Office of Export Enforcement
U.S. Department of Commerce

Julie L. Salcido

Special Agent in Charge, San Jose

26th Annual ECCO Training

LLNL, California

June 18, 2014

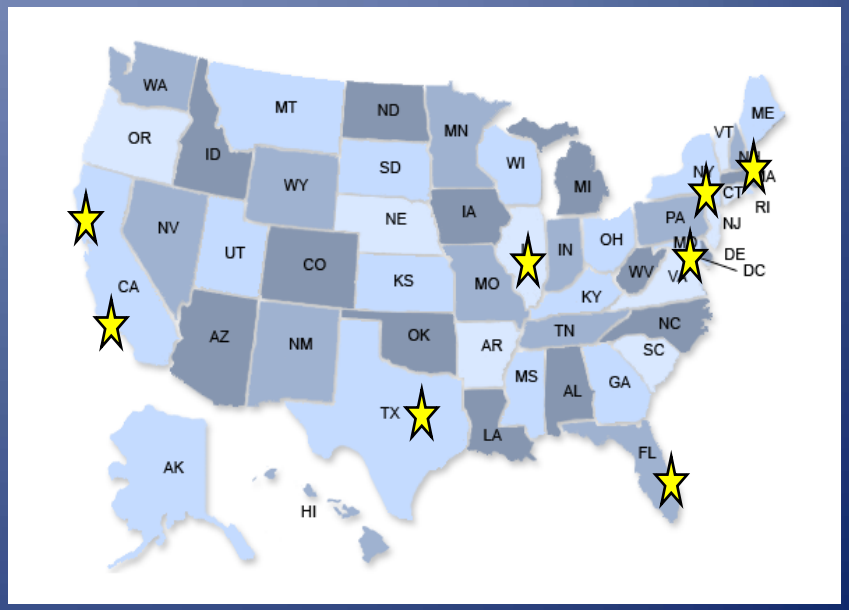
Export Enforcement Organization

Office of Export Enforcement

- Headquarters, Washington, D.C.
- 9 Domestic Field Offices
- OEE personnel are also detailed to Export Control Officer assignments in Singapore, India, China, Russia, Hong Kong, UAE

Export Enforcement

- **Office of Export Enforcement (OEE)**
- **Office of Antiboycott Compliance (OAC)**
- **Office of Enforcement Analysis (OEA)**



Export Control Officer Locations

- **Beijing, China**

- **Hong Kong, China**

- **Dubai, UAE**

- **Moscow, Russia**

- **New Delhi, India**

- **Singapore**

EXPORT CONTROLS

Based on item, destination, end-user and end-use.

- What is it?
- Where is it going?
- Who is getting it?
- What are they going to do with it?

Enforcement Priorities

End-Use/User Controls

Entities List, sensitive technology transfer and unauthorized military use; diversion of U.S. goods to embargoed destinations.

Regime Controlled Items

NS, NP, MT,CB, CW

Combating Illegal Transshipment

In 2013, OEE detained 351 suspect shipments and made 84 seizures of unauthorized exports.

Office of Export Enforcement

OEE enforces the Export Administration Regulations (EAR) and shares jurisdiction with the Federal Bureau of Investigation (FBI) and Department of Homeland Security Enforcement (DHS/HSI).

Office of Export Enforcement

OEE routinely works with various U.S. intelligence and defense agencies for threat assessment and the enforcement of U.S. Export Laws.

Enforcement Activities

Educate Exporters - Outreach

Check exporters and customers prior to a license being issued

Post Shipment checks on end-users and end-uses – Sentinel Program

Review ATS/AES - Export Declarations

Review Visa Applications

Detain suspect exports

Seize unauthorized exports

Issue Temporary Denial Orders

Prepare cases for civil or criminal prosecution

Enforcement Statistics (Criminal)

Criminal Action Data	2012	2013
Convictions (individual)	27	52
Criminal fines	$4.8 million	$2.7 million
Forfeitures	$5 million	$18 million
Imprisonment (months)	187	881

Enforcement Statistics (Administrative)

Admin Action Data	2012	2013
Cases Resolved	32	63
Total Civil Penalties	$7.3 million	$6.1 million
Total Denial Orders Issued*	14	35
Total Warning Letters Issued	231	240

*Total represents Temporary Denial Orders (initial orders, modifications and renewals), Section 11(h) Orders, and any suspended orders that were later activated.

Voluntary-Self Disclosure Statistics

In FY2012, 179 VSD cases were closed. In FY2013, 194 VSD cases were closed. In FY 2013 3.2 million dollars in civil fines were administered.

VSD Case Result	2012	2013
Warning Letters	133 (75%)	126 (65%)
No Violation/No Action	27 cases (15%)	44 (23%)
Other**	13 cases (7%)	23 (12%)
Administrative Penalty	6 cases (3%)	1 (<1%)
Criminal Penalty	0	0

**Other – referral to other agency, rolled into existing case, entered in error, etc.

Enforcement Priorities under ECR

2014 Export Review Priority Focus:

- Night Vision – Sensors – Infrared
- Unmanned Aircraft Systems and components
- Foreign Distributors receiving US exports authorized under STA.
- ITU 30 - BIS Information Triage Unit (OEA) routine consultation with DTSA regarding 30 key ECCNs to examine the bonafides of declared end-users.

Enforcement Priorities under ECR

End Use Monitoring

Inspection to Prevent Diversion

- Post Shipment Verification/Pre license Checks
- Daily AES review of STA Exports
- Review and Monitor Series 600 exports

RECENT ENFORCEMENT CASES – Computerlinks FZCO

- In April 2013, Computerlinks FZCO of Dubai, UAE entered a settlement agreement with BIS related to 3 charges of evasion of the Regulations and agreed to pay the maximum penalty, $2.8 million. This penalty amount was 2 x the total value of contract. The unprecedented maximum penalty reflects the serious nature of the violations.
- During 2010 and 2011, Computerlinks purchased US origin network monitoring equipment controlled for National Security and Anti-terrorism reasons for resale to Syria, knowing the end-user was the Syrian Telecommunications Establishment (STE) and that the deal violated US law. STE used this equipment as a tool to monitor private citizen communications to repress government opposition.

RECENT ENFORCEMENT CASES – Computerlinks FZCO

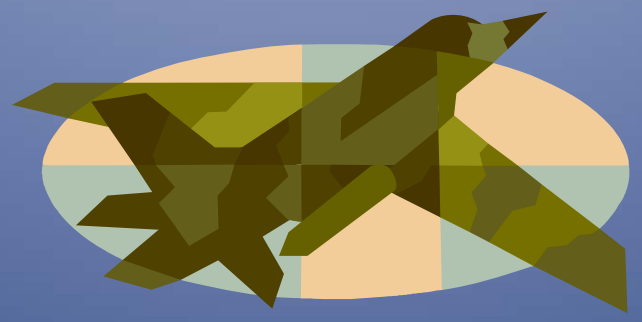
- BIS imposed the statutory maximum penalty in this case which was twice the value of the goods. This is the second highest BIS fine ever and first imposition of a statutory maximum fine based on twice the value of the goods.

- The maximum penalty was imposed because Computerlinks personnel were aware of the US embargo of Syria, knew the true end-user and lied about the destination of the equipment to US suppliers were all contributing factors to this noteworthy penalty assessment.

OEE OUTREACH
HOW DO WE DECIDE WHO TO VISIT?

- Strategic significance of the products a company makes or sells.
- Regularity of foreign visitors – visas.
- Export and licensing history.
- Information from other investigations or industry sources.
- In 2013, OEE made 1,522 outreach contacts with industry.

Best Practices to avoid diversion



August 31, 2011, BIS Published New “Best Practices” for Industry to Guard Against Unlawful Diversion through Transshipment Trade.

REAL Examples from recent cases

Red Flags seen in recent investigations

- Use of Virtual Offices – U.S. and foreign
- Source of Funds – payment received from unusual or unrelated source
- Trade inquiries show from prohibited end-users or destinations, followed by similar order from reseller in known transshipment country
- Package Forwarding Services – see FBI advisory

BIS accepts settlement related to illegal exports of NS Controlled Manufacturing Technology

- A California company released of export controlled “Lean Etch” manufacturing technology to a Russian national working at their US facility. To resolve potential charges, the company agreed to pay a fine of $115,000 in a case that highlights the importance of maintaining robust Deemed Export compliance to prevent unauthorized access to controlled US technology and data

BIS settles Freight Forwarder case related to shipments delivered to Syria via UAE

- The U.S. Department of Commerce alleged that during 2010 and 2011, Aramex Emirates, LLC, located in Dubai, U.A.E, facilitated unlicensed exports of U.S. origin network devices and software to Syria, via the U.A.E.
- The Aramex cargo team had previously been cautioned that U.S. export regulations prohibited the transfer of U.S. goods to Syria.
- In May 2014, Aramex agreed to pay a BIS civil penalty in the amount of $125,000 to resolve the charges.

VOLUNTARY SELF-DISCLOSURE – Part 764.5

- Benefits of submitting a VSD
- Great Weight Mitigation of 50%
- The majority of VSD cases result in Warning letter or no adverse action
- Costs of <u>not</u> disclosing violations
- Risk of criminal investigation and associated costs
- Damage to Brand/Corporate Reputation

How the Government Determines Appropriate Enforcement Action

Voluntary Disclosure Investigations generally consider these key factors:

What was the item or technology transferred?
How serious is the potential damage to National Security?
Where did the item or technology end up?

Would a license have been approved for that end-user/end-use?

How did the violation happen? Isolated mistake? Intentional bad act? Systemic problem? Negligence?

How was the violation discovered?

What steps did the company take to investigate and rectify?
Was the company cooperative and concerned about compliance?
How will the company prevent future violations?

Protecting U.S. Security through Prevention and Enforcement

Julie L. Salcido
Special Agent in Charge
San Jose Field Office

408-291-4211

Julie.Salcido@BIS.DOC.GOV