Supply Chain Security
Best Practices

Presenters:
Bernice Conley, Supply Chain Security Specialist
Cecelia Ross, Supply Chain Security Specialist
Long Beach C-TPAT Office
Overview

- Definition of a Best Practice
- Best Practices Catalog
- Best Practices Examples
Best Practices Catalog

- Best practices were identified by Supply Chain Security Specialists during C-TPAT validations and site visits conducted between 2003-2005

- Abstracted from over 1,000 validation reports

- Developed for the trade to use in strengthening their company’s supply chain security program
Definition of a Best Practice

- Exceeds minimum security criteria/guidelines
- Incorporated into partner’s business process (ex. policies, procedures, job descriptions)
- Integrates people, processes, and technology
- Incorporates checks, balances, and accountability
- Testing, Auditing, Recording, Follow-up (TARF)
How far should you go…

with testing?

Supply Chain Security in a New Business Environment
Best Practices: Management Support

- Proactively engaged
- Engages key players to integrate security into processes, policies, and procedures
- Encourages communication/outreach
- Encourages continuous improvement

Supply Chain Security in a New Business Environment
Best Practices: Trade Data

- Automated Commercial Environment (ACE)
- Advanced Trade Data Initiative (ATDI)
- Electronic Data Interface (EDI)
- Advanced Shipping Notices (ASNs)
- End to End supply chain visibility
Best Practices: Risk Analysis Self-Assessment

- Documents security plan and procedures
- Prioritizes supply chain security issues
- Identifies emerging security risks/threats and takes action to minimize risk
- Re-addresses security as business operations and environment change
Best Practices: Business Partner Requirements

- Written procedures for supplier/vendor/service provider selection, include security requirements

- Contractual requirements include security

- Established code of conduct for business partners

- Selection of business partners includes:
  - Internal collaboration
  - Integrity/background screening

- Random audits & site visits of business partners’ premises

Supply Chain Security in a New Business Environment
Best Practices: Container Security Inspections/Seals

- Documented policies and procedures
- Consistency/accuracy - 100%
- Inspections/verifications documented
- Verified and tracked throughout the supply chain
- Checks, balances, and accountability
- Technology (e-seals, smart-box, etc.)
Best Practices: Container & Conveyance Storage/Tracking

- Documented procedures to IMMEDIATELY address anomalies
- Monitor and track all containers and conveyances from point of stuffing to domestic distribution center
- Technology (RFID, GPS, etc)
- Random checkpoints
- Daily inventory of equipment

Supply Chain Security in a New Business Environment
Best Practices: Access Controls

- Documented policies and procedures
- Advanced visitor approval required
- Appointments for deliveries/visitors
- Biometrics
- Visible work area restrictions (e.g., color-coded uniforms)
- Segregated driver waiting areas
- Escalation matrix

Supply Chain Security in a New Business Environment
Best Practices: Procedural Security

- Documented policies and procedures (ex. data security, manifests, purchase orders, shipping/receiving)

- System to identify, track, report, and follow-up on breaches and incidents

- Specialized packing materials, unique shipping marks, palletizing, and shrink-wrapping to detect tampering

- Anonymous (undercover) observers to identify internal conspiracies

- Rotating employees to prevent collusion

- Sensitive document destruction to prevent identity theft

Supply Chain Security in a New Business Environment
Best Practices: Personnel Security

- Documented policies and procedures
- Comprehensive background/criminal checks for employees, contractors, temps, and vendors, as permitted by law
- Identity documents submitted by prospective employee are verified
- Code of Conduct
  - Incorporates security
  - Acknowledgment of receipt obtained from employees
  - Training provided to employees
  - Consistently enforced by management
Best Practices: Security Training & Awareness

- Documented security awareness training
- Awareness training conducted at employee orientation and ongoing
- Specialized training for human resources, shipping/receiving, buyers/salesmen, drivers, etc.
- Integrity training
- Dual-use product awareness
- Security awareness and outreach training to business partners
- Utilizing law enforcement & security professionals
Best Practices: Physical Security

- Checklist covering all physical security components
- Routine and random facility inspections/maintenance
- Trained & equipped personnel
- Penetration assessments conducted
- Back-up systems in place and routinely tested
Best Practices: Information Technology

- Documented policies and procedures
- Password configuration and access levels (change, limit, terminate)
- Routine updates/upgrades, firewalls, virus protection, anti-Spyware, encryption-wireless technology
- Continuous IT security training (ex. Interactive, web-based training)
- Tracking and accountability of system users
Essential Ingredients of a Best Practice:

- Testing
- Auditing
- Recording
- Follow-up
Supply Chain Security
Best Practices

Partnership is the Key!

Supply Chain Security in a New Business Environment