Facilitation and Security in the Global Trade and Logistics Supply Chain: The AEO scheme and the Mutual Recognition Agreements/Arrangements (MRAs)

Co-funded by the European Union and Thai Customs Department of Thailand

Sofitel Sukhumvit Hotel, Bangkok
31 October 2013

By Dr. Juha HINTSA, CBRA, Switzerland
• Foreword
• Session 1. The EU AEO program: purpose, criteria / requirements, process and benefits
• Session 2. The EU AEO´s current situation, including statistics on company participation and on EU member states
• Session 3. AEO-programs global situation: countries with AEO-programs; AEO benefits, projections and trends
• Session 5. Mutual Recognition Arrangements, MRAs, of the AEOs
Foreword: Why AEOs?
All illicit in global supply chains

Raw material sourcing, "from land and water": minerals, metals, oil, gas, animals, plants, timber etc.

Manufacturing: parts production, semi-finished goods, final assembly, process manufacturing etc.

Transport: maritime, air, road, rail etc.

Export and import activities

Warehousing, distribution, wholesale and retail

Reverse logistics

Multiple stages
Exploiting supply chain system to cause damage at target destinations; acts of terrorism

Wildlife crime

Reverse logistics

Multiple stages

Export and import activities

Multiple stages

Warehousing, distribution, wholesale and retail

Multiple stages

Transport: maritime, air, road, rail etc.

Raw material sourcing, "from land and water": minerals, metals, oil, gas, animals, plants, timber etc.

Manufacturing: parts production, semi-finished goods, final assembly, process manufacturing etc.

Counterfeit manufacturing, transport, distribution and sales

Violation of hazardous waste, e-waste and other waste regulations

Smuggling for fiscal fraud

Smuggling by violating restrictions and prohibitions

Exploiting supply chain system to cause damage at target destinations; acts of terrorism
## Examples of illicit goods

<table>
<thead>
<tr>
<th>Trafficking in:</th>
<th>Examples of associated commodities</th>
<th>Supply chain crime type:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterfeits</td>
<td>Apparels, electronics, spare parts, pharmaceuticals</td>
<td>Counterfeiting</td>
</tr>
<tr>
<td>Highly taxed goods</td>
<td>Alcohol, cigarettes, petroleum products</td>
<td>Duty and excise fraud</td>
</tr>
<tr>
<td>Narcotics</td>
<td>Cocaine, heroin, cannabis, synthetic drugs</td>
<td>Smuggling of prohibited goods</td>
</tr>
<tr>
<td>Pharmaceuticals</td>
<td>Counterfeit medicines, pharmaceuticals imported without appropriate licenses, stolen pharmaceuticals</td>
<td>Smuggling of prohibited / restricted goods</td>
</tr>
<tr>
<td>Polluting substances</td>
<td>Halon chemicals, hazardous waste</td>
<td>Pollution crime</td>
</tr>
<tr>
<td>Quota-restricted commodities</td>
<td>Hand bags, apparels</td>
<td>Violation of trade quotas</td>
</tr>
<tr>
<td>Stolen goods</td>
<td>Cars, art, electronics</td>
<td>Cargo crime</td>
</tr>
<tr>
<td>Weapons</td>
<td>Rocket launchers, hand guns</td>
<td>Smuggling of prohibited / restricted goods</td>
</tr>
<tr>
<td>Wildlife</td>
<td>Elephant ivory, rhino horns, illegally logged timber</td>
<td>Wildlife crime</td>
</tr>
</tbody>
</table>

## Cybercrime in supply chains

<table>
<thead>
<tr>
<th>Cybercrime objective</th>
<th>Access to confidential information</th>
<th>Control over computer systems</th>
<th>Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline activity</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cargo crime</strong></td>
<td>Logistics information: routing of shipments, content of shipments, scheduling etc. Vulnerability information: weak spots in security systems of terminals, ports and warehouses, etc.</td>
<td>Shut down or dislocation of surveillance cameras Manipulation of access control system</td>
<td>Coordination and planning within and between criminal groups Marketing transportation services via bogus websites set up for cargo crime purposes Web-sales and marketing of illegal goods</td>
</tr>
<tr>
<td><strong>Smuggling</strong></td>
<td>Vulnerability information: weak spots in anti-smuggling controls</td>
<td>Manipulation of shipment targeting results</td>
<td>Coordination and planning within and between criminal groups</td>
</tr>
<tr>
<td><strong>Counterfeiting</strong></td>
<td>Blueprints of genuine products Theft of serial numbers of products (spare parts, pharmaceuticals etc.)</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td><strong>Sabotage</strong></td>
<td>Vulnerability information: weak spots in security systems of terminals, ports and warehouses etc.</td>
<td>Malicious tampering of supply chain related computer systems such as air traffic control, rail way control system, ERP-systems of businesses</td>
<td>Intimidation and blackmailing via internet Coordination and planning within and between criminal groups</td>
</tr>
</tbody>
</table>

Taxonomy for "all illicit activities" in global supply chains

How to differentiate the good from the bad ones?

<table>
<thead>
<tr>
<th>CLIENT CATEGORIES</th>
<th>Voluntary compliance; People who want to comply</th>
<th>Assisted compliance; People who try to comply but dont always succeed</th>
<th>Directed compliance; People who will avoid complying if they can</th>
<th>Enforced compliance; People who deliberately do not comply</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLIENT BEHAVIORS</td>
<td>Voluntary compliance; Informed clients</td>
<td>Attempting to comply; Uninformed clients</td>
<td>Resistance to compliance; Will avoid if possible</td>
<td>Criminal intent; Illegal activity</td>
</tr>
</tbody>
</table>

Source: WCO Risk management guide (2011)
Key information sources – EC DG TAXUD

- AUTHORISED ECONOMIC OPERATORS. THE AEO COMPACT MODEL. WORKING DOCUMENT TAXUD/2006/1452
- Where AEO related questions can be answered in the Member States Customs authorities
- AUTHORISED ECONOMIC OPERATORS GUIDELINES – Main source!
- Threats, Risks and Possible solutions
- Self assessment questionnaire – AEO guidelines
- Explanatory notes for AEO-Self Assessment Questionnaire
- Security Declaration for Authorised Economic Operators AEO (Annex 3)
- COMMISSION REGULATION (EC) No 1875/2006 of 18 December 2006
- COMMISSION REGULATION (EU) No 197/2010 of 9 March 2010
- COMMISSION REGULATION (EC) No 1192/2008 of 17 November 2008

All available on DG TAXUD web-site
Key information sources - WCO SAFE package

- **Compendium of Authorized Economic Operator Programmes 2012 edition – Key source!**
- SAFE Framework of Standards to Secure and Facilitate Global Trade, June 2012.
- Customs Guidelines on Integrated Supply Chain Management
- AEO Implementation Guidance - How to develop an AEO programme
- Trade Recovery Guidelines
- Model AEO Appeal Procedures
- **PSCG (Private Sector Consultative Group) on AEO benefits – Key source!**
- Guidelines for the procurement and deployment of scanning/NII equipment
- SAFE Data Element Maintenance Mechanism
- The Authorized Economic Operator and the Small and Medium Enterprise - FAQ
- **Guidelines for developing a mutual recognition arrangement/agreement – Key source!**
- AEO Template

All available on WCO web-site
Cross-border Research Association, CBRA

Private and public sector perspectives on:


Compliance management: Supply chain security standards, voluntary programmes, security regulation.

Overall security management systems: risk management systems, security management models and tools, security management metrics

Note: ANNEX 1 announces our plans for a new AEO-MRA survey!
The EU AEO program: purpose, criteria / requirements, process and benefits
Three types of AEO in the EU

• Customs simplifications (AEOC)
• Security and safety (AEOS)
• Full (AEOF) [amalgamating AEOC and AEOS]
EU AEO four main requirement areas

• Record of Compliance (applicable to AEOF/C)
• Satisfactory system of managing commercial and transport records (applicable to AEOF/C)
• Proven financial solvency (applicable to AEOF/C)
• Appropriate security and safety standards (applicable only to AEOS/F)
Application process steps with EU AEO

1. A thorough communication and consultation process is undertaken via the AEO Database;
2. A detailed security profile of the applicant is constructed;
3. Compliance/solvency requirements are checked;
4. A risk assessment is undertaken;
5. The applicant performs a security self-evaluation;
6. If there are security issues arising from the risk assessment and the self-evaluation dialogue is held suggesting appropriate course of action to reduce, mitigate or remove the risks which represent a problem
7. If these actions are implemented and an audit satisfies the customs authority of compliance, the AEO status is granted
EU AEO and "control of business"

1. Providing a visible audit trail
2. Having strategies and measures to identify and mitigate risks
3. Having a system and procedures for ensuring compliance management with the rules of trade, cargo handling and transport
4. Having delegated responsibility for security training and awareness
5. Having a system and procedures for monitoring, reviewing, reporting and acting upon security issues
Supply chain actors

Companies involved in global supply chains

A. Companies who own the cargo, and typically make their profits from the physical products, as price mark-ups etc. A.k.a. "Cargo owners"

Example A1. Manufacturers
Example A2. Distributors
Example A3. Retailers
Example A4. Importers/exporters

B. Companies who do not own physical products, but focus on moving and storing goods, and related administrative services etc. A.k.a. "Logistics sector"

Example B1. Physical transport orientation
Example B2. Physical warehouse orientation
Example B3. Logistics administration orientation, including customs brokers
EU AEO –
Types of actors included

- Manufacturers
- Exporters
- Freight forwarders
- Warehouse keepers and other storage facility operators
- Customs agents
- Carriers
- Importers
- Others, for example, terminal operators, stevedores and cargo packers.
EU AEO - Security requirements

- Building security
- Appropriate access controls
- Cargo security
- Handling export/import licenses (as appropriate)
- Business partner security
- Personnel security
- Security awareness programmes
**CBRA 8-layer Supply chain security model**

<table>
<thead>
<tr>
<th>1. RISK MANAGEMENT LAYER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. DESIGN AND PLANNING LAYER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply chain design</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. PROCESS CONTROL LAYER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sourcing / making / transport / distribution processes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. SUPPLY CHAIN ASSETS – SECURITY MANAGEMENT – LAYER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilities</td>
</tr>
<tr>
<td>Secure design</td>
</tr>
<tr>
<td>Monitoring</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5. HUMAN RESOURCES MANAGEMENT LAYER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiring</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>6. BUSINESS PARTNER MANAGEMENT LAYER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screening</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. AFTERMATH CAPABILITIES LAYER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business continuity</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8. DISRUPTING CRIMINAL / ILLICIT SUPPLY CHAINS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disrupt sourcing / making / transport / distribution</td>
</tr>
</tbody>
</table>

*Note: ANNEX 2 contains an additional CBRA model on security measure performance levels*
EU AEO and Small and medium sized enterprises, SMEs – some "relaxed requirements"

- Building security
- Appropriate access control
- Cargo security
- Security awareness program

"Even if the AEO criteria apply to all businesses regardless of their size, article 14a (2) of the CCIP lays down the legal obligation that the customs authorities shall take due account of the specific characteristics of economic operators, in particular of small and medium-sized companies".
EU AEO and certificates/authorisations granted by customs and other governmental authorities

- Existing customs authorisations
- Certificates granted by aviation agencies or authorities
- International Ship and Port Facility (ISPS)
- Eligibility of the European Central Bank Eurosystem credit assessment framework (ECAF)
- The Sarbanes-Oxley-Act (SOX)
- AEO or similar programmes in third countries
- Transports Internationaux Routiers (TIR)
- Others: Verifiable compliance with security requirements and standards set by intergovernmental organisations, such as IMO, UNECE, OTIF, UPU and ICAO
EU AEO and commercial standards and certifications

- Certificates according to ISO 27001
- ISO 9001:2008 (quality)
- ISO 28000: 2007 (supply chain security)
- TAPA Certificates (Transported Assets Protection Association)
EORI-number in the EU

• Every economic operator in or outside the EU which is involved in international trade to or from the EU, lodging customs declarations, Entry or Exit Summary Declarations, must have an Economic Operator Registration and Identification (EORI) number.

• This comprises a 2-digit country identifier (e.g. GB123456789000), a reference based on the company's existing VAT number (e.g. GB123456789000) and a 3-digit suffix (e.g. GB123456789000).
EU AEO Direct benefits

- Easier admittance to customs simplifications
- Prior notification
- Reduced data set for entry and exit summary declarations
- Fewer physical and document-based controls
- Priority treatment of consignments if selected for control
- Choice of the place of controls
Examples of possible indirect EU AEO benefits

- reduced theft and losses;
- fewer delayed shipments;
- improved planning;
- improved customer service;
- improved customer loyalty;
- improved inventory management
- improved employee commitment;
- reduced security and safety incidents;
- lower inspection costs of suppliers and increased co-operation;
- reduced crime and vandalism;
- improved security and communication between supply chain partners.
Other possible EU AEO benefits

- Recognised as a secure and safe business partner
- Improved relations with Customs
- Improved relations and acknowledgement by other government authorities
# Two multinational company AEO case studies - functions & actors

<table>
<thead>
<tr>
<th>Internal vs. external</th>
<th>Examples with the two CBRA case studies</th>
</tr>
</thead>
</table>
| **Internal functions** | • Security function  
                          • Environment, health, safety (EHS) and quality functions  
                          • Trade compliance management  
                          • Logistics department  
                          • Manufacturing function  
                          • Supplier management function  
                          • Human resources department  
                          • Information systems and data management function  
                          • Legal affairs  
                          • Corporate social responsibility unit |
| **External actors** | • Supply network  
                          • Freight forwarders  
                          • Transport carriers  
                          • Port and airport operators  
                          • Warehouse keepers  
                          • Customs brokers |
Two multinational company AEO case studies – pre-existing documentation

<table>
<thead>
<tr>
<th>Case company A: Policy, guideline, instruction document</th>
<th>Pp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss Prevention in Warehouse</td>
<td>62</td>
</tr>
<tr>
<td>Loss Prevention in Transportation</td>
<td>58</td>
</tr>
<tr>
<td>Confronting contraband</td>
<td>17</td>
</tr>
<tr>
<td>Corporate Code of conduct</td>
<td>46</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Case company B: Policy, guideline, instruction document</th>
<th>Pp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Commitment Service Provider</td>
<td>8</td>
</tr>
<tr>
<td>Security Commitment Supplier</td>
<td>6</td>
</tr>
<tr>
<td>Code of Conduct</td>
<td>4</td>
</tr>
<tr>
<td>Routine for Cargo Handling</td>
<td>4</td>
</tr>
<tr>
<td>Security Rules and Tips Employees</td>
<td>15</td>
</tr>
<tr>
<td>Incident Report</td>
<td>2</td>
</tr>
<tr>
<td>Specification for Construction of Warehouse</td>
<td>17</td>
</tr>
<tr>
<td>Security regulations for external work</td>
<td>1</td>
</tr>
<tr>
<td>Interview guideline</td>
<td>1</td>
</tr>
<tr>
<td>Transit Contingency Plan</td>
<td>10</td>
</tr>
<tr>
<td>Security Policy</td>
<td>1</td>
</tr>
<tr>
<td>Duty of confidentiality</td>
<td>29</td>
</tr>
</tbody>
</table>
Two multinational company
AEO case studies – Top and bottom 5 requirements

<table>
<thead>
<tr>
<th>Top 5 and Bottom 5</th>
<th>Case company A</th>
<th>Case company B</th>
</tr>
</thead>
</table>
| The top 5 EU AEO questions covered by the guidelines | 1. Security requirements imposed on others
2. Routines for checking incoming transport
3. Sealing of outgoing goods
4. Active means of transport
5. Routines for checking outgoing transport | 1. External boundaries of premises
2. Routines for access or entry of vehicles, persons and goods
3. Standard operating procedures in case of intrusion
4. Uniform marking of goods
5. Routines for checking outgoing transport |
| The 5 least covered EU AEO questions | 1. Certification for safety and security purposes by others
2. Parking of private vehicles
3. Routines for verifying security measures imposed on others
4. Procedures for access to keys
5. Maintenance external boundaries and buildings | 1. Routines for verifying security measures imposed by others
2. External control procedures
3. Additional safety and security measures for access to goods
4. Threat assessment by others
5. Security requirements imposed by others |
“….Companies with AEO accreditation should expect positive outcomes as uncertainty of unplanned supply chain delays is reduced and therefore inventories and safety margins could be lowered. In all, this should lead to better customer service through improved and more predictable supply chain planning…”