Terminal and Container Cargo Security

Mark A. Tierney
General Manager
Security and Compliance
Maersk Inc

"A.P. Moller is committed to show constant care and to prevent breaches of security associated with our operations, and ranks security considerations equally with commercial and operational factors in managing our business.

We will, in close co-operation with responsible authorities, take all measures necessary to constantly maintain the highest security standards in the organization, at shore facilities, as well as onboard our vessels."

Maersk Security Program (MSP)

- Group-wide initiative to fully integrate security with business processes
- Ensure we protect our assets
  - Colleagues
  - Business
  - Facilities
  - Vessels and Cargo
- Framework
  - Global approach / Local implementation
  - Uniform
  - Practical
  - Flexible
  - Compliant with laws / regulations

MARITIME TRANSPORTATION SECURITY ACT OF 2002

- **Facility Assessments**
  - Vulnerability and threat assessments
  - By USCG with update every 5 years
  - Assessment done by or on behalf of owner/operator
- **Maritime Transportation Security Plans**
  - 3 distinct, but overlapping layers of security plans
    - National Maritime Transportation Security Plan
    - Area Maritime Transportation Security Plan
    - Facility Security Plans (also applies to Vessels)

FACILITY PLANS

- Contain Provisions To:
  - Establish/maintain physical, passenger, cargo, personnel security
  - Control access to all areas
    - Identify and control restricted areas
  - Provide for procedural and communications security
  - Maintain/Calibrate/Test security systems and standby
- Identify measures to deter a transportation security incident or threat
- Provisions for training, drills, and exercises
- Audit yearly-Government re-submission every 5 years

Elements of Facility Security

1. Access

- to prevent facility entry of unauthorized people, vehicles, vessels and dangerous substances/devices

- scalable methods at all access points for screening (& tallying) of all people (visitors, vendors & employees), vehicles, vessels & cargo accessing the facility

2. Restricted Areas

- specific areas within a facility (or the entire facility.) that require higher security protection; are clearly marked/signed, & limited to authorized personnel

3. Cargo Handling/Control

- to deter tampering

- prevent improper containers from being accepted & stored at the facility

Elements of Facility Security cont…

4. Vendors, & Vessel Stores, Bunkers

- control & screening is scalable depending and coordinated between FSO and VSO

5. Facility, Operations, & Movement Monitoring

- lighting, CCTV & other surveillance hardware, security guards & patrols, automatic intrusion devices; (calibration & testing of hardware & systems required to be documented)

6. Incident Response

- respective facility plans outline specific protocols for contacting local CG, LE, emergency response and other necessary responders

- detailed mustering areas & evacuation procedures

7. Drills & Exercises

- drill to test particular element of facility security
- Exercise to fully test security program

MAERSK TERMINALS

- Security guard service
  - Union supplied uniform security guards in 4 locations
  - Contract vendor guard service in 5 locations
  - Port Authority supplied security (police) in 3 locations
- Technology
  - Biometrics for access areas (palm/thumb)
  - Proximity cards
  - CCTV
    - Digital (228 to be installed in Elizabeth)
  - Current and efficient cargo management systems

Access Technology

TRANSPORTATION SECURITY INCIDENT RESPONSE PLANS

- Incorporate into facility and vessel plans
- Comprehensive response to emergency:
  - Notify/coordinate w/Federal, State, local authorities, including FEMA
  - Secure facility
  - Evacuate personnel

Terminal Security

Facility Security Officer (FSO):

- Drafts Facility Security Plan
- Incident response
- Ensures regulatory compliance (external relations)

Transportation Worker Identification Card Program
TWIC

MÆRSK

Protect Individual Privacy

- Collection of minimum data elements
- Secure record control system and network
- Employs advanced information technology to protect personal information
- System wide encryption implementation

Improves Security

- Reduced risk of fraudulent or altered credentials
- Biometrics used for secure, positive match of individual to authorized access level and clearances
- Ability to interface and communicate with other agencies
- Ability to disseminate “threat alerts”

Enhances Commerce

- Increased process speed and efficiency
- Enables improved management and utilization of resources
- Expanded e-government potential
- Public-private partnership
- Economies of scale purchasing
- Eliminates need for redundant credentials and background investigations
- Leverages current security investment and legacy systems

TWIC PROTOTYPE PARTICIPANTS

Cargo Security Approach

1. Supply chain visibility
2. Supply chain security
3. Container security

Security Initiatives

Marine Transportation

- ✓ ISPS (International Ship and Port Facility Security) Code
- ✓ MTSA (Maritime Transportation Security Act of 2002)

Supply Chain Security

- ✓ C-TPAT (Customs-Trade partnership Against Terrorism)
- ✓ CSI (Container Security Initiative)
- ✓ OSC (Operation Safe Commerce)
- ✓ Customs and Border Protection “Smart Box”
- ✓ Retail Industry Leaders Association (RILA)

MTSA (Maritime Transportation Security Act of 2002)

DHS requested COAC (Commercial Operations Advisory Committee) via the MTSA Subcommittee to assist the in evaluation of proposals in three areas:

1. Performance standards for physical security for intermodal containers.
2. Development and implementation of Secure System of Transportation mandate.
3. Quantitative performance metrics to measure the success of specific DHS cargo security programs and to guide future efforts.

1. Physical Security for Intermodal Containers.

A. Party that loads the container must seal it immediately.

- ✓ Under a safe and secure stuffing process
- ✓ Shipper must use ISO high security seal
- ✓ Shipper must provide the seal number

B. Recording Seal Changes

- ✓ Legitimate reasons to break a seal create discrepancies
- ✓ The carrier (trucker, rail, ocean) must be notified
- ✓ New seal must be recorded

C. Ocean Carrier Seal Verification

- ✓ Is it an ISO standard seal?
- ✓ Is the seal intact?
- ✓ Is it the same seal provided by the shipper?

2. Secure Systems of Transportation

Five Elements

(1) screening and evaluating cargo;

(2) establishing standards for securing and monitoring cargo;

(3) developing security standards for shipping containers, including standards for seals and locks;

(4) identifying methods for the United States government to ensure and validate compliance with the program;

(5) implementing other measures to ensure the security and integrity of international intermodal transport.

C-TPAT : New Draft

- Appropriate security measures must be implemented and maintained throughout the importer's supply chains - based on risk.
  - Determine risk throughout supply chains based on their business model (i.e., volume, country of origin, routing, potential terrorist threat via open source information, etc.)
- Importer must work with business partners to ensure pertinent security measures are in place and adhered to by their direct/contracted business partners
  - Security "Standards" cover :
    - Business Partners, Container Security, Facility Access, Personnel
    - Procedural, Training and Awareness, Physical Security, IT

C-TPAT (Customs Trade Partnership Against Terrorism)

Maersk Client Needs:

C-TPAT Application:

- Commercial Information
- Vendor communication
- Shipment process (factory or CFS stuffing)

C-TPAT Validation:

- Customs verification of clients
- Origin Visits to observe security
- Review of policies and procedures

Customs and Border Protection “Smart Container”

Testing sensors that detect intrusions.

- **Container Security Device (CSD)**

  – sensors can communicate to CBP officers that particular containers have been tampered with or opened.

- **ISO mechanical seal appropriately secured by the "Pardo hole" or its equivalent**.

  – Mandatory "price of admission" for the Southern Border FAST program.

  – In the near future a requirement for all C-TPAT containerized shipments into the United States.

Smart Shipment vs. Smart Box

Recognize the security value of "**smart shipment**" transactions between known parties committed to total supply chain security vs. utilizing "**smart containers**" that do not address point of stuffing, the most vulnerable area in the supply chain.

SMART SHIPMENTS = ***GREENLANE***

Operation Safe Commerce

- Gap analyses of sample supply chains, involving New York/New Jersey, Los Angeles/Long Beach, and Tacoma/Seattle ports.

- Sample supply chains as test grounds for security technologies, and process improvements.

Maersk approach:

Applying technology based on transportation business process

Maersk Logistics participated in a supply chain moving cargo from Malaysia through Seattle / Tacoma.

- The testing and analysis lasted one year.
- Cargo security down to the carton level.

Retail Industry Leaders Association

MÆRSK

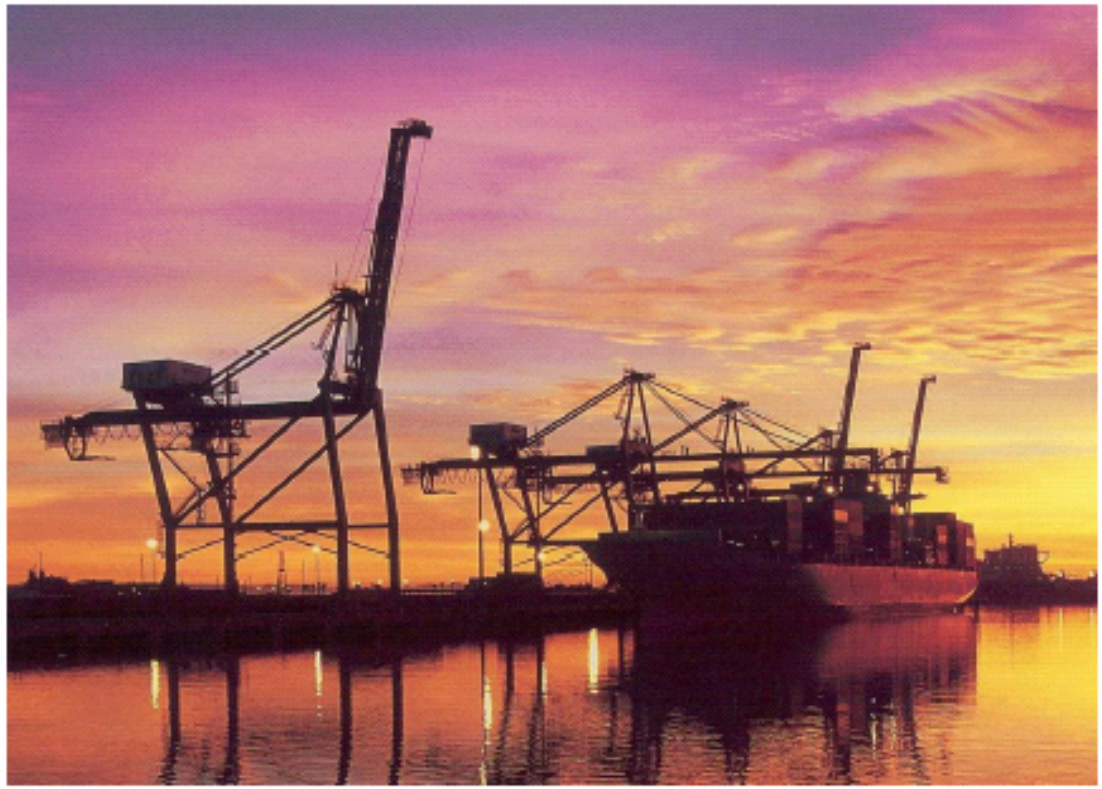
Supply chain Security Committee:

1. Foreign Manufacturer and Consolidator Security Standards Working Group
2. Foreign Port Facility Security Implications Working Group
3. Physical Container Security Working Group (incorporates Container Seal Best Practices accomplishments)

Trusted Partner/Trusted Transaction

1. Supply Chain Visibility
   - ✓ Better Commerce Through More efficiency
2. Supply Chain Security
   - ✓ Integrity of Partners
3. Container Security
   - ✓ Integrity of Container

Radiation Portal Monitor (RPM) Program



Office of Field Operations
Bureau of Customs and Border Protection

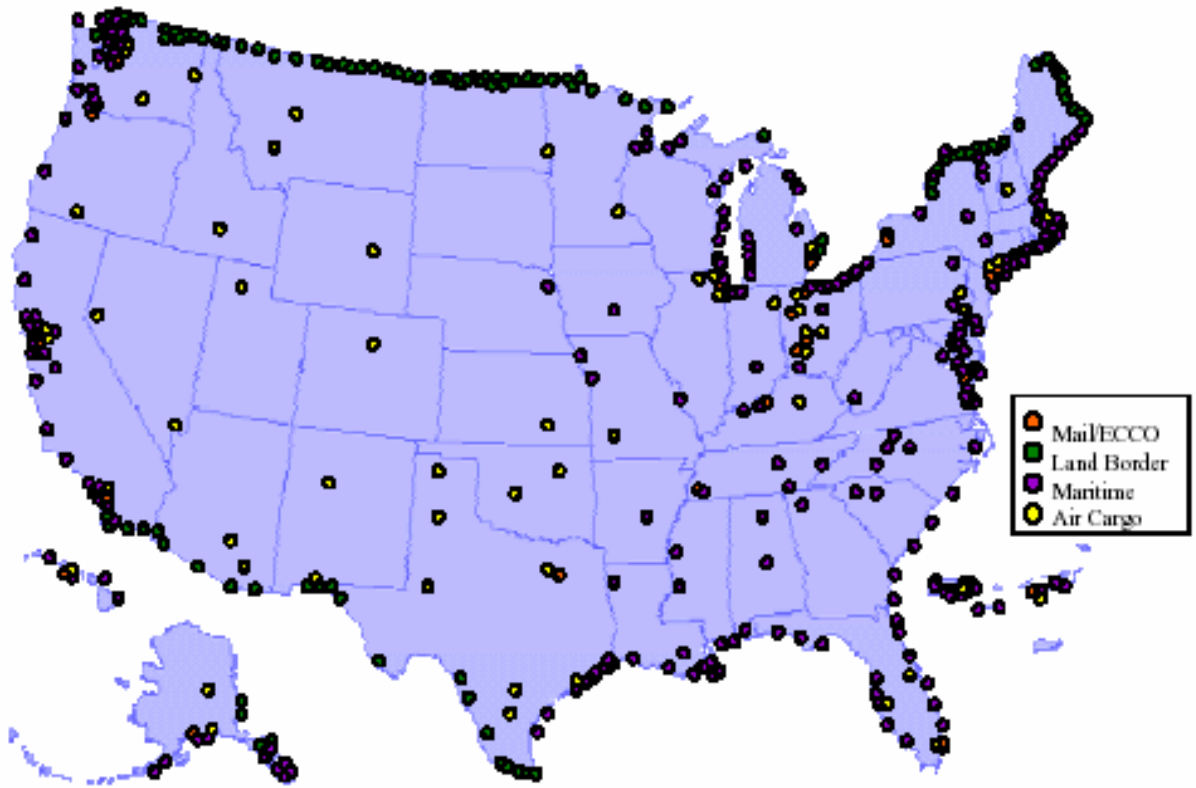
Applied Technology Division
Bureau of Customs and Border Protection

Pacific Northwest National Laboratory
US Department of Energy

CBP Program for Monitoring for Radioactive Materials

- **Objective:** Prevent the illicit import of nuclear and radiological materials into the Port
- **Need:** To protect high-risk locations and large economically important operations (high interest by Congressional staffers and GAO)
- **Strategy:** Screen all imported containerized cargo with highly sensitive gamma and neutron detectors called Radiation Portal Monitors or RPMs

Goal is 100% Screening



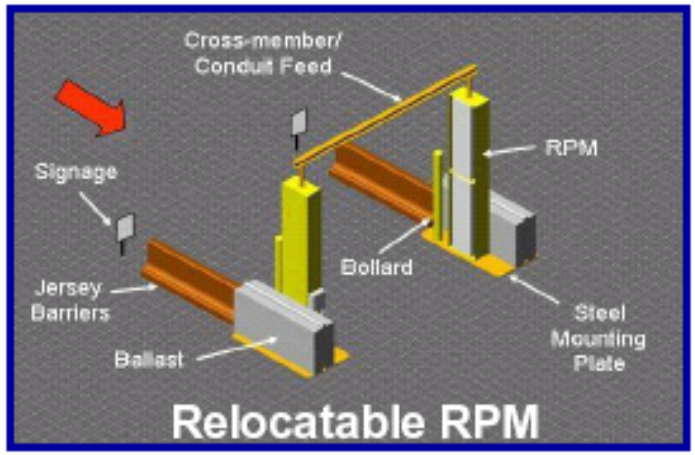
57,000 trucks/containers/day

333,000 vehicles/day

2,500 aircraft/day

600 vessels/day

Deployment Configurations for Seaports



Radiation Portals: APMT Elizabeth

Security In Action – “The Layered Approach”

Container Stuffing

Intermodal Truck Transit

Foreign Terminals

Ocean Transit

U.S. Terminals

Intermodal Rail Transit

Intermodal Truck Transit

Container Delivery

MÆRSK

THANK YOU