Security Policies and Procedures

April 26, 2012

Kristen Whelan
Transportation Consultant
kwhelan@libertyint.com
www.libertyint.com

Customs-Trade Partnership Against Terrorism

What is C-TPAT?

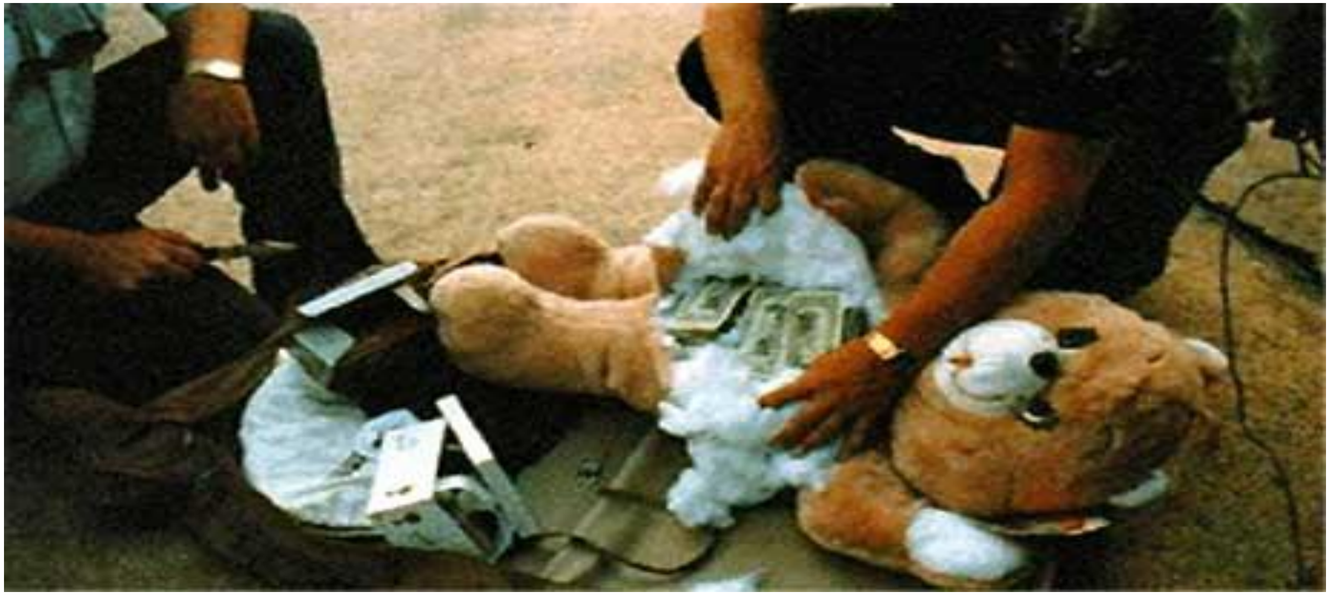
- CBP and Industry Leaders working together to enhance national security and facilitate legitimate cargo.
- Strengthening the international supply chain through the exchange of ideas, knowledge, and “best practices”.
- C-TPAT is the largest government-private sector partnership to emerge from the terrorist attacks on September 11, 2001.
- C-TPAT was launched in November 2001 with seven major importers who also saw the need for the focus on supply chain security.
- The guiding principles for C-TPAT have been enhanced supply chain security, partnership, and a voluntary program.

What are the threats?

- Terrorism, sabotage
- Trafficking – drugs; conventional, nuclear, chemical or biological weapons
- Illegal entry–stowaways i containers, trailers
- Theft of cargo, personal property or information

Concealment Methods

- Money leaving US
- Drugs/WMD entering US



C-TPAT Benefits

- Securing the Homeland
- As part of contingency planning, C-TPAT partners will be the first to participate in the restoration of trade
- Reduced Examinations
- Front of line treatment
- Assigned Supply Chain Security Specialist
- Access to other programs (Free And Secure Trade (FAST), Importer Self Assessment (ISA), Simplified Entry, etc.)
- Supply Chain Security Conferences hosted by C-TPAT yearly
- Mutual Recognition – e.g. EU

What are the added benefits of participating in C-TPAT?

Companies that spend on supply chain security can expect an advantage far outweighing the costs of implementing security processes, according to a study by Stanford University.

The study quantified some of the benefits of investing in security:

- Companies collectively reduced their Customs inspections by 48%
- Increased the automated handling of their imports by 43%
- Saw a 29% reduction in transit times
- Asset visibility in the supply chain improved by 50%
- 30% improvement in on-time shipping to their customers
- Reduced time taken to identify problems by 21%
- Reduced time taken for problem solving dropped by 31%
- Reduced inventory theft by 38%
- Excess inventory was reduced by 14%
- Reduced customer attrition by 26%

C-TPAT Security Criteria

Security Criteria for importers

Business Partner Requirements

- Documentation that they are a C-TPAT member
- Non-C-TPAT member, written or electronic confirmation or survey indicating they meet C-TPAT security criteria

Container Security

- Written sealing procedures (PAS ISO 17712 seal)
- Seven-point inspection prior to loading / upon receipt
- Container Storage, secure locations, preventing of unauthorized entry into container or storage area

Physical Access Controls

- Visitor procedures (including deliveries and mail) – Logbooks, visitor badges, escorted access
- Employment Procedures – Identification system

C-TPAT Security Criteria

Personnel Security

- Procedures in place to screen prospective employees & to periodically check current personnel (Background & employment history)
- Personnel termination procedures in place to remove access

Procedural Security

- Document processing – accurate, complete & safeguarded
- Manifesting procedures – accurate and timely

Security Training and Awareness

- A threat and security awareness program established for all employees
- Employees must be made aware of the procedures the company has in place to address a situation and how to report it

Business Partner Requirements

- C-TPAT certification – OR -
- Other security certification – AND -
- Comply with C-TPAT importer security criteria
- AND complete survey and make visits to audit
- Applies to
  - Suppliers who import raw materials, equipment, tooling used in production, etc.
  - Suppliers who ship directly from overseas to Company locations worldwide
  - Customs Brokers
  - Freight Forwarders
  - International carriers

Vendor Standards

- Credit worthiness - a cash poor company (individual) may be a desperate company (individual)
- How do documents arrive at your facility or your broker's facility? a sudden change in procedure by vendor must be questioned
- Who signs the docs? Sudden change in personnel should be questioned / reviewed for all vendors
- Who is training new personnel at your vendor site – always ASK!

Verify, Verify, Verify!

- Require proof of insurance

Container Security

- Container/trailer security
  - Includes container/trailer seals
    - Seals should be stored in a secure area
    - ISO certified bolt seals only
    - One or two people should handle seals
    - Record & track each & every seal number used for shipments
  - Location containers or trailers are stored
    - Should be in an enclosed, secure area & trailer locations should be tracked
  - Inspection prior to loading
    - Use the 7-point inspection process
    - Document the trailer inspection
    - Shipper Load & Count Cargo – be extra careful checking
    - No one’s looked at shipper load & count since the container was sealed at the factory
    - Could be anything in that container

Cargo Security Recommendations

- Use CTPAT Certified Service Providers
- Use forwarders with web based tracking
- Check truck id's & container id’s for all deliveries
- Deliveries by appointment only
- MAKE RANDOM UNANNOUNCED VISITS!
- Your cargo is as secure as the driver moving it
- Trucking is the trickiest point in cargo security
- Cargo at rest is cargo at risk – keep cargo moving and avoid weekend moves
- Map your supply chain – know where your cargo is at all times

Physical Access Controls Security

- Physical security
  - Fencing
    - Perimeter controls to keep unauthorized people from having access to your trailers or building
  - Locks and alarms
    - Keep unauthorized people out of secure areas
    - If an emergency door is opened, an alarm should sound
  - Cameras
    - Show people arriving and leaving
    - Show shipping and receiving areas
  - Cargo handling and storage facilities must have physical barriers that guard against unauthorized access

Physical Access Controls ID’s

- Physical access controls
  - Employee identification and access
    - Employees should wear their badges at all times
    - Access to shipping and receiving areas should be limited to employees who need to be there
  - Visitor identification
    - All visitors must sign in and obtain a visitors badge
    - Visitors should be escorted while in the building

Visitor Policy
Key Take Aways

- How do you know someone is a visitor?
- What happens if you see an unescorted visitor?
- If something happens, how can I go back to my visitor log to figure out who was here?
- Care & control – I know what’s happening and who is in my building

Personnel Security

- Personnel Security
  - Pre-employment screening
  - On-going background checks
  - Watching for suspicious behavior or activity

Procedural Security

- Procedural Security
  - Document control
    - Limited access to blank forms and completed document storage
  - Shipping and receiving controls
    - Discrepancy reports and follow-up
  - Report threats and suspicious shipments
  - Security training
- Information Technology Security
  - Password protection
  - Limit access to data storage areas
  - Anti-virus software/ Firewalls
  - IT security policies, procedures and standards must be in place and provided to employees in the form of training

Documentation Standards

- Look at type set - is it different anywhere in the doc?
- Use of white out or similar product?
- Wrong invoices are often used to clear goods – cross check your documents to the PO
- If you can’t check all documents, perform random checks
- Is document illegible or in a foreign language?
- Are documents missing? Why?
- Does weight on invoice match packing list, airwaybill and delivery order?
- Is piece count the same across all documents?

DO NOT ACCEPT ANY DISCREPANCIES!

File & Documentation Protection

- Who has access to files?
- What leaves by way of hard or soft copy?
- Who keeps track of what's been "signed out"
- History files - purge them - ON TIME!
- Periodically audit - make sure nothing is missing

Cargo Marking & Document Protection

- Check marks & numbers against documents
- Change carton markings yearly
- Avoid use of company name & address on cargo
- Keep documents secure – not w/cargo
- Shred all old documents
- Keep documents in a locked or secure area
- Computer system secure? Who has access to print a PO?

DC Security

- Have set receiving processes
- Check marks carefully
- Process must identify overages & shortages
  - COUNT, COUNT & RECOUNT!
  - Rigorously pursue all overages and shortages
  - Segregate cargo that’s not your own in a secure area
- Must check container numbers & seals against seal report / pre-alert from supplier
- Official stripping reports – senior management audit against import documents
- Limit access to your facility
- Simple things like - restrooms for truck drivers
- Use simple common sense – if something looks wrong, it probably is a problem

Courier & USPS Security

- Every package accounted for
- Who are they?
- “Weak Link" - often ignored
- Insist on same standards
- Certify them

Become A Hard Target

- Take security seriously
- Maintain a low profile
- Layer your security
- **Be Aware!**

Reporting Suspicious Activity

- Post security rules where customers, employees and vendors can see them - DETERRENT
- Simple procedure for reporting irregular or illegal activity
- Incentive program for reporting suspicious activity

Change Is Good

- Randomness of activity enhances security
  - Show up at unscheduled or unexpected hours
- Sudden shift changes in cargo loading area
  - Unannounced audit of cargo loading area here & there
- Sudden shift changes in vendor payment area
- These are soft targets
- Rotate security on an unscheduled basis
- Unannounced visits to vendor sites

Continual Evolution Of Security
Change= Hard Target

- Unexpected change makes thieves/terrorists look elsewhere
- Risk assessments of your vendors
- High risk countries meet higher standards
- Risk score for each vendor
- Random 3rd party spot checks
- Layered security
- Enforcement - what are the consequences?

How Criminals Circumvent Security Measures

- Loitering near the facility observing procedures, asking questions
- Taking pictures, obtaining plans or making diagrams of facilities
- Impersonating workers i.e. pest control
- Calling or e-mailing employees about procedures

Recognizing Potential Security Risks

- Activity out of the norm
- Loitering out of normal sight lines
- Attempts to bypass security
- Clothing not suited to the weather
- Noises or odors not expected from containers
- Containers with holes, patches, missing or damaged seals or seal numbers that don’t match
- Incorrect Hazmat labels for cargo
- Can you think of others?

Common Scams

- Last minute documents or deliveries
- Receipt or transaction under pressure
- Have a policy for receipt of cargo or documents in time for handling
- Have a policy for controlling last minute events
- Have a policy for notification of senior management when events occur
- SCAM SIGNAL: Is the person exceptionally nervous, rushed or angry without good reason?

Internal Conspiracy
Here & There

- 80% of all theft in USA through internal conspiracy!
- Create and control separate receiving area
- 2 people verify each shipment
- Alternate roles frequently
- Shipping: one person assembles the order, one checks it, another loads the truck
- Minimizes theft AND errors

Preventing Internal Conspiracy Here & There

- Frequent inventories
- Close key control - key duplication
- Record of key use - termination policy
- Update / change security procedures at least once per year

Best Preventation Education & Awareness

…our employees & vendors know security is important!

- Educate employees
- Know our partners
- Create and share our security policy expectations
- Use C-TPAT certified service providers
- Implement a Security Policy and Procedures
- Secure our facilities, systems and conveyances
- Be conscious of security day to day

Securing the Supply Chain
What can we/you do?

- Challenge unfamiliar or unidentified visitors in the office or warehouse
- Don’t share system passwords
- Report in confidence any suspected or actual anomaly (irregularity) or illegal activity to management

Securing the Supply Chain
What can we/you do?

- Report potential security risks to management i.e. broken lock, fence, security light, etc.
- Don’t share information outside your company
- Be wary of outside requests for information about company policies, procedures, assets, etc.

Questions?

Kristen Whelan, Liberty International

kwhelan@libertyint.com

(401) 727 – 1776 ext. 121