

# Supply Chain Security vs. Port Security



AAPA Terminal Management Seminar  
Long Beach, CA  
January 25, 2005

# Today's Objectives

---

- ▶ Provide overview of supply chain security vs. port facility security vs. vessel security
- ▶ Who, what, where, why and how in each role
- ▶ Update on status of Operation Safe Commerce and other supply chain security initiatives



# Supply Chain vs. Port Security

## Who.....

### ▶ Facility Security

- ▶ Customs & Border Protection (C&BP)
- ▶ Maritime Administration (MARAD)
- ▶ US Coast Guard
- ▶ Ports
- ▶ Terminal Operators
- ▶ Transportation Security Administration (TSA)
- ▶ Labor

### ▶ Supply Chain Security

- ▶ Shippers
- ▶ Carriers
- ▶ Logistics providers
- ▶ Foreign ports and terminals
- ▶ US ports and terminals
- ▶ TSA, MARAD and C&BP
- ▶ Labor

# Who.....

---

## ▶ Vessel Security

- ▶ U.S. Coast Guard is responsible for:
  - Monitoring and tracking all vessels
  - 96 Hour notification
- ▶ Customs & Border Protection
  - Crew review (with USCG)



# What- Port Security

---

- ▶ Effort based upon IMO SOLAS and revised ISPS Code
- ▶ Congress Passed the MSTA of 2002
  - ▶ Required Plan and implementation by July 2004
- ▶ Five rounds of port security grants



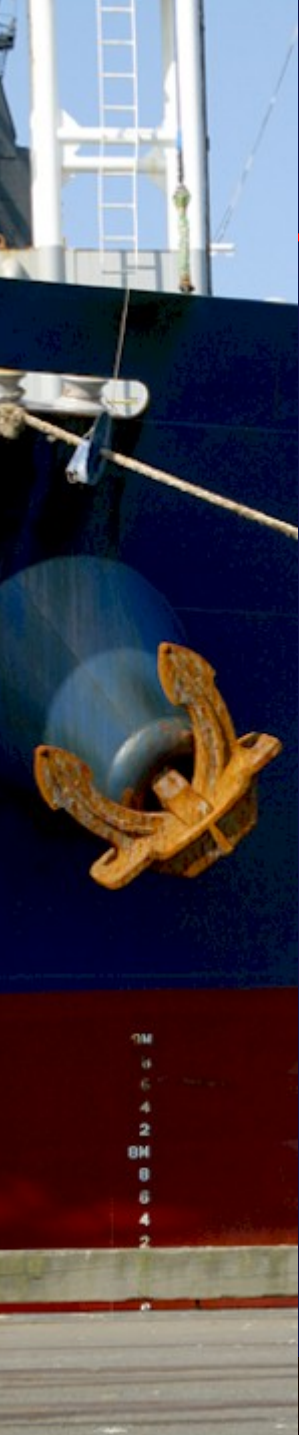
# Port Security Grants

- ▶ AAPA estimated \$1.4 billion required
- ▶ TSA/MARAD Grants Totaling \$516 million
  - ▶ Round 1- \$93 M Awarded: June 2002
  - ▶ Round 2- \$169 M Awarded: July 2003
    - ODP grant -\$75 M Awarded: June 2003
  - ▶ Round 3-\$179 M Awarded: December 2003
  - ▶ Round 4- \$50 M Awarded: September 2004
  - ▶ Round 5- \$150 M: Being developed, Spring 2005 release

# Port Security: Strategic Vision

---

- ▶ Integrated approach w/ policies, procedures, systems and personnel
- ▶ Integration of information with
  - ▶ First responders
  - ▶ USCG, MARAD, C&BP
  - ▶ Other Ports
- ▶ No Port is considered "weak link"





# Port Security: Actions and Achievements

---

- ▶ Security plans submitted July 1, 2004
  - ▶ AAPA has verified 100% (63 of the 84 ports reporting) compliance
- ▶ Initial focus of grant request
  - ▶ Port access controls
  - ▶ Perimeter security improved
  - ▶ Creation of awareness and training programs
  - ▶ Establishing information sharing protocol
  - ▶ Facility controls and coordination





# Supply Chain Security: Existing Initiatives

---

- ▶ C-TPAT- Voluntary program between C&BP and shippers
- ▶ CSI- C&BP and foreign Ports
- ▶ Operation Safe Commerce
- ▶ C&BP 24 Manifest rule, FDA Bio-terrorism rule
- ▶ Private initiatives- SST, StarBest
- ▶ RPM- Radiation Portal Monitoring System (C&BP)
- ▶ Smart Container initiative (C&BP)



# Operation Safe Commerce

- ▶ Federally funded program (\$58 Million) for container security
- ▶ Series of supply chain demonstration projects (19 projects)
- ▶ Three load centers-
  - ▶ Ports of Seattle and Tacoma
  - ▶ Ports of Los Angeles and Long Beach
  - ▶ Port Authority of New York/New Jersey
- ▶ Use of commercially available, off the shelf technology



# Operation Safe Commerce Vision

---


**Develop an architecture that forms the basis of international standards for a secure supply chain**

- ▶ Repeatabe, scalable, and cost effective
- ▶ Maintains or facilitates the smooth flow of trade
- ▶ Enhances threat security while also enhancing theft security



# Operation Safe Commerce Mission

---

- 
- ▶ **Identify the vulnerabilities**, at each step in the supply chain.
  - ▶ Determine, document and test the **best policies, procedures, processes and technology available** to prevent the introduction of unmanifested material into the global supply chain.

# OSC Schedule

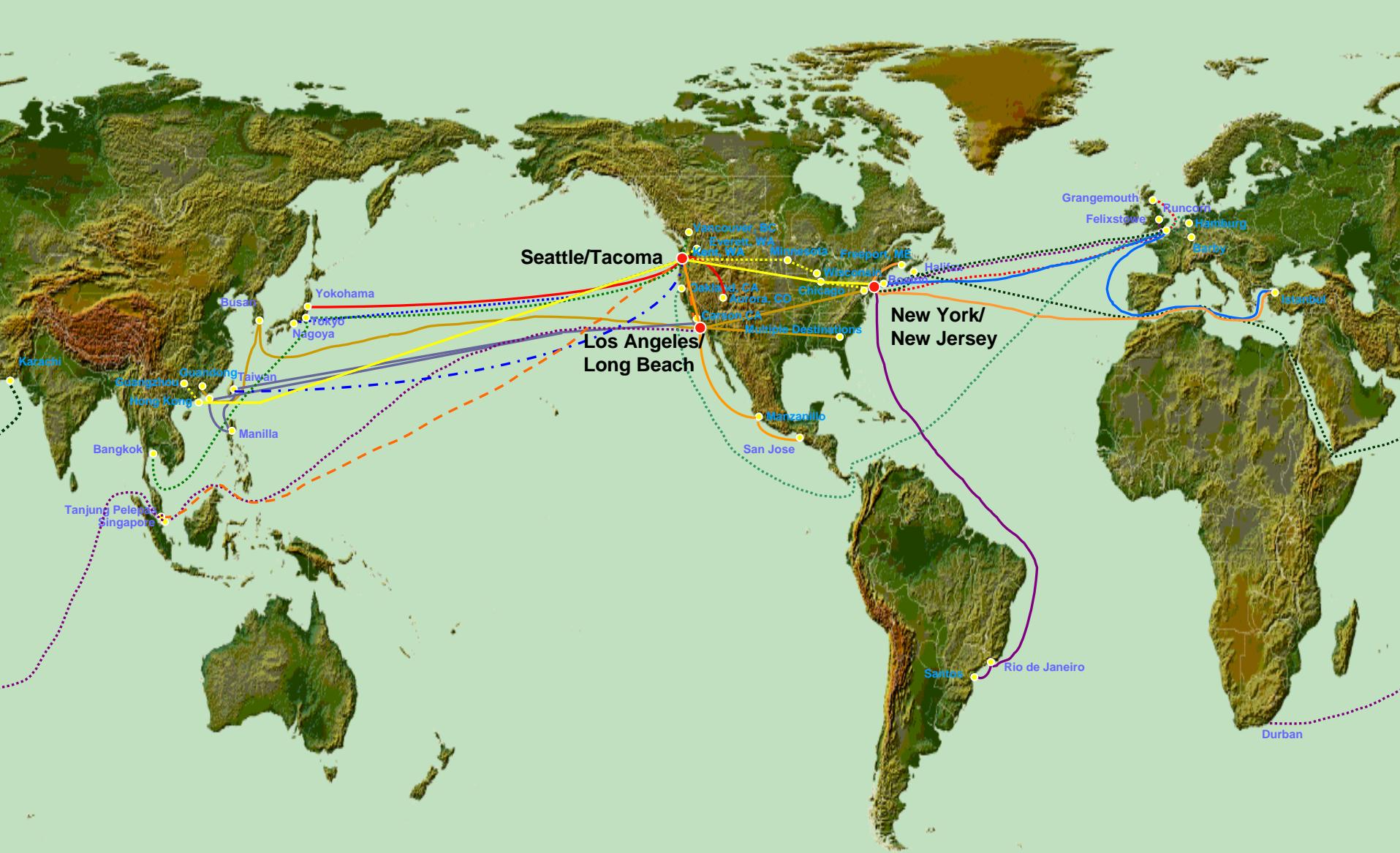
---

- ▶ OSC Round II (\$58 Million, 19 projects)
  - ▶ Funding approved May 2003
  - ▶ Formal notification of awards August 1, 2003
  - ▶ NY/NJ and Tacoma/Seattle submitted final reports Oct 2004 (LA/LB Mar 2005)
  
- ▶ OSC III (\$17 million authorized)
  - ▶ Start up April 2005
  - ▶ Completion Oct 2006



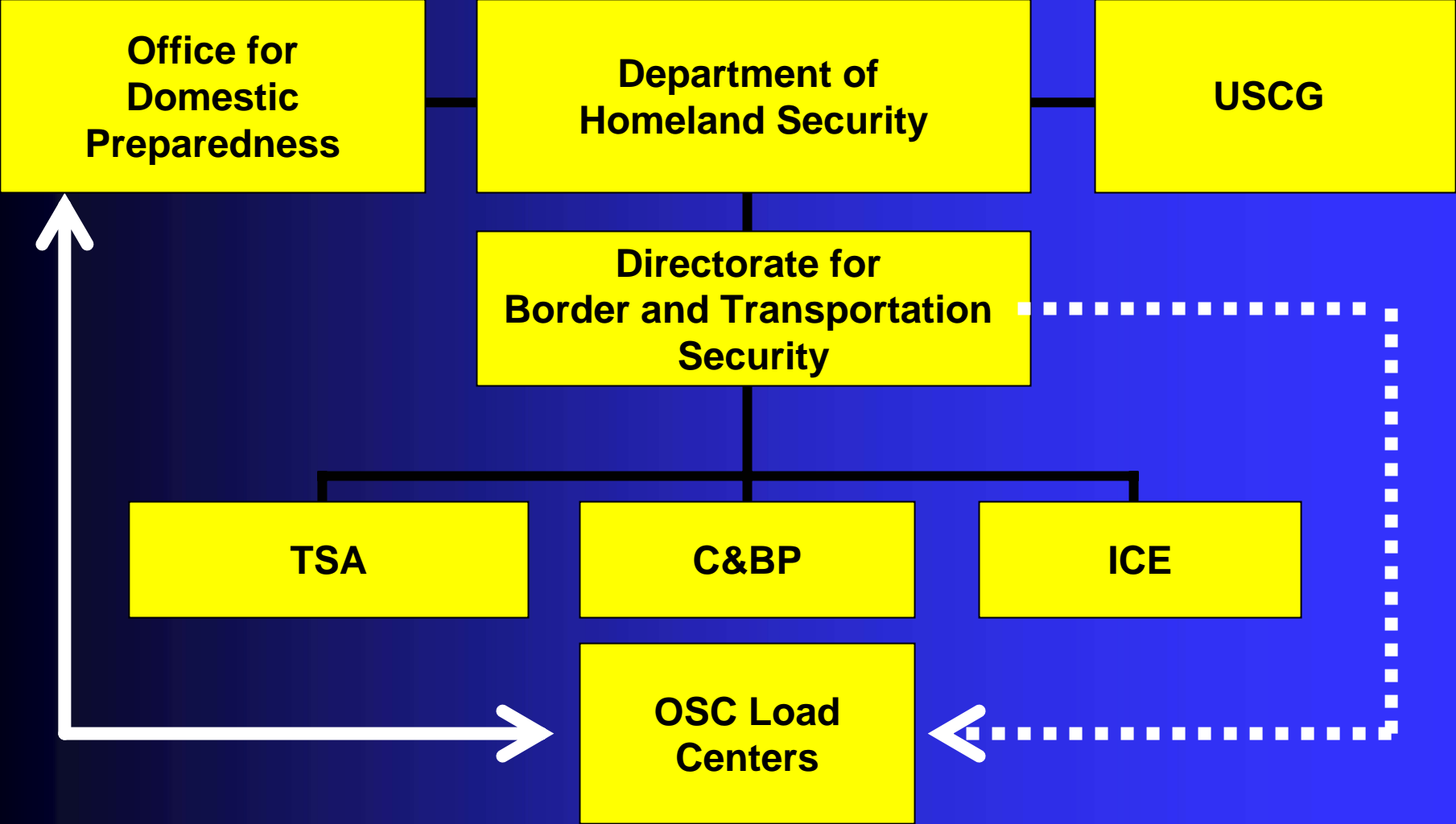


# Operation Safe Commerce All Project Supply Chains

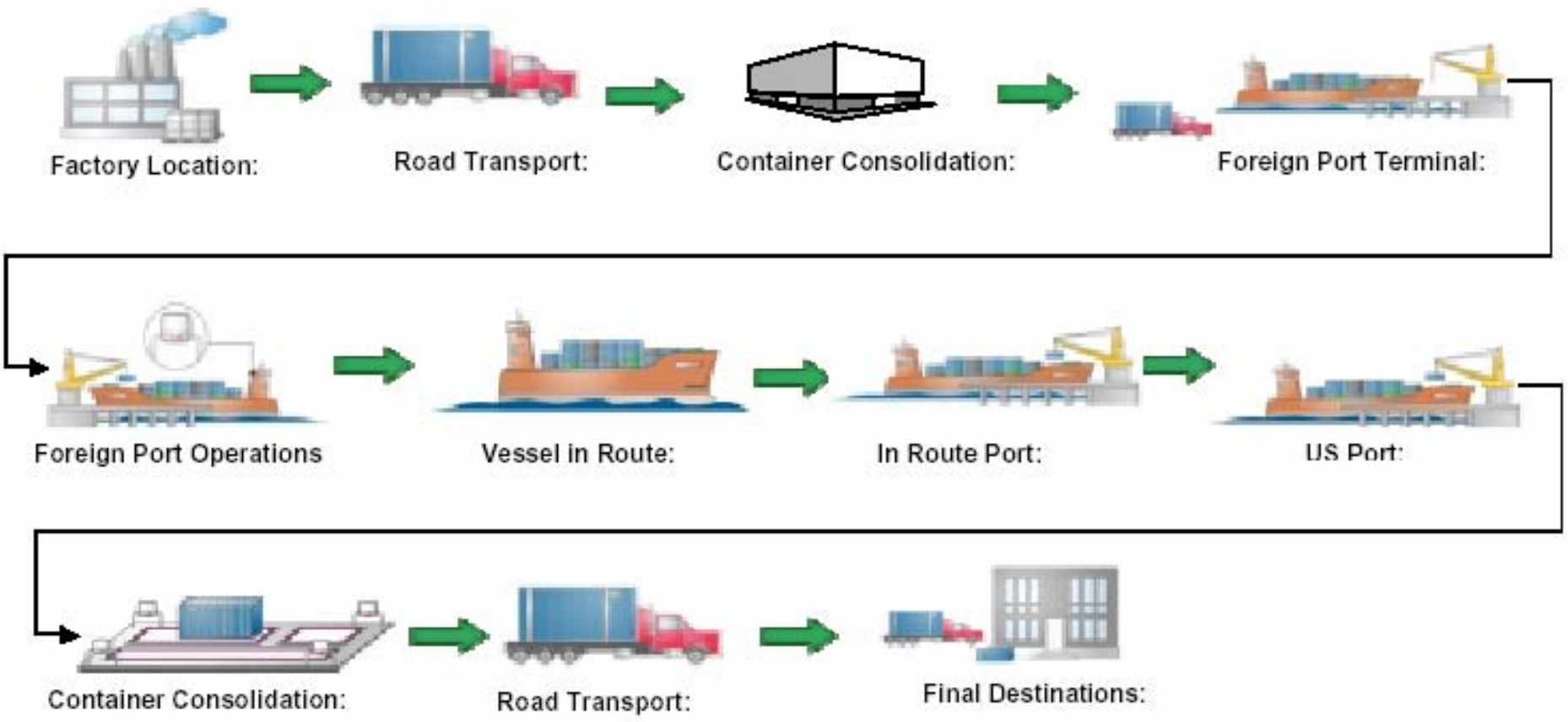




# National OSC Organization and Guidance



# Typical Supply Chain



# Load Center Stakeholders

---

- ▶ Staff of LC Steering Committee
- ▶ Terminal Operators
- ▶ PMA
- ▶ ILWU
- ▶ Railroads
- ▶ Trucking and Drayage firms
- ▶ Shippers/logistics providers
- ▶ Maritime shipping organizations



# Seattle/Tacoma OSC II

## Lessons Learned

---

- ▶ Most significant risk is foreign drayage
- ▶ No one project defined the ultimate solution
- ▶ Final report recommended performance standards versus specific technology
- ▶ Solution requires multi-sensor approach
- ▶ Effective Supply Chain Event Management system required
- ▶ Labor and PMA must be involved



# Seattle/Tacoma OSC II

## Lessons Learned (cont.)

---

- ▶ Supply chains are unique, dynamic
  - ▶ System wide solution required
  - ▶ NVOCC's have significant impact
- ▶ Open architecture required—not proprietary solutions
- ▶ Solutions must be commercially viable
  - ▶ Must enhance productivity/efficiency
  - ▶ Those that enhance inventory control/yard management most likely to be implemented
- ▶ Complete supply chain visibility essential
- ▶ Layered approach to security

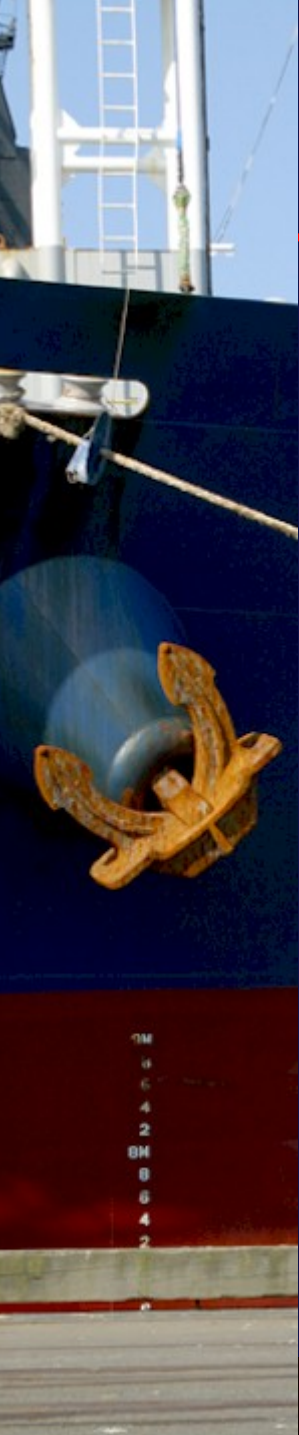


# Seattle/Tacoma OSC II

## Lessons Learned (cont.)



- ▶ Improved policies, procedures, practices and trained personnel reduced risk significantly
- ▶ Overseas C-TPAT suppliers need independent validation
- ▶ Bolt Seals & e-Seals commercially viable to detect door opening – not removal or intrusion thru walls
  - ▶ Disposable solutions better than reusable solutions
- ▶ Supply chain event management systems that facilitate trade and security most likely to succeed
- ▶ 3<sup>rd</sup> party inspections viable for high risk origins



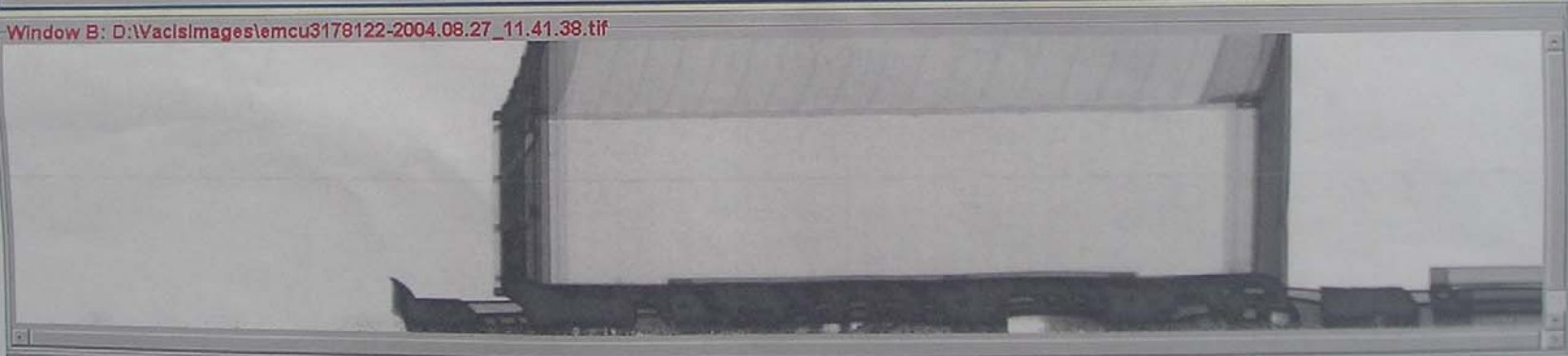
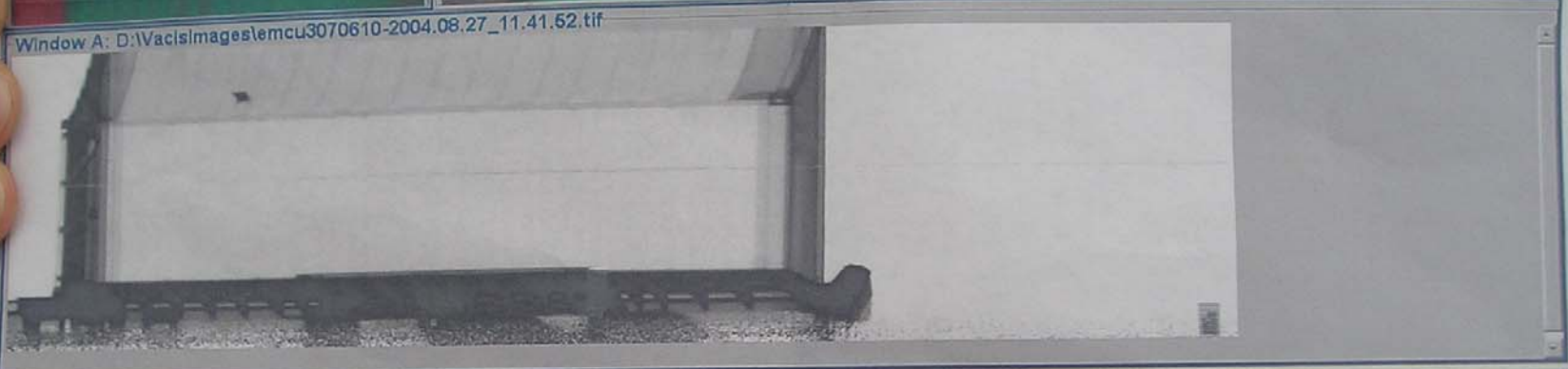
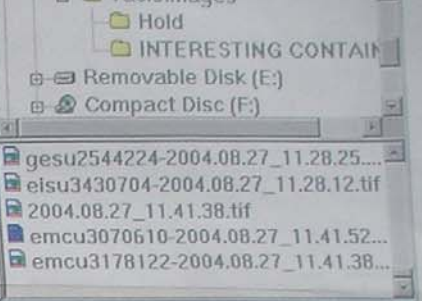
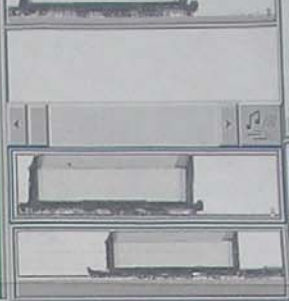


# Seattle/Tacoma OSC II

## Lessons Learned (cont.)

---

- ▶ Air sampling (Bio/Chem) – Too long
- ▶ Document authentication – Some countries
- ▶ CCTV - Could not read barcode/OCR
- ▶ Data loggers - Minimal value forensics only
- ▶ GPS - Line of Sight, Battery issues
- ▶ Information imaging – Cost & integration issues
- ▶ No power/internet in rural areas



Speed = 0.6 mph    Window A    X-    Y-    Intensity =    Zoom = 1.0    Pages = 0/1    Original







# OSC III Project Goals and DHS Criteria

---

- ▶ Based on “best-of-breed” from OSC II
- ▶ Enhance point of stuffing security measures
- ▶ Deploy promising tamper evident solutions
- ▶ Support new seal requirements for loaded inbound marine containers
- ▶ Promote better information collection



# OSC III Project Goals and DHS Criteria (cont.)

- ▶ Integrate existing C&BP and USCG policies and protocols
- ▶ Propose domestic interdiction processes and mechanisms
- ▶ Increase OSC volume of shipments
- ▶ Conduct cost-benefit analyses
- ▶ Probe for gaps





# OSC III Project Goals and DHS Criteria (cont.)

---

- ▶ Account for nodes where mode of transport changes
- ▶ Propose need for and value of international standards
- ▶ Account for and measure security enhancements' commercial return on investment
- ▶ Establish testing protocols and quantitative performance metrics

# Commissioner Bonner's 5 Point Cargo Security Strategy

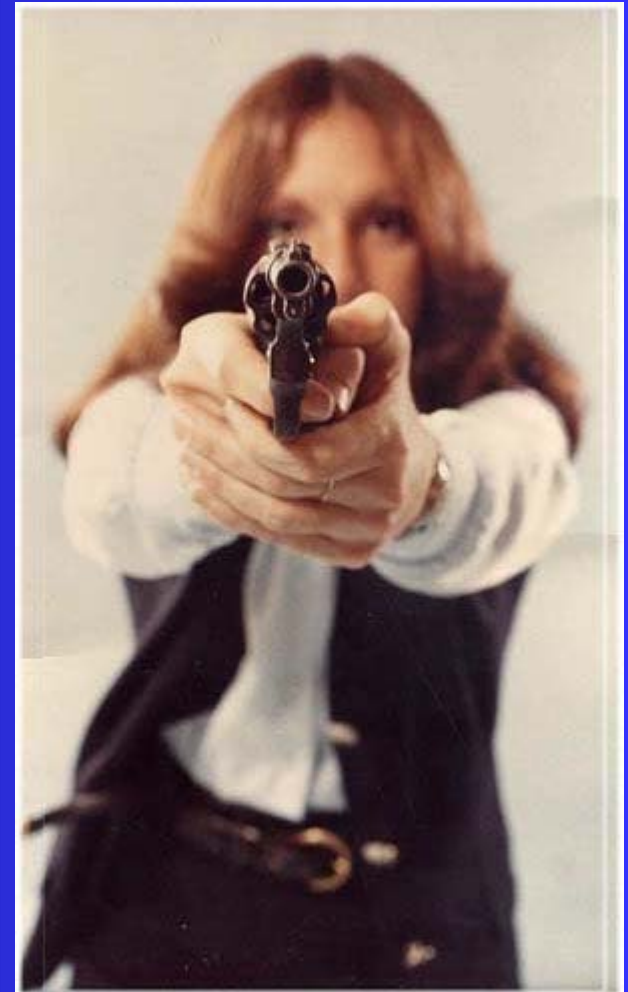
- ▶ 24-Hour Rule
- ▶ Automated Targeting System
- ▶ CSI (currently in 32 container ports)
- ▶ C-TPAT (7,000 companies)
- ▶ Smart Boxes- Directly linked to Operation Safe Commerce testing and findings



# Summary

---

- ▶ We are safer today than yesterday and we will be safer tomorrow than today
- ▶ The biggest bang for the \$\$\$ is in supply chain security
- ▶ We must have cohesive and uniform direction from the top of DHS
- ▶ From the Cargo Security Summit- We must have coordinated contingency plans for maintaining maritime commerce when an event occurs.



# Discussion and Questions



# Inspections and Protocols

---

- Seal visibility and change protocols
- Empty container inspection protocols
- Education and training standards
- Container stuffing protocols
- Known carriers assigned to custody, segments of supply chain
- Alarm management and response protocols

# SCEM Feeds and Controls

---

- ▶ Intrusion Detection Devices/Alarm Protocols
- ▶ Transit time rules for each custodian
- ▶ Seal number audit at each transfer point
- ▶ Known or nominated shipper audits
- ▶ In-out gate EDI feeds from terminals
- ▶ Load, unload EDI feeds from carriers
- ▶ AMS audit, MID-HTS-USA
- ▶ Driver Credentials validated, audits



# Shipper Responsibilities and Tasks

---

- ▶ Assign Coordinators (Security and IT Systems)
- ▶ Appoint Data Integrator
  - Coordinate data interchange between OSC SCEM and Logistic Systems
- ▶ Participate in executive steering committee
- ▶ Evaluate results and reports

# Shippers Responsibility and Tasks

---

- Require Origin factories and Transportation Suppliers Participation
  - C-TPAT Vulnerability Survey conducted by PNWLC
  - Policies, procedures for training and access to stuffing and materials work in progress
  - Empty control, ordering, inspection policies
  - Driver credentials validated at empty delivery and stuffed container pick-up
  - Seal management and control, installation policies
  - Device installation, training and supervision
  - EDI transaction activity to SCEM, to PO, Seal #, Device #, Driver ID and AMS filing access

# PNWLC Responsibilities

---

- ▶ Interface with ODP, DHS, CBP
  - ▶ Financial and Technical Reporting
- ▶ Project management
- ▶ Final report writing
- ▶ Budgeting and Financial Controls
- ▶ Vendor contracts, performance and payment
- ▶ Liaison with Labor, terminal management
- ▶ Testing with Sandia
- ▶ Interface with other load centers

# Data Integrator Responsibilities

---

- ▶ Manage integration with shippers IT
- ▶ Manage integration with SCEM external and internal data sources
- ▶ Manage rule-sets for alarm notice
- ▶ Integrate technologies and devices into SCEM
- ▶ Assist in incident response protocols