C-TPAT
5 Step Risk Assessment Process Guide

C-TPAT Training Seminar
March 2010

Table of Contents

Attachments

5 Step Risk Assessment Process
Introduction

In order to assist C-TPAT Partners with conducting a risk assessment of their international supply chain(s) in accordance with C-TPAT minimum security criteria, the 5 Step Risk Assessment Process is recommended.

This reference guide contains some of the basic tools, resources, and examples C-TPAT partners should consider using when conducting a risk assessment on their international supply chain(s). The information contained herein is intended to serve as a guide, and is not "all inclusive" of what should be included in an international supply chain security risk assessment.

The 5 Step Risk Assessment Process includes:

1. Mapping Cargo Flow and Identifying Business Partners (directly or indirectly contracted)
2. Conducting a Threat Assessment focusing on: Terrorism, Contraband Smuggling, Human Smuggling, Organized Crime, and conditions in a country/region which may foster such threats and rate threat – High, Medium, Low
3. Conducting a Vulnerability Assessment in accordance with C-TPAT Minimum Security Criteria and rate vulnerability – High, Medium, Low
4. Preparing an Action Plan
5. Documenting How Risk Assessments are Conducted

It is understood that some C-TPAT members may have numerous supply chains which may present a monumental task when conducting a comprehensive security risk assessment of their international supply chains. Therefore, it is recommended for C-TPAT members to identify their "High Risk" supply chains by conducting a threat assessment at the point of origin/region and where the cargo is routed/transshipped, and then conduct a comprehensive security vulnerability assessment of those supply chains. Conversely, if supply chains involve a limited number of business partners or related business partners, their supply chain security risk assessment may not require such extensive efforts.

Risk Assessment Process
Definition of Terms

The definition of terms below is intended as a guide when examining the roles of parties involved in the international supply chain.

Instruments of International Traffic (IIT): Containers, trailers, flatbeds, unit load devices (ULDs), lift vans, cargo vans, shipping tanks, bins, skids, pallets, caul boards, cores for textile fabrics, or other specialized containers arriving (loaded or empty) in use or to be used in the shipment of merchandise in international trade.

International Supply Chain Security: Encompasses securing all of the following processes from the cargo's point of origin (factory/farm) until its arrival and distribution in the United States: Procurement, Production, Packing, Staging/Storing, Loading/Unloading, Transportation, and Document Preparation.

International Supply Chain Security Risk Assessment: Process of identifying the security threats, vulnerabilities, and weaknesses throughout the international supply chain and prescribing corrective actions with follow-up procedures to ensure weaknesses have been mitigated.

Loading/Unloading: Placing cargo in/on or taking cargo out/off of an IIT, including containers, trailers, vessels, planes etc.

Mapping Cargo Flow/Parties Involved: Method of identifying all parties involved and their prospective roles in the following processes throughout the international supply chain: Procurement, Production, Packing, Staging/Storing, Loading/Unloading, and Document Preparation of cargo destined for the United States. All partners involved both directly and indirectly in exportation/movement of the goods from the point of origin to the importer's distribution center must be included. Some examples of parties involved in the international flow of cargo include, but are not limited to, the following:

- factories
- farms
- suppliers
- export packing facilities
- buying/selling agents
- trading companies
- freight forwarders
- non-vessel operated common carriers (NVOCCs)
- inland truck/rail carriers
- warehouse/consolidation/deconsolidation facilities
- feeder vessels
- rail depots
- trailer/container yards
- shipyards

- local drayage companies
- international air/rail/sea/truck carriers
- Customs brokers.

Packing: Encompasses both packing the goods for export into non-reusable containers and reusable instruments of international traffic (IIT). It includes but is not limited to placing goods in/on pallets, cartons, cardboard boxes, crates, bins, or other specialized containers. It also entails bundling, wrapping, shrink-wrapping, and other types of packaging.

Procurement: Ordering products or services from business partners in the international supply chain. Raw materials that go into making the exported products are excluded from this process. These products only pertain to finished cargo/raw material that will be exported to the United States. Services include indirect procurement methods for goods shipped to the United States such as buying agents and trading companies.

Production: Making, growing/harvesting, or assembling products to be exported to the United States.

Risk Rating: Assigning numerical values to threats and vulnerabilities identified during a supply chain security risk assessment (e.g. 1-Low, 2-Medium, and 3-High).

Staging/Storing: Placing products and/or IITs at a location of "rest" prior to or during movement to the United States. This includes any warehousing/consolidation/deconsolidation of goods and/or facilities where goods wait to be loaded onto another transit mode such as a rail depot or shipyard in the country of origin or other countries the goods may transit through on the way to the United States.

Supply Chain Security Action Plan: Identifies security weaknesses and vulnerabilities found during the risk assessment process for a business partner. The plan assigns responsibility for corrective actions/mitigation strategies (internal and external), establishes deadlines/timeframes, documents evidence of actions taken, outlines processes used to verify actions have been taken, and delineates the final outcome.

Transportation: Movement of cargo throughout the international supply chain. Transporting the goods for export to the United States includes any domestic legs of the goods' journey in the country of origin to the Port of Export, from the Port of Export to any countries that the goods may transit through, to the US Port of Entry, and to the US domestic distribution center.

Security Risk Rating

Each C-TPAT partner is responsible for establishing its own overall Security Risk Rating System based on its business model. It is understood that businesses use various methodologies for rating risk within their international supply chains. However, the following "Risk Ratings" are recommended when examining security threats and vulnerabilities within the international supply chain.

Threat Assessment

There are many "Open Sources" which provide information on threats within the international supply chain. After conducting research, it is recommended to assign a threat risk rating based on the following.

1 - Low Risk - No recent incidents/intelligence/information
2 - Medium Risk – No recent incidents/some intelligence/information on possible activity
3 - High Risk – Recent incidents and intelligence/information

A Score of 3 in any of the following areas would deem the supply chain "High Risk"

1) Terrorism
2) Contraband Smuggling
3) Human Smuggling
4) Organized Crime

Vulnerability Assessment

One method that may be used to conduct a vulnerability assessment is sending security surveys to Business Partners who are not eligible or do not participate in the C-TPAT program. Security surveys should be based on the process performed by the business partner in the international supply chain (e.g. Procurement, Production, Packing, Storage, Loading/Unloading, Transportation, and Document Preparation). Questions should ask the business partner to describe security measures used, and not only be "Yes/No" questions. The survey should address whether or not a system of checks, balances, and accountability are in place, particularly in areas of Securing Instruments of International Traffic, Tracking and Monitoring Cargo, Seal Security, and Business Partner Screening (sub-contracted).

The following is a recommended risk rating of vulnerabilities for C-TPAT minimum-security criteria categories: Business Partner Requirements, Securing Instruments of International Traffic, Procedural Security, Physical Security, Physical Access Controls, Personnel Security, Security and Threat Awareness Training, and Information Technology Security.

1 - Low Risk - Meets all applicable Minimum Security Criteria (Musts and Shoulds)
2 - Medium Risk - Meets all applicable "Musts" Minimum Security Criteria, but does not meet all "Shoulds"
3 - High Risk – Does not meet all "Must" Minimum Security Criteria

For example,

1) If all "Musts" for Procedural Security were met, the risk rating for that category would be "1-Low risk."
2) If all "Musts" were met for Procedural Security and "Shoulds" were not met, the rating would be "2-Medium Risk."
3) If one "Must" is not met for Procedural Security, then it would be rated a "3-High Risk," because a supply chain security measure is only as strong as its weakest link.

Post Incident Analysis and Risk Rating

Based on a study conducted by the C-TPAT Program in June 2009 on factors which contributed to Security Breaches, the following data should be taken into consideration when conducting a Security Vulnerability Assessment.

34% Conveyance Security: Conveyances not inspected
35% Business Partner Requirements: Failure to Screen Business Partners
41% Instruments of International Traffic (containers, trailers, pallets, etc. not secured/properly inspected prior to loading
44% Seal Controls: Lack of Seal Procedures
53% Transportation Monitoring: Inadequate Transportation Monitoring
68% Security Procedures not followed (lack of checks, balances, accountability)

90% - Involved "trucks" as the mode of transportation for breached cargo

5 Step Risk Assessment Process

Step	Process	Description	Methods	Resources
1	Map Cargo Flow and Business Partners	Identify ALL parties involved in the following processes: 1) Procurement 2) Production 3) Packing 4) Storage 5) Loading/Unloading 6) Transportation 7) Document Preparation	1) Request information from supply chain partners 2) Review documentation (BOLs, manifests, invoices, etc.) to determine routing 3) On site visits/audits of the supply chain	See Attachment A: Example of Mapping Cargo Flow, Identifying Business Partners, and Processes
2	Conduct Threat Assessment	Identify and rate the risk of threat (High, Medium, Low) for the country and region for each international supply chain, using the following (at a minimum): 1) Terrorism (political, bio, agro, cyber) 2) Contraband Smuggling 3) Human Smuggling 4) Organized Crime 5) Conditions fostering above threats	1) Open source internet information (government and private organizations) 2) Representative/Contacts "on the ground" at origin 3) Law enforcement (foreign/domestic), local state, federal/national 4) Trade and security organizations 5) Assigned C-TPAT SCSS	See Attachments B: Threat Assessment Resource List Attachment C: Threat Assessment Example
3	Conduct Vulnerability Assessment	For all business partners in the international supply chain (directly contracted or sub-contracted): 1) Identify the process they perform 2) Verify partners meet applicable minimum security criteria 3) Rate their compliance within each applicable minimum-security criteria category (High, Medium, Low)	1) SVI Number/C-TPAT Membership 2) Membership in "Mutual Recognition Program" 3) Security Surveys 4) Site visits by company representative 5) Site visits by overseas personnel/agents 6) Business reports 7) Security certifications covering C-TPAT minimum-security criteria 8) 3rd party supply chain security assessments	See Attachment D: Vulnerability Assessment Using C-TPAT Minimum-Security Criteria
4	Prepare Action Plan	Establish a corrective action plan to address gaps or vulnerabilities found in business partner's security programs.	1) Word Document 2) Excel Spreadsheet 3) Project Management Software	See Attachment E: Action Plan and Follow-Up
5	Document How Risk Assessments are Conducted	A description of the company's approach, policies, and procedures for conducting an international supply chain security risk assessment.	1) Document company's Policy for conducting International Supply Chain Security Risk Assessment 2) Document Procedures used to conduct International Supply Chain Security Risk Assessments	See Attachment F – Documenting Risk Assessment Process, Policies, and Procedures

Attachment A - Example of Cargo Flow and Partners - Ocean Cargo - LCL

Step 1 - Sample - Map Cargo Flow, Identify Partners, and Processes

Notes: Ensure partners map out all variations of a supply chain - For example, FCL vs. LCL; From one factory to various ports of export; From one factory using different modes of transportation (Air vs. Sea); Any other potential variations that would alter the movement of cargo or the individuals involved in the process. Always remember - **"Freight at Rest is Freight at Risk".**

Sub-contracting increases risk within a supply chain, particularly where security requirements have not been conveyed or verified.

Partner	Process	Cargo Movement - if applicable	Known Details About Provider	Days Cargo is "At Rest" at this stage	Transport Mode	If entity physically handles cargo, who selects them as a provider?
XYZ Manufacturer	Production, Packing, Document Preparation	Point of Departure	Location: City 123, Country Origin; Years doing business with - 22; Family Owned and Operated	0	N/A	
Export Broker/FF	Prepares Documentation for Export	N/A	Unknown	NA	N/A	
Foreign Inland Carrier ABC	Inland Transporation	Picks up cargo from factory and Consolidator EFG	Location: City 123, Country Origin; Contracted by factory - in Business 22 years; Parent Company C-TPAT in USA	0	Truck	
Consolidator LMNOP	Unloading, Storage, Loading	Unloads cargo from inland truck carrier, stores LCL, loads with other customers' cargo	Location City 123, Country Origin; Contracted by factory - in business 2 years	2	N/A	
Inland Carrier JKL	Inland Transporation	Picks up cargo from consolidator and transports to Port of Export	Location: City 123, Country Origin; Contracted by factory; in business 22 years; Parent Company C-TPAT in USA	0	Truck	
Port Terminal - Origin	Storage	Receives and stores container in container yard until ready to go on vessel	Location: City 456, Country Origin; operated by government body; MTSA/ISPS Compliant	4	N/A	
Sea Carrier	Transportation	Transports cargo from port of lading	Location: City 456; Country Origin; Parent Company C-TPAT in USA	3	Vessel	
Port Terminal - Transit Country	Storage	Receives offloaded container at country of transshipment	Location: City 183, Transit Country; unknown; Unknown MTSA/ISPS Compliant	**10**	**N/A**	
Sea Carrier	Transportation	Transports cargo from country of transshipment	Location: City, New Country; unknown	10	Vessel	
Port Terminal - USA	Storage	Unloads cargo from Sea Carrier's vessel and stores until domestic transport picks up	Location: City 42, USA ; MTSA/ISPS Compliant	2	N/A	
Domestic Drayage Carrier Picks up	Transportation	Picks up cargo from terminal	Unknown	0	Truck	
Consolidator/ Deconsolidator	Unloading, Storage, Loading	Receives LCL Cargo, consolidates, ships to destination	Location: City 42, USA - Cross dock facility	1	N/A	
Long Haul Carrier	Transportation	Transports cargo to distribution center	Location: City, USA - Unknown	0	Truck	
U.S. Distribution Center/Consignee	Unloading	Receives cargo	Location: City 53, USA	2	N/A	

Attachment B

RISK ASSESSMENT RESOURCE LIST*

Customs & Border Protection: www.cbp.gov

CIA – The World Fact Book: https://www.cia.gov/library/publications/the-world-factbook/

Information Technology Security: http://www.us-cert.gov/nav//nt01/

Federal Trade Commission – Identity Theft/Data Breach: http://www.ftc.gov/bcp/edu/microsites/idtheft/

Licensed Freight Forwarders/NVOCC/OTI/Terminal Operators: http://www.fmc.gov/

U.S. Department of State - Terrorist Threats/Country Information: http://travel.state.gov/travel/cis_pa_tw/pa/pa_1161.html

Federal Motor Carrier Safety Administration – Check Carriers: http://www.fmcsa.dot.gov/safety-security/safety-security.htm

Manufacturer Seal Requirements – U.S./Mexico FAST: http://www.customs.gov/xp/cgov/trade/cargo_security/ctpat/fast/us_mexico/mexico_manuf/manuf_seal_requirements.xml

Global Security Newswire is now available: http://gsn.nti.org/gsn/

7 Signs of Terrorism: http://www.homelandresponder.org/pages/7signs.html

State Dept. Overseas Security Advisory Council: www.osac.gov

National Cargo Security Association: www.tncsa.org

FBI Infrastructure Security: www.infragard.net

International Chamber of Commerce: www.icc-ccs.org

Cargo Security Alliance: www.securecargo.org

U.S. Department of Commerce: www.commerce.gov

International Maritime Organization: www.imo.org

Department of Transportation: www.phmsa.dot.gov

ASIS International: www.asisonline.org

World Bank: Web.worldbank.org

Transported Asset Protection Association: www.tapaonline.org

Business Alliance for Secure Commerce: www.wbasco.org

Department of Homeland Security Crisis Management Planning: www.ready.gov

Information Systems Audit and Control Association: www.isaca.org

Department of Homeland Security: www.dhs.gov

International Container Owners Association: www.containerownersassociation.org

U.S. Postal Service: www.usps.com/communications/news/security/mailcenter

Supply Chain Information Sharing and Analysis:
https://secure.sc-investigate.net/SC-ISAC/

Note: C-TPAT partners should also consult with local law enforcement when conducting threat assessments. In addition, there are many private for profit organizations who offer security risk assessment services.

This list is not all inclusive and is not meant to be an endorsement of any organization or service.

Attachment C

Step 2: Sample Threat Assessment

1 - Low Risk - No recent activity/intelligence/information
2 - Medium Risk – No recent incidents/some intelligence/information on possible activity
3 - High Risk – Recent incidents and intelligence/information
Note: For C-TPAT Purposes a "3" for any of the Threat Risk Factors below would result in a "High Risk" rating for the supply chain

Partner: Factory-Supplier ABC

Location: Country X, Y, Z

Region: Region J-K

Threat Risk Factor	Risk Rating: 1-Low - - NA/No 2-Medium 3-High – Incidents/Information	Activity	Source
Terrorism (Political, Bio, Agro, Cyber)	3	2009, 2010 - Recent domestic bombings and violence against U.S. based interests	Name of news publication, government site, open source information, intel service, etc.
Contraband Smuggling	3	2005-Present - location known for narcotics exports and weapons smuggling	Name of news publication, government site, open source information, intel service, etc.
Human Smuggling	1	2000-2005 - numerous incidents of human smuggling; none since 2005	Name of news publication, government site, open source information, intel service, etc.
Organized Crime	1	1998-2003 - Drug cartels operating throughout country/ region	Name of news publication, government site, open source information, intel service, etc.
Conditions within a country which may foster any of the aforementioned threats (e.g. poverty, social unrest, political instability).	2	Demographics - 35% population lives in poverty; a few social movements underway with anti-western sentiments	Name of news publication, government site, open source information, intel service, etc.
Other: Theft, Pilferage, Hijacking, Piracy, IPR, Piracy	2	2007 – Incidents of piracy along shipping route; none reported since late 2007	Name of news publication, government site, open source information, intel service, etc.

Overall Threat Risk Rating = 3

Vulnerability Assessment
Attachment D

Partner Name:	**Supply Chain Process: Transportation**	
Security Point Of Contact:	**Phone Number:**	**E-mail Address:**
Country Location:	**Region:**	**Instruments of International Traffic Used:**

Sample Risk Ratings: 1 - Low Meets/Exceeds all Minimum Security Criteria (MSC - Musts and Shoulds) 2-Medium Meets "Musts" not all "Shoulds" 3 - Does not meet all "Musts" criteria N/A - Not applicable. Note: If a "Must" criterion is not met in a category, the score for the entire category should be "3".

Processes/Roles Performed (including responsibility for sub-contracting) - Note: 1 business partner may perform multiple roles: For example, the factory may not only produce, but they may pack, load, and transport cargo. The key is to ensure that each process is secured in the supply chain.

Effective Security System = Meeting all MSC + Oversight + Accountability + Checks and Balances

Supply Chain Process	C-TPAT Security Criteria - Determine as applicable to process	C-TPAT Sub-Criteria (Note-Some applicable sub-criteria may not be listed - must be tailored for each supply chain)	M- Must S- Should	Method to Verify Adherence	Vulnerabilities Identified	Sub-Category Risk Rating	Category Risk Rating	Best Practices Identified
Transportation/Movement - (Note: 85%+ Cargo disruption occurs in transit)	**Business Partner Requirements - Sub Contracting**	Screens sub-contracted source	M	Does not verify references. Contracts with lowest bidder	Unknown business partner/security procedures	3	**3**	

Transportation/Movement -cont'd		C-TPAT Certified (if eligible)	M	Does not verify	Failure to adhere to C-TPAT MSC	3		
		Verifies adherence to C-TPAT Criteria (if not eligible)	M	Does not verify	Failure to adhere to C-TPAT MSC	3		
		Participate in security program administered by foreign customs administration	S	Does not verify	Failure to adhere to C-TPAT MSC	3		
		Sub-contracting requirements	M	Does not have any	No leverage to enforce C-TPAT MSC	3		
	Securing Instruments of International Traffic	Transportation Monitoring	M	Visit	Does not actively monitor GPS to know where drivers are at all times; sub-contractor procedures unknown	3	**3**	
		Seal Inspections in transit	M	Reviewed Drivers' Logs	None	1		
		Container inspections in transit	M	Reviewed drivers' Inspection Sheets post trip	None	1		
		Written procedures stipulating how seals are controlled and affixed - meeting all C-TPAT requirements	M	Reviewed written procedures submitted and found in compliance with C-TPAT	None	1		

	Procedural Security	Procedures to report anomalies to law enforcement	M	Reviewed written procedures	None	1		
		Ensure accurate, complete, legible information	M	Documented Procedures reviewed and verified	None	1	**1**	
		Documents/Information protected against exchange, loss, erroneous information	M	Documented Procedures reviewed and verified	None	1		
		Process to resolve overages, shortages	M	Documented Procedures reviewed and verified	None	1		
		Procedures to ensure information is reported accurately and timely	M	Documented Procedures reviewed and verified	None	1		
	Physical Security (as applicable)	External Fences / Barriers	S	Site Visit	None	1	2	
		Internal Fences / Barriers	S	N/A	N/A	N/A		
		Gates/Gate Houses	M	Site Visit	None	1		

		Parking	S	Site Visit	None	1		
		Building Construction	M	Site Visit	None	1		
		Locking Devices	M	Site Visit	None	1		
		Lighting	M	Site Visit	None	1		
		Video Surveillance	S	N/A	N/A	N/A		
		Alarm Systems	S	Site Visit	No alarm system - Intrusion may go undetected despite guard on duty	3		
	Physical Access Controls	Restricted Access to conveyance and container during transit						
		Employee Access Controls						

		Visitor Access Controls						
		Vendor / Contractor Access Controls						
		Delivery Access Controls						
		Challenging and Removing Unauthorized Persons						
		Access Device Control (Badges, Keys, etc.) issuance / removal by management and must be documented						
		Access Termination Procedures						
		Compliant with MTSA / ISPS						
	Personnel Security	Screen prospective employees who transport cargo						

Security and Threat Awareness Training	Aware of the procedures to address a situation and report it							
	Specialized training seal controls, container, and conveyance inspections							
	Dispatcher tracking / monitoring							
	Threat Awareness Training							
Information Technology (As applicable)	Restricted access to automated transportation monitoring systems (GPS); Password Changes, etc.							
Oversight	System to Audit / Test all security measures related to transportation process							

Attachment E

Step 4 - Sample Risk Assessment - Action Plan and Follow-Up

Supply Chain Partner Name: Factory XYZ

Site/Location:

Point Of Contact Name: **Phone Number:** **E-Mail**

Supply Chain Process	C-TPAT Criteria	Vulnerability Identified	Corrective Action(s) Required/Mitigation Strategy	Responsible Company POC	Responsible Partner POC	Progress Review Date	Corrective Action Deadline	Evidence Action Taken	Verified By and Date	Outcome
Procurement										
Production										
Packing										
Loading/Unloading/ Stuffing/Sealing										
Storage/Staging - Product, Conveyance, Container, Shipping Instruments (Pallets, Boxes, Bags, etc.)										
Transportation										
Document Preparation										

Attachment F

Step 5
Documenting
Risk Assessment Process
(Policy & Procedures)

A company's documented risk assessment process (e.g. policies and procedures) should contain at minimum the following information:

1) Date Risk Assessment Process established

2) Identify parties responsible for keeping the process up-to-date, including "back-up" persons

3) When risk assessments must be conducted (e.g. new supplier or service provider overseas)

4) How often risk assessments must be conducted (e.g. as circumstances dictate or at a minimum annually for most C-TPAT partners (quarterly basis– highway carriers)

5) Required frequency of review/updates to process/policies/procedures (e.g. annually, bi-annually, as needed, etc. to the risk assessment policy/procedure)

6) How Threat Assessments of the International Supply Chain are to be conducted (e.g. sources used to determine threat – see examples on Threat Assessment Resource sheet provided)

7) How Vulnerability Assessments on the International Supply Chain are to be conducted (e.g. send surveys, site visits, C-TPAT Status, participation in a foreign supply chain security program)

8) How follow-up is conducted on "action items" (e.g. site visits may be required in some cases, in others documentation/photographs may be submitted)

9) Process for training key individuals who are responsible for the processes

10) Management oversight and accountability for ensuring the process is carried out consistently and effectively