Screening, Vetting and Monitoring Suppliers, Freight Forwarders, Customers and Other Third Parties: How to Comply with Supply chain, End-Use and End-User Requirements?

Jonathan Epstein
Partner
Holland & Knight LLP
1.202.828.1870
Jonathan.Epstein@hklaw.com

Joel Sherman
Director, Compliance and Sustainability
KEMET Electronics Corp

Tweeting about this conference?
#ACIEAR
Third Party Compliance is the New “Normal”

• What is the U.S. exporter’s responsibility with respect to third-parties?
  • End-User and End-Use restrictions
  • Risk of diversion

• What are the risks third-parties create?

• What are common and best practices with respect to third-parties
  • Can we delegate responsibility to third-parties (e.g., freight forwarder/distributor in the U.S.?)
  • Initial vetting of third-parties - CDD Rule
  • Provision of information regarding classification
  • End-user certificates
  • Contractual safeguards
  • Audit rights of third-parties
  • Ongoing monitoring of existing clients
  • Training third-parties
Risk of Non-Compliance By Distributors/Customers

ZTE, has agreed to a record-high combined civil and criminal penalty of $1.19 billion.

FOR IMMEDIATE RELEASE
Tuesday, March 7, 2017
Office of Public Affairs
202-482-1881
publicaffairs@doc.gov

Secretary of Commerce Wilbur L. Ross, Jr. today announced that China's ZTE Corporation and ZTE Kangbau Telecommunications Ltd., known collectively as ZTE, has agreed to a record-high combined civil and criminal penalty of $1.19 billion, pending approval from the courts, after illegally shipping telecommunications equipment to Iran and North Korea in violation of the Export Administration Regulations (EAR) and the Iranian Transactions and Sanctions Regulations (ITSR).

As part of the settlement, ZTE has agreed to pay a penalty of $661 million to Commerce's Bureau of Industry Security (BIS), with $500 million suspended during a seven-year probationary period to deter future violations. This civil penalty is the largest ever imposed by the BIS and, if the criminal plea is approved by a federal judge, the combined $1.19 billion in penalties from Commerce, the Department of Justice, and the Department of Treasury, would be the largest fine and forfeiture ever levied by the U.S. government in an export control case.

"We are putting the world on notice: the games are over," said Secretary Ross. "Those who flout our economic sanctions and export control laws will not go unpunished — they will suffer the harshest of consequences. Under President Trump's leadership, we will aggressively enforce strong trade policies with the dual purpose of protecting American national security and protecting American workers."

In addition to these monetary penalties, ZTE also agreed to active audit and compliance requirements designed to prevent and detect future violations and a seven-year suspended denial of export privileges, which could be quickly activated if any aspect of this deal is not met.

"The results of this investigation and the unprecedented penalty reflects ZTE's egregious scheme to evade U.S. law and systematically misled investigations," Secretary Ross said. "This penalty is an example of the extraordinary powers the Department of Commerce will use to vigorously protect the interests of the United States. I am very proud of the outstanding work of the Department's Bureau of Industry and Security, Office of Export Enforcement, and Office of Chief Counsel."

Note: the current penalty is subject to judicial approval and is in addition to the $1.21 billion penalty ZTE agreed to pay in China as part of its settlement with the U.S. Department of Justice, Department of Treasury, and Department of the Treasury.

Source: Commerce Department
Export Risk Created by Third-Party

• Customer is bad actor
  – Intends to divert to unlawful end-user, end-use
  – Is in fact itself owned or controlled by an SDN (barred end-user)

• Your direct customer doesn’t have processes in place to vet customers
  • Smaller distributors
  • Brokers/resellers

• Reseller doesn’t know or understand classification
1. Export and reexport of controlled items to listed countries
   • If ECCN – exception / license to export
   • If EAR99 – no export to embargoed countries / persons

2. Reexport and export from abroad of foreign-made items incorporating more than a *de minimis* amount of controlled U.S. content
   • Subject to the EAR if above *de minimis* (as low as 10%)

3. Reexport and export from abroad of the foreign-produced direct product of U.S. technology and software

4. Engaging in actions prohibited by a denial order

5. Export or reexport to prohibited end-uses or end-users
General Prohibitions – EAR § 736.2

6. Export or reexport to embargoed destinations
7. Support of proliferation activities
   • U.S. persons may not assist in certain proliferation activities described in Part 744 / may not export certain chemicals
8. In transit shipments and items to be unladen from vessels or aircraft
   • Need a license for transit shipments through certain countries
9. Violation of any order, terms, and conditions
   • Become part of the EAR
10. Proceeding with transactions with knowledge that a violation has occurred or is about to occur
Export Control Restrictions on Russia/Russian Entities

• BIS rules prohibiting export or reexport of goods subject to U.S. export jurisdiction can create difficult compliance issues

• Entity List Designations come in two flavors:
  • If the entity is also an SDN, then generally the export or reexport of any goods subject to U.S. export jurisdiction is prohibited
  • If the entity is also an SSI then generally the export or reexport is only limited to goods where the goods are going to a prohibited end-use (e.g., in Russian Arctic, shale, deepwater offshore oil, or gas production or exploration)

• Other item-specific military end-use, end-user restrictions and restriction on certain equipment used in oil products

• BIS has set a high bar on diligence: knowledge requires affirmative knowledge that items are not destined for such prohibited end-use
Practical Issues Created by Crimea

- U.S. Persons cannot engage in any export, import, investment, or facilitate any transactions with the Crimea Region of Ukraine.
- No person can export goods subject to U.S. export jurisdiction to Crimea.
- Crimea is not a country but a region that does not show up in routine checks.
  - “Crimea does not show up in the address line of an entity.
    - Address of party may show up as in Ukraine or Russia depending on politics.
  - Screening tools are not set up to determine whether an entity is in Crimea or not.
  - Some companies based in Crimea have moved their headquarters to Russia, but are still effectively operating out of Crimea.
Military End-Use/End-User Restrictions

• 15 C.F.R. § 744.21 – Applies to China, Russia, Venezuela
  • Cannot export 9X515 or 600 series ECCNs to these countries without a license – to any end-user/end-use
  • Cannot export items in Supp. 2 to Part 744 to China, Russia, Venezuela if you have “knowledge” item is intended for:
    • Military End-Use in China
    • Military End-Use or End-User in China

• Supp. 2 includes: Certain materials, electronics, computers, telecommunications, sensor lasers, navigation/avionics, marine and aviation items controlled under 900 series ECCNs that would otherwise not require licenses to these countries

• Military end-use means the item will be incorporated into or is intended for use in or in development, product of military items (i.e., ITAR, 600 series ECCN)

• Military end-user is broadly defined to include national policy, government intelligence, etc.
Are There Best Practices For Supply Chain Diligence?

- No one size fits all
- Different risk profile for different entities
  - Supplier v. Foreign Distributor
- Enormous differences:
  - Between sectors (financial v. commodities)
  - Between large and small companies
  - Foreign and domestic companies
Consider OECD Guidance Model for Responsible Supply Chains

1. Establish strong company compliance management system
2. Identify and assess risk in supply chain (red flags)
3. Implement a strategy to respond to risks
4. Conduct internal audit of supply chain due diligence
5. Report results (internally unless disclosure required)

Know Your Counterparty (KYC)

“But customer is not willing to disclose their end customer….”
Identifying Counterparty Risk

- Do you source materials from high risk areas?
- Do you sell material to high risk areas?
- Has your company outsourced IT services?
- Do you conduct technology marketing campaigns at your facilities?
- Do you vet returned products (potential counterfeit)
Should You Be Training Your Supply Chain Partners?

- Anecdotally we do not typically see active training of supply chain partners
  - Companies are worried about liability if they supply incomplete/incorrect information, or partner relies on out of date information
  - No time/budget for such training
- We expect to see the cost/benefit analysis shift
  - Potential costs of partner engaging in series of violations far outweighs risk
  - Training can be given with appropriate caveats/cautions
  - Training can be done cheaply by webinar/recorded and combined with other training (anticorruption)
  - No one understands your product like you do
  - Smaller entities may not have dedicated compliance staff
Provision of Information Regarding Classification

• Practice of OEM refusing to supply specific ECCN or End-Article descriptions to component manufacturers, distributors, end-users
  • Arises out of liability concerns – however …

• Some of the largest companies in the world, including Boeing, Apple, Microsoft and Cisco will provide ECCNs for all their major products on their website

• Potential implications for not providing information:
  • Component manufacture may have 600 or 515 series item manufactured overseas because they don not know the end article
  • Downstream distributor/export may misclassify
  • BIS guidance that manufacturer is best person to classify
Initial Vetting of Third-Parties – A Risk Based Approach

• The Government says this is what we should be doing and it should save money/resources, but why is it so hard?
  • Easier to administer and audit a “standard” checklist/onboarding process for each new customer
  • Requires less training, less discretion
  • Defining risk is subjective, and low-risk doesn’t mean zero-risk
    • Ex: Not screening domestic customers
• Can you create a base level system with:
  • Carve outs/white lists for known U.S. customers
  • Enhanced diligence if certain factors are triggered (e.g., one-off shipper, other red flags)
Initial Vetting - Screening

• Screening of customers has become de-facto requirement in many industries

• Third-party screening providers offer sophisticated solutions:
  • Screen against a selectable number of lists
  • Include information not found on government lists
  • Adjustable fuzzy logic
  • Record keeping functions
  • Integration into logistics/invoicing system for automatic checks

• Screening is only one element of vetting third-parties
• Your Company is negotiating an agreement to give a UAE company exclusive distribution rights to sell your civil aviation parts in the Middle East. What diligence should you conduct?
  • Screen distributor against blacklists?
  • Conduct an Internet search of information about it?
  • Use paid business intelligence reports (D&B)?
  • Have distributor provide articles of organization, good standing, and information documenting ownership?
  • Have distributor fill out and sign a Due Diligence Questionnaire?

• Your company in negotiating a supply agreement with a major U.S. publically traded aerospace manufacturer – How does your diligence change?
The Panama Papers – Identification/Verification of Beneficial Owners

• Increased U.S. interest in identification of beneficial owners for U.S. financial institutions overlaps with sanctions issues
  • Rush to finalize Customer Due Diligence Rulemaking for U.S. financial institutions
    • Final Rule issued May 11, 2016
  • Places requirement on U.S. banks and certain other financial instructions to:
    • identify and verify customers
    • identify ultimate beneficial owners – which include 25% owners and persons who may exercise control (e.g., CEO)
• Why are we talking about this here?
  • Attempt to set floor and “standards”
  • One government agencies attempt to parse “risk”
Panama Papers -- Continued

- For the first time there is real guidance on what is acceptable minimum level of diligence:
  - One can rely on a written certification from the “customer” attesting to who its beneficial owners are (absent other red flags)
    - Note this is an actual identification, not an attestation that the beneficial owner is not an SDN
  - Allows for “white listing” of certain types of entities
  - Identifies certain types of transactions as low risk such as insurance where there is no cash payout – as opposed to life insurance and other structured products
Can We Delegate Compliance to Third-Parties?

• Generally the answer is **NO!**
  - Except reasonable reliance on OEM classification of its own item

• Difference between using a broker/freight forwarder for customs/export clearance and relying on them form due diligence.
  • FYI they are likely acting as your agent and you are indemnifying them
  • They are typically relying on information you provide them regarding export classification
    • You are relying on their technical expertise in the filing process

• Freight Forwarders –BIS has penalized a number of U.S. and foreign freight forwarders for “aiding and abetting” or otherwise failing to have adequate internal measures
Contractual Provisions and End-Use Certificates

- Export (Sanctions) clauses in contractual documents
  - Becoming more sophisticated and even sometimes contentious
  - BIS expects that such clause will exist
  - Enforceability/utility of such clauses vary greatly
- End-Use Certifications – Typically a unilateral statement by third-party either on a periodic or transaction basis
  - Only “required” in limited circumstances
  - Useful tool to put third-party on notice but typically has no contractual teeth
- Neither Export Clauses nor End-Use Certifications constitute “due diligence”
- Generally we recommend against including “restrictions” on export/reexport broader than the law requires
End-Use Certificates

• Common Elements:
  • Acknowledgement that goods are/may be subject to the EAR, ITAR or other laws
  • Agreement not to divert (sell, resell, transfer, export, reexport) in breach of U.S. law
  • Agreement not to export to embargoed countries (in violation of law)
  • Agreement not to export to prohibited end-users, end-use
  • Certification requires signature

• Less Common:
  • Statement that person is not barred entity
  • Indemnity obligation
Drafting Problems with End-Use Certificates

• “We will not export or reexport Seller’s goods to Cuba, Iran, North, Korea, Sudan or Syria, or any restricted/embargoed countries as may be designated by the U.S. Government.”

• “Restricted country is not defined – does this mean Lebanon?
• Sudan no longer subject to embargo. May lawfully export to Cuba under license/license exceptions.

• “We will not export or reexport Seller’s goods to Cuba, Iran, North, Korea, Sudan or Syria, or any restricted/embargoed countries subject to sanctions as may be designated by the U.S. Government [in violation of U.S. law] [unless otherwise authorized by the U.S. Government under applicable law].”
Drafting Problems with End-Use Certificates

• “We acknowledge that U.S. law prohibits the export or reexport with individuals or companies listed on the BIS Denied Persons or Unverified List, OFAC SDN list, and State Department Debarred List.”

• Misstates U.S. law – Can export EAR items to ITAR debarred list
  • Under-inclusive – What about entity list?

• We acknowledge that U.S. law generally prohibits the export or reexport with certain designated individuals or companies including without limitation those listed on the BIS Denied Persons, Entity List or Unverified List, OFAC SDN list, and State Department Debarred List.
End-Use Certificates

• If the goal is to ensure compliance provide information:

• These Products are classified as controlled encryption under Export Control Classification Number (ECCN) 5D002 of the U.S. Commerce Control List, 15 C.F.R. Part 774, and controlled for export purposes for National Security Reasons, and are being provided to the Distributor under license exemption "ENC" (Encryption Items), pursuant to § 740.17(b)(1), which places certain limitations on the further resale or distribution of the Products.”
Export Compliance Clause

• Clause will vary depending on type of contract:
  • International distribution agreement versus P.O. terms and conditions
  • export controls may be rolled into clause covering sanctions, anti-money laundering, anti-corruption, anti-boycott

• Move toward more sophisticated and specific clauses in long term agreements. Why?
  • Generic compliance with “all applicable laws” difficult to enforce
  • Expectations of government
  • Engender compliance by third-parties
Distributor warrants and represents that it has an export control program, including procedures, training, and compliance personnel necessary to ensure compliance with [U.S. export laws] [with the representations in Sections X.X].

- As a “Query” in Due Diligence Questionnaires
- Reference to specific annex that spells out the “minimum requirements”
Export Compliance Clause: Breach

- Does/Should your export clause have “teeth”?

- “Vessel Owner shall not be obligated to comply with voyage orders from Charterer that in Owner’s reasonable judgment would breach [sanctions clause]. If the Vessel is already Trading when a sanction is applied, or Owner discovers the Trading may breach [Sanctions Clause], Charterer shall be obligated to issue alternative voyage orders within 48 hours of receipt of owner’s notification of their refusal to proceed. If Charterers do not issue such alternative voyage orders, the Owners may [discharge cargo, etc.]”

- If it has “teeth” and you don’t enforce, how will that play before the OEE?

- Specific Indemnity for Breach:

  - “Charterer further undertakes to hold Owner, upon first demand, in full and without any reservation or limit for any fines, costs (such as discharge, reloading, shifting, forwarding and any other operational cost), expenses, legal costs and defense fees, surveys, etc., that Owner may sustain as a result of breach of [Sanctions Clause]”
Ongoing Monitoring of Existing Partners/Customers

• What are U.S. companies doing?
  • Automated rescreening of clients/vendors against watch lists on daily, monthly, quarterly basis is common
  • Some companies perform new Customer Due Diligence on their key business customers/vendors on a periodic basis (annually)
  • Some companies send out new certificates on a period basis (annually)

• What would be a reasonable practice for the following entities?
  • Software company sends periodic updates to all licensed end-users of B2B software-has 500,000 licensees
  • Company sells electronic components primarily to distributors and some large manufacturers in the U.S. and Asia
Should You Audit Your Business Partners?

- Historically rarely saw audit rights associated with export, sanctions, anti-corruption compliance
- Beginning to see this more (particular on anti-corruption side)
- Thoughts about including such clause:
  - Clause should give you the right (but not the obligation) to audit their compliance function
  - If you never intend to exercise audit right, how will this look to regulators?
  - May make more sense for freight forwarder than other partners
  - Often clause is generic and the term “audit” is unclear
    - High level review of compliance program or actual spot check audit of actual transactions?
Questions?