1. **Setting the Stage: U.S. Export Controls and Sanctions**

2. **China Enforcement Actions (EAR/ITAR focus) and the Following Risk Areas:**

   - **Due Diligence/Screening Challenges**
   - **Technical Data**
   - **Foreign Produced Items**
   - **Freight Forwarder**

BARNES & THORNBURG LLP

This is a public, non-confidential forum so please do not provide any confidential information.

Questions asked will be answered in the hypothetical.

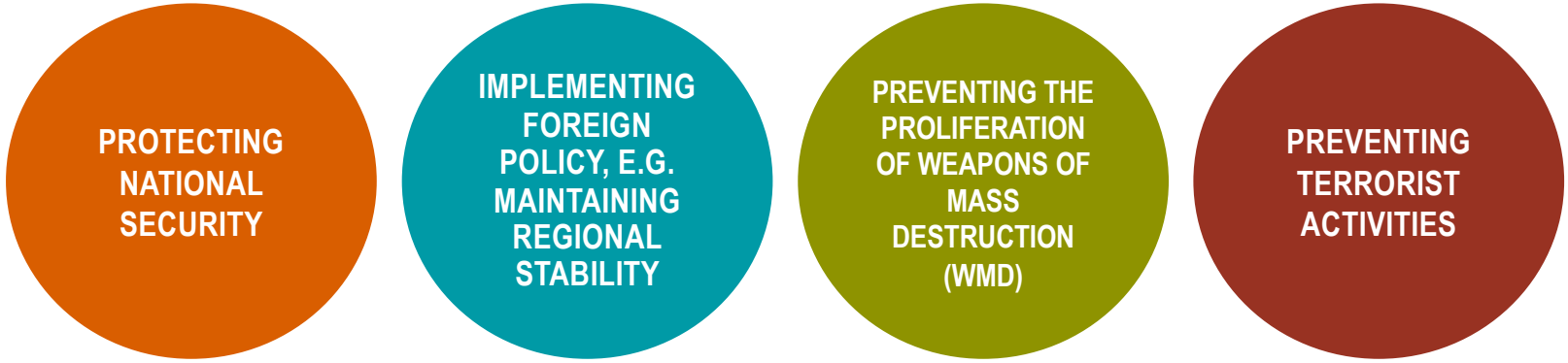
Information provided should not be construed as legal analysis, advice, or opinion on any specific facts or circumstances. This seminar, discussion, and question and answer session is not intended to specifically address or answer any specific legal issues. Please direct specific legal issues to your attorney for further consideration.

BARNES & THORNBURG LLP

SETTING THE STAGE: U.S. EXPORT CONTROLS AND SANCTIONS

BARNES & THORNBURG LLP

U.S. Export Control Policy: Restricts the Export, Re-export, and Transfer of Goods, Services and Technology for the Purposes of:



BARNES & THORNBURG LLP

Jurisdiction and Regulations

- Directorate of Defense Trade Controls (“DDTC”)
- International Traffic in Arms Regulations (“ITAR”)
- U.S. Munitions List (“USML”)
- Defense articles and defense services

- Bureau of Industry and Security (“BIS”)
- Export Administration Regulations (“EAR”)
- Commerce Control List (“CCL”)
- Export Control Classification Numbers (“ECCN”) and “EAR99”
- “Dual-use” and “600 Series” items

- Office of Foreign Assets Control (“OFAC”)
- Economic sanctions programs
- Embargoed countries and destinations
- Specially Designated Nationals (“SDN”) and other restricted parties

BARNES & THORNBURG LLP

Potential Consequences for Non-Compliance

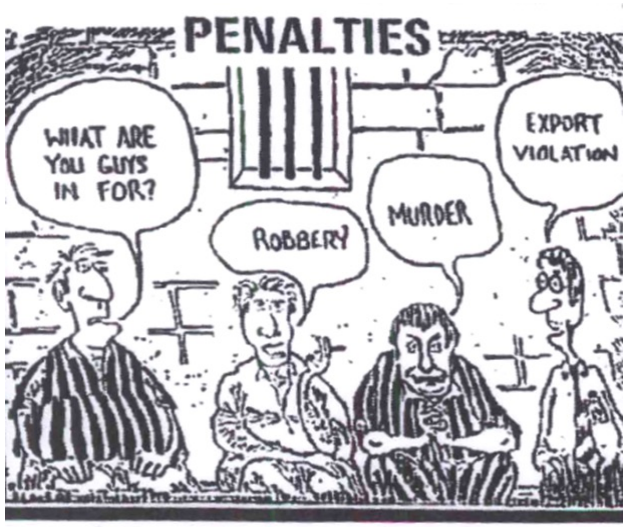
	Max Civil Monetary Penalties Per Violation (Inflation Adjusted Annually)
ITAR	**Greater of $1,271,078 or 2x value of transaction**
EAR	**$374,474 or 2x value of transaction**
OFAC	**$377,700 or 2x value of transaction**

- Penalties can also include debarment, audits, monitors, seizure and forfeiture of goods, and other corrective actions

BARNES & THORNBURG LLP

Criminal Penalties

- In addition to civil penalties, the agencies thru the DOJ can pursue criminal penalties
- Criminal monetary fines can be up to $1 million per violation
- Can also include up to 20 years of imprisonment



Source: Society for International Affairs

BARNES & THORNBURG LLP

DUE DILIGENCE/SCREENING CHALLENGES

Enforcement – Due Diligence and Screening

TE Connectivity (2024)

- BIS imposed a $5.8 million civil penalty against TE Connectivity and its related Hong Kong entity for shipments of low-level items to parties tied to the People's Republic of China's (PRC) hypersonics, unmanned aerial vehicles (UAV), and military electronics programs.
- Between Dec. 2015 to Oct. 2019, TE made 79 unauthorized exports:
  - Chinese companies on the BIS Entity List
  - Unauthorized end use (i.e., unmanned aerial vehicle "UAV" end use)
- Most of the items involved were classified EAR99.
- Some sales occurred through distributors in China. Certain TE employees in China concealed the true end users.
- Among the unauthorized exports included exports to "NPU North West Poly Tech University" and BIS Entity List included four aliases for NPU.
- TE's screening processes failed to flag these transactions

Prohibited End Uses and End Users

Despite the items being classified as EAR99, TE still needed to ensure the items were not going to a prohibited end user or prohibited end use. Remember the EAR's General Prohibitions 4-10.

- Prohibited End **Users**, such as:
  - Entity List and Unverified List: many entities listed are in China
  - Military End Users: diligence challenges in China due to civil/military fusion
  - Various other lists, e.g., Debarred or Denied Party Lists, Specially Designated Nationals (SDNs) and non-SDN Lists

- Prohibited End **Uses**, such as:
  - Missile technology, UAVs, biological/chemical/nuclear weapon
  - Advanced computing, supercomputer, IC manufacturing end use restrictions
  - Military end use and military intelligence end use restrictions

BARNES & THORNBURG LLP

Insight: Screening and Due Diligence Challenges

Doing business in China requires a high level of awareness, even if the exported items are EAR99. In TE's case, there were end user/use certificates, yet violations still occurred. Be trained on and aware of red flags.

What are some potential <u>end use/user</u> red flags when doing business in China?

- Similar name/address to restricted party
- Masking end user- consignee is a distributor/trading company
- English and Mandarin name variants do not match
- Co-location with entities of concern, including university campuses
- Generic technology applications
- Obfuscating location/address
- Masking defense affiliations
- Omitting website military references or little to no web presence

BARNES & THORNBURG LLP

Due Diligence Resources

Supp. No. 3 to EAR Part 732 "Red Flags" and Know Your Customer is a great resource. Some examples:

- Party's address is similar to that of a party on a prohibited party or sanctions lists, or their physical location is unusual (e.g., residential address)
- Party listed as ultimate consignee does not typically engage in business consistent with using the exported items
- Customer is reluctant to offer information about end use of the item

BARNES & THORNBURG LLP

Advanced Computing/Supercomputer Rules

BIS has over the past few years published amendments to the EAR targeting China's use of advanced computing, supercomputer, and semiconductor manufacturing technology for military advantage.

- Within the rules, there are several that are end user/end use based, such as:
  - Restricting the ability of U.S. persons to support the development or production of advanced ICs or shipment of semiconductor manufacturing into China and other countries of concern
  - End use controls on supercomputers, advanced-node ICs, and semiconductor manufacturing equipment in China and other countries of concern

- BIS has added more red flags to Supp. No. 3 Part 732 to address this risk area.
  - Example: new customer request an item or service that was designed or modified for an existing or former customer that is now designated on the Entity List.

BIS Military End User Rules

Military End Use/User (MEU) rules are intended to prevent entities in certain countries, including China, to address national security risks associated with civil/military fusion.

- Military end use:
  - Incorporation into a defense article or "600 series" munitions item
  - Any item that supports/contributes to the operation, installation, maintenance, repair, overhaul, refurbishing, development, or production of a military/munitions item

- Military end user:
  - Armed services and national guard
  - National police
  - Government intelligence/reconnaissance organization (other than military-intelligence)
  - Any person/entity whose actions/functions are intended to support a military end use

BARNES & THORNBURG LLP

BIS Military End User Rules

- Scope for Belarus/Russia: all items subject to EAR (incl. foreign-produced items per 15 CFR § 734.9(g) and EAR99 items)
- Scope for Burma, Cambodia, China, Nicaragua, and Venezuela: specific CCL items, unless otherwise informed by BIS.

Why Care about MEU Rules?

- Common reasons why some exporters believe the MEU rules do not apply or are not a high compliance risk:
  - All items we export are widely-available or COTS products that require no export license to almost all global destinations.
  - My company is not in the defense industry.
  - We use screening software, so our systems will automatically stop the company from doing business with a listed military end user.

BARNES & THORNBURG LLP

Global Screening and Due Diligence Challenges

Although China presents its own unique set of export compliance challenges, screening and due diligence practices applicable to other countries (most notably, Russia) will be helpful.

Examples:

- Identifying items that are at higher risk of diversion (e.g., Common High Priority List (CHPL) items)
- Third countries flagged as higher risk for transshipment
- 50% rule and identifying ultimate beneficial owners

BARNES & THORNBURG LLP

Due Diligence and Screening Hypothetical

- Your company asks you to conduct due diligence and restricted party screening for a Chinese electronics distributor/vendor. The Chinese company's business address is located in Hong Kong.

- In screening the address, you learn that the Chinese company shares the same address as two entities designated on the SDN list. But the screened entity does not have a name match with the two SDN's.

- How do you handle? Can the red flag of an address match be overcome by additional due diligence?

BARNES & THORNBURG LLP

Due Diligence and Screening Hypothetical

- When there is an address match but no name match, OFAC notes that this is a requirement to conduct additional diligence, e.g., requiring more information about the entity you're dealing with and seeing what information they can provide to help clear up the potential match.

- Ensure a risk-based approach on the additional diligence and depending on information collected, take that risk-based approach and see if the information is enough to clear up the potential match.

- Perhaps collect information about ownership to verify whether OFAC's 50% rule applies.

BARNES & THORNBURG LLP

EXPORTS OF TECHNICAL DATA

Enforcement – Technical Data

3D Systems Corp. (2023)

- 3D printing technology company headquartered in the U.S. with dozens of global locations, including in China.
- DDTC imposed a $20 million civil penalty, plus requirements to hire an external special compliance officer for one year and conduct two external audits.
- BIS imposed a $2.8 million civil penalty and required two external audits.
- Three main issues: (i) export of technical data to or for overseas third-party suppliers, (ii) export of technical data to foreign employees, (iii) export of technical data between IT servers.

BARNES & THORNBURG LLP

Enforcement – Technical Data

3D Systems Corp. (cont.)

- Issue #1:
  - 3D is U.S. manufacturer that also utilized third-party suppliers, primarily in China, to assist in fulfilling customer orders for on-demand manufacturing solutions. 3D would receive technical data from its U.S. customers (e.g., blueprints).
  - 3D failed to obtain the accurate export classification of its customers' technical data, which turned out to be ITAR and highly-controlled EAR technical data requiring an export license. As part of the quotation process, 3D ended up e-mailing the technical data to its staff or directly to the third-party suppliers in China.

BARNES & THORNBURG LLP

Enforcement – Technical Data

3D Systems Corp. (cont.)

- Issue #2:
  - 3D had foreign-person employees in the U.S., and IT system did not track individual access of ITAR-controlled technical data. 3D also had foreign-person employees in roles that were likely to receive ITAR-controlled technical data, resulting in "deemed exports" of ITAR technical data without authorization.
- Issue #3
  - 3D's email exchange server was stored in the U.S. but was also "mirrored" as a backup in an unencrypted server in Germany. The email exchange server contained export controlled technical data, e.g., in quotation emails or troubleshooting technical issues. The "mirroring" of the email exchange server resulted in unauthorized exports of ITAR and EAR technical data.

Insight: Voluntary Self Disclosures

A customer notified 3D of potential violations in connection with export of technology to China and informed 3D that it had filed a disclosure with BIS. Nearly 2 years later, BIS reached out to 3D about its conduct and issued a warning letter. During this time, 3D continued to export technical data to China. 3D eventually filed disclosures and expanded its disclosure to ITAR violations.

Decision-making for voluntary disclosures

- When is the right time to file a voluntary disclosure?
- Which agency to file with?
- Is the disclosure really voluntary, especially if China is involved?

BARNES & THORNBURG LLP

Insight: Voluntary Self Disclosures

- **Timing**: VSD should be filed prior to the time that the U.S. Government, has learned the same or substantially similar information from another source and has commenced an investigation or inquiry in connection with that information.

- **Jurisdiction**: If unsure of jurisdiction, you can file an initial notification of voluntary disclosure with both BIS and DDTC.

- **China** is a proscribed country under the ITAR (126.1). Also, BIS says failure to voluntarily disclose "significant potential violation" can be an aggravating factor.

BARNES & THORNBURG LLP

Insight: Handling of Technical Data/Technology

3D Systems took corrective action by implementing formal written work instructions and also created a secure, auditable portal to handle storage and transfer of technical data

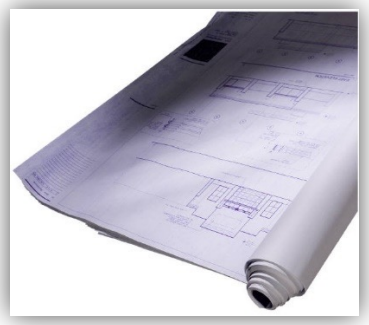
- What procedures does your company have for identifying and the intake/handling of technical data from third parties?
  - Export control certification documenting jurisdiction and export classification
  - Incorporate ITAR/EAR clauses in commercial documents, such as in Non-Disclosure Agreements, Terms and Conditions, Contracts, Purchase Orders/Confirmations
  - Identify potential problems in advance of sending technical data (e.g. require employees downloading controlled technical data to confirm location and nationality of recipient)

BARNES & THORNBURG LLP

Forms of “Technical Data” and “Technology”

Any tangible or intangible form such as:

- Written or oral communications (emails, phone or video conference)
- Blueprints
- Drawings
- Photographs
- Plans
- Diagrams
- Models
- Manuals
- Engineering designs and specifications
- Computer-aided design files
- Formulae
- Tables
- Electronic media
- Information revealed through visual inspection (e.g., technical demonstration)



Technical Data/Technology - Best Practices

What if the technical data originates from your company?

- Marking of Technical Data
  - Drawings, specs, etc.
  - Include jurisdiction and classification for such data

Example:

"Technical Data/Technology Subject to U.S. International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). Export, reexport or transfer outside of the U.S. or to non-U.S. persons, whether located in the U.S. or outside the U.S., without prior U.S. Government authorization is prohibited"

BARNES & THORNBURG LLP

Insight: “Deemed Exports”

3D did not track individual access of export controlled technical data. 3D also placed foreign person employees in roles that were likely to receive export controlled technical data without first obtaining authorization.

A “Deemed Export” can occur through any release of “technical data” or “technology” to a “foreign national” in the United States, such as:

- Visual inspection of equipment and facilities that *reveals* technical data/technology
- Meetings, teleconferences, web meetings
- Electronic transfers, emails
- Providing source code to a foreign person (not object code)

BARNES & THORNBURG LLP

Insight: “Deemed Exports”

- Review your export compliance procedures on “access”
  - Having procedures to prevent access may be the best practice for companies with foreign person employees and frequent visitors
    - Dedicated server or electronic files; password protection; locked file cabinets and file rooms; training foreign employees on what they can’t see
    - Relying on NDA’s, certificates, audits

- Be wary though of discrimination violations in efforts to comply with export controls. Recent enforcement by DOJ: “[E]xport control laws do not justify or authorize an employer to discriminate against non-U.S. citizens”. Employer cannot exclude candidates from consideration for employment based on nationality.

BARNES & THORNBURG LLP

Technical Data Hypothetical

- Your company asks you to search for lower cost overseas vendors in China to manufacture a customer-designed item. In your RFQ process, you are supposed to attach the customer's technical documents.
- Also, several of your colleagues in the U.S. are from China, with some recently becoming permanent residents and others here on H1B visas.
- How do you handle? What are some measures you can take to assess and mitigate risk?

BARNES & THORNBURG LLP

FOREIGN PRODUCED ITEMS

Enforcement – Foreign-Produced Items

Seagate Technology (2023)

- Seagate is a U.S. data storage company with operational HQ in the U.S. and dozens of global locations.
- BIS imposed a $300 million civil penalty for violations related to selling hard disk drives (HDDs) to Huawei Technologies Co. Ltd. (Huawei) in violation of EAR, due to the foreign direct product (FDP) rule. BIS also required three audits of its export compliance program.
- Seagate has overseas manufacturing sites in China, Northern Ireland, Malaysia, Singapore, Thailand. These sites used third-party equipment, including testing equipment, that were subject to the Export Administration Regulations (EAR) in manufacturing HDDs.

Enforcement – Foreign-Produced Items

Seagate Technology (cont.)

- In 2020, Seagate entered into a multi-year strategic cooperation agreement to supply HDDs to Huawei. At the time of the agreement, Huawei was on BIS' Entity List, and BIS' foreign direct product (FDP) rule involving Huawei had been in effect for several months. Despite the fact other Seagate competitors had stopped selling HDDs to Huawei, Seagate continued to do so, mistakenly believing that the FDP rule did not apply.
- In 2021, Seagate received notification from a supplier of equipment that if the equipment was being used for production of items for Huawei, a BIS license would be required. Seagate continued its shipments to Huawei, and during the one-year period in question, Seagate exported approximately $1.1 billion in HDDs to Huawei.

BARNES & THORNBURG LLP

Insight: Foreign-Produced Items Subject to the EAR

Seagate assumed that its foreign-produced items were not subject to the EAR. This mistaken assumption was one of the reasons that Seagate continued to sell items to a party it knew was on the BIS Entity List.

Remember: Even foreign made items may be subject to the EAR. Foreign subs/sister companies may need to comply with the EAR even where the end items were not made in the U.S.

- Foreign items incorporating more than ***de minimis*** amount of controlled U.S. content are subject to the EAR and may require a license for export or reexport.
- Foreign items that are the ***direct product*** of certain U.S. technology or software are also subject to the EAR and may require a license for export or reexport.

BARNES & THORNBURG LLP

De Minimis Principles

Non-U.S. made items can become subject to the EAR when:

- Commodities that 'incorporate' controlled commodities or are 'bundled' w/ controlled software
- Software that is 'commingled' with controlled software
- Technology that is 'commingled' with or is drawn from controlled technology

Definition of "controlled content" is destination-specific: Ask yourself "Does the content require a license to that destination?"

BARNES & THORNBURG LLP

De Minimis Calculation

Basic formula

- **fair market value of the controlled U.S. content in the foreign-made item,**
- **divided by fair market value for the foreign-made item,**
- **then multiplied by 100.**

Example: U.S.-origin field programmable gate array valued at $600 is incorporated into German acoustic towed hydrophone array valued at $6000, will be sent to China

$$\frac{600}{6000} \times 100 = 10\%$$

Foreign Direct Product (FDP) Rule

- Distinct from *De Minimis* Rule
- A foreign-produced item can be "subject to the EAR" even if the item incorporates zero U.S.-origin content
- EAR can have jurisdiction over foreign direct products of U.S. technology or software

BARNES & THORNBURG LLP

Foreign Direct Product (FDP) Rules

There are multiple FDPRs, and BIS keeps adding new ones:

- 15 CFR 734.9(b) - National Security FDP Rule
- 15 CFR 734.9(c) - 9x515 FDP Rule
- 15 CFR 734.9(d) - “600 series” FDP Rule
- 15 CFR 734.9(e) - Entity List FDP Rule
- 15 CFR 734.9(f) - Russia/Belarus/Crimea region of Ukraine FDP Rule
- 15 CFR 734.9(g) - Russia/Belarus-Military End User FDP Rule
- 15 CFR 734.9(h) - Advanced Computing FDP Rule
- 15 CFR 734.9(i) - Supercomputer FDP Rule
- 15 CFR 734.9(j) – Iran FDP Rule
- 15 CFR 734.9(k) – Semiconductor Manufacturing Equipment FDP Rule

Foreign Direct Product (FDP) Rule

Two Key Questions for FDPRs

1) Product Scope

- What is the classification of the U.S.-origin technology/software used to produce the foreign product?
- What is the classification of the end item produced with the U.S. technology/software?

2) Country/End User/End Use Scope

- What is the country of destination?
- Who will be the end user or what will be the end use?

BARNES & THORNBURG LLP

FREIGHT FORWARDER RISKS

Enforcement – Freight Forwarder Cases

Richard Shih & Seajet Company (2024)

- Shih owns international logistics and freight forwarding company and had an existing business relationship with Chinese freight forwarder Seajet Company Limited (Seajet).
- In Sept. 2018, BIS added Seajet and its Chinese co-owner to the Entity List. In June 2021, BIS added Hisiang Logistics Company Limited to Entity List as an alias for Seajet.
- Between Sept. 2018 and May 2022, Shih's company conducted more than 1,000 shipments of items from U.S. to Seajet and Hisiang. Shih and his company knew that Seajet and Hisiang were on the Entity List.
- Federal export officers repeatedly educated Shih's company about the Entity List (in Dec. 2018, BIS officials warned against exporting items to Seajet)!
- Shih pleaded guilty to conspiring to violate ECRA (18 U.S.C. § 371, which carries a maximum sentence of up to five years in federal prison)

BARNES & THORNBURG LLP

Enforcement – Freight Forwarder Cases

USGoBuy, LLC (2021 and 2024)

- U.S. package forwarding company serving non-U.S. based customers exported riflescopes to the UAE and China
- These exports were made on behalf of a customer that USGoBuy knew was based in Iran. Exports to UAE and China alone required a license.
- Penalty in 2021 consisting of $5,000 fine, external audit of compliance program, and 3-year probationary period
- But the story doesn't end there…
  - During probationary period, USGoBuy failed to implement corrective actions
  - In 2024, BIS activated denial order, taking away UsGoBuy's export privileges for 3 years

BARNES & THORNBURG LLP

Insights: Freight Forwarders Are Liable Too

- The U.S. Department of Justice and BIS are holding freight forwarders and other logistics companies accountable for their role in export control violations.

- **Assistant Secretary for Export Enforcement Matthew S. Axelrod**:
  - "Freight forwarders play an outsized role in the export of items overseas and, accordingly, are expected to help uphold the law rather than subvert it."

- BIS released freight forwarder guidance and best practices to help logistics community with export control compliance obligations.

BARNES & THORNBURG LLP

Freight Forwarder Guidance from BIS

BIS Updates Freight Forwarder Guidance and Best Practices

- https://www.bis.gov/freight-forward-guidance

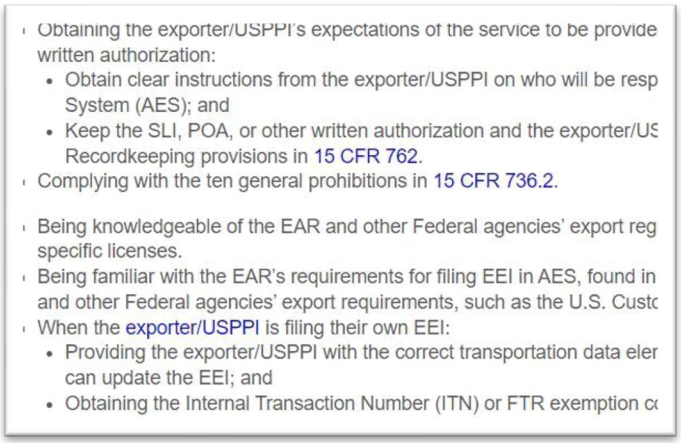
> "The freight forwarding community serves as a linchpin in the global supply chain, ensuring that the right goods get to the right place," said **Assistant Secretary for Export Enforcement Matthew S. Axelrod**. "This guidance emphasizes the importance of a risk-based compliance program to ensure that freight forwarders and exporters prevent sensitive items from going to the wrong place, including into the hands of terrorists and other malign actors."

"Forwarders must comply with EAR requirements even when their actions are dependent upon information or instructions given by those who use their services."

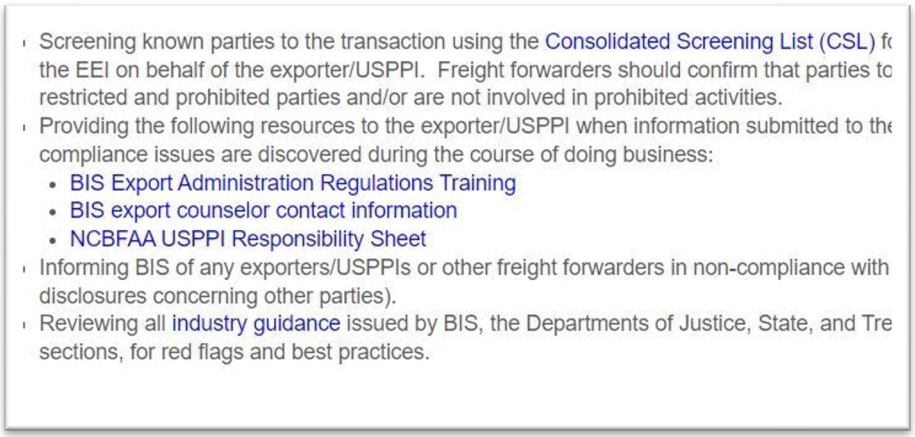
BARNES & THORNBURG LLP

Freight Forwarder Guidance from BIS

Roles and responsibilities and best practices – use as a checklist



- Obtaining the exporter/USPPI's expectations of the service to be provide written authorization:
  - Obtain clear instructions from the exporter/USPPI on who will be resp System (AES); and
  - Keep the SLI, POA, or other written authorization and the exporter/US Recordkeeping provisions in 15 CFR 762.
- Complying with the ten general prohibitions in 15 CFR 736.2.
- Being knowledgeable of the EAR and other Federal agencies' export reg specific licenses.
- Being familiar with the EAR's requirements for filing EEI in AES, found in and other Federal agencies' export requirements, such as the U.S. Custc
- When the exporter/USPPI is filing their own EEI:
  - Providing the exporter/USPPI with the correct transportation data eler can update the EEI; and
  - Obtaining the Internal Transaction Number (ITN) or FTR exemption c



- Screening known parties to the transaction using the Consolidated Screening List (CSL) fc the EEI on behalf of the exporter/USPPI. Freight forwarders should confirm that parties tc restricted and prohibited parties and/or are not involved in prohibited activities.
- Providing the following resources to the exporter/USPPI when information submitted to the compliance issues are discovered during the course of doing business:
  - BIS Export Administration Regulations Training
  - BIS export counselor contact information
  - NCBFAA USPPI Responsibility Sheet
- Informing BIS of any exporters/USPPIs or other freight forwarders in non-compliance with disclosures concerning other parties).
- Reviewing all industry guidance issued by BIS, the Departments of Justice, State, and Tre sections, for red flags and best practices.

For full list, see: https://www.bis.doc.gov/index.php/all-articles/24-compliance-a-training/export-management-a-compliance/48-freight-forwarder-guidance

BARNES & THORNBURG LLP

Freight Forwarder Guidance from BIS

Notable forwarder roles and responsibilities and best practices

- Screening known parties confirming that parties are not on any restricted/prohibited party lists or involved in prohibited activities
- Looking for red flags, including checking documents for boycott language
- When the forwarder is filing EEI:
  - note any missing information including ECCN and license authorization
  - questioning and resolving any discrepancies – look at commercial invoice, SLI/POA, EEI data
- When there is a license, ensure transaction and EEI is consistent with the license
- Being knowledgeable of the regulations and providing compliance resources to exporter when information provided to forwarder appears inconsistent with regulations
- Record retention (5 years, but note recent change in sanctions requirements to 10 years)
- Inform U.S. agency of non-compliance via voluntary self disclosure (VSD) process

BARNES & THORNBURG LLP

Thank you!

Any Questions?

Please send any follow-up questions to:

Luis.Arandia@btlaw.com

&

Clinton.Yu@btlaw.com

BARNES & THORNBURG LLP