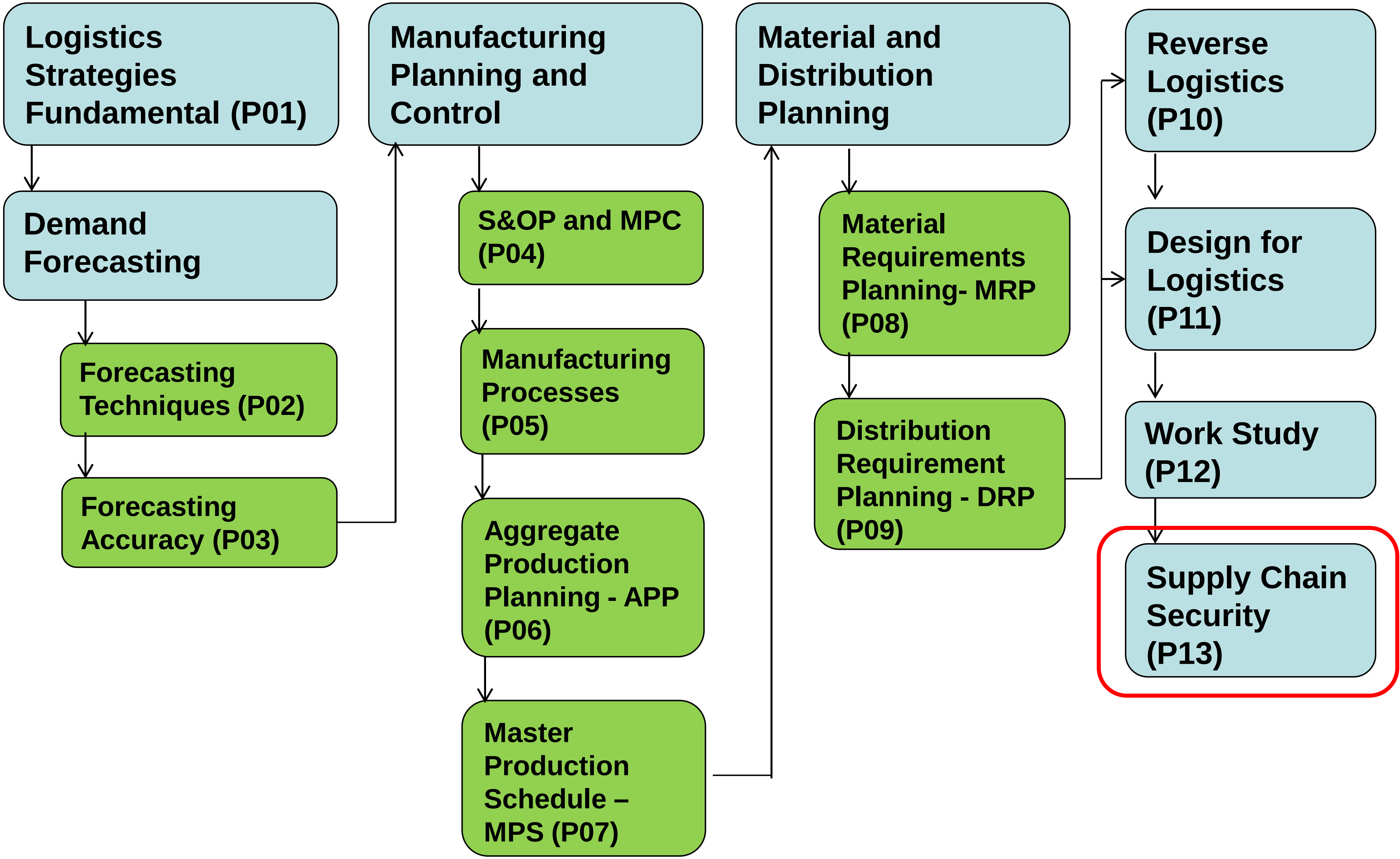
Problem 13
Supply Chain Security

SCHOOL OF ENGINEERING

E222 – Logistics Planning and Control

E222 Logistics Planning and Control – Topic Tree



Logistics Strategies Fundamental (P01)

Demand Forecasting

Forecasting Techniques (P02)

Forecasting Accuracy (P03)

Manufacturing Planning and Control

S&OP and MPC (P04)

Manufacturing Processes (P05)

Aggregate Production Planning - APP (P06)

Master Production Schedule – MPS (P07)

Material and Distribution Planning

Material Requirements Planning- MRP (P08)

Distribution Requirement Planning - DRP (P09)

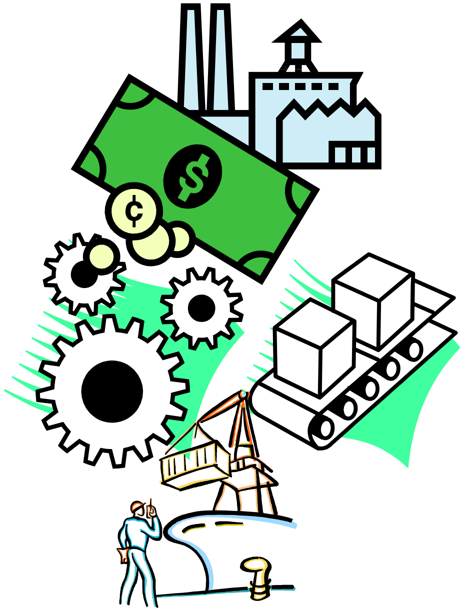
Reverse Logistics (P10)

Design for Logistics (P11)

Work Study (P12)

Supply Chain Security (P13)

P13 – Supply Chain Security



- Explain Key aspects of Supply Chain/ Logistics Security
- Describe Major Supply Chain Security Initiatives
- Identify potential security breaches and make recommendations to overcome it
- Enhance the Supply Chain/Logistics Security with Product Visibility

Supply Chain/Logistics Security

Why security along the supply chain?

Helps to prevent:

- **Nuclear, biological and chemical materials falling onto wrong hands**
- **Theft/Pilferage**
- **Sabotage**
- **Pirates**
- **Product contamination**
- **Environmental hazards**
- **Counterfeit product introduction**
- **Contraband goods etc…**

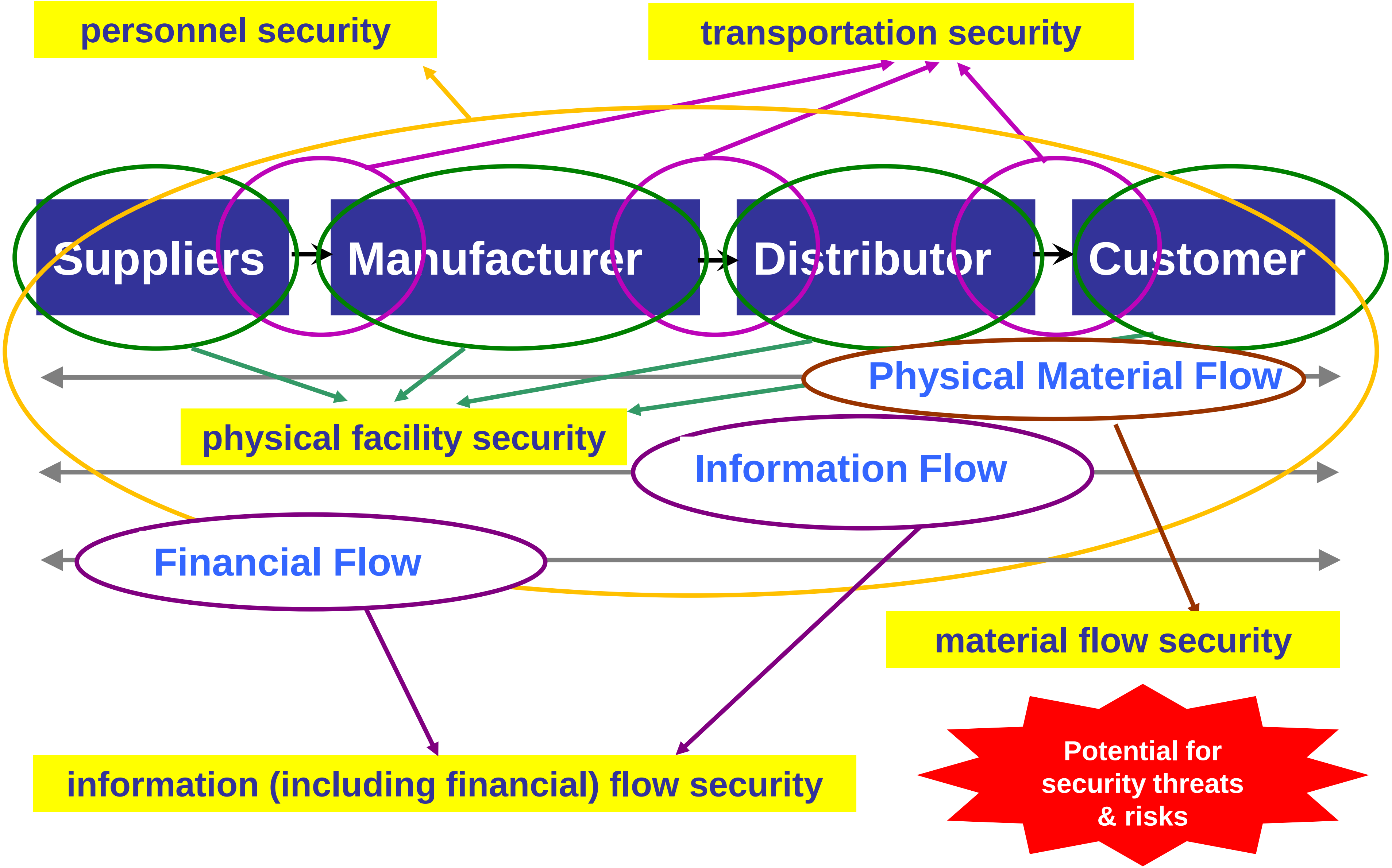
Implications (Some facts & figures…)

- **Global transit loss estimates- $30 to $50 Billion/year**
- **Typically 2-8% income reduction for Fortune 500 companies due to poor security**
- **Estimated, 80% of cargo thefts are “made to order thefts”**
- **Threat rated “severe” in Brazil, Russia, South Africa, Indonesia, Nigeria & Malaysia**

What would be the cost of an effective terrorist attack using the supply chain- UNKNOWN ??? But will be impactful

- ✓ **An attack would probably cause major international disruptions and closure of some businesses in the supply chain**

Supply Chain Security



personnel security

transportation security

Suppliers

Manufacturer

Distributor

Customer

Physical Material Flow

physical facility security

Information Flow

Financial Flow

material flow security

information (including financial) flow security

Potential for security threats & risks

1. Transportation Security

- **Regular and emergency communication equipment**
- **Security training of staff**
- **Non-intrusive inspection technology**
- **Focus on petroleum and cargo vessels**
- **Secure the movement of Inter-modal containers**
- **Secure air cargo and aircraft**
- **Reduce vulnerabilities to Catering, Refueling, Maintenance equipment**

2. Information Flow Security

- **Password protection**
- **Firewalls**
- **Compartmentalize information/segregate data**
- **Encryption**

3. Personnel Security

- Conduct personnel background checks
- Obtain security clearances
- Identification and verification

4. Material Flow Security

- Apply tracking and tracing technologies to monitor freight
- Use sensors to detect and report intrusions or tampering with the shipments while en-route or at a transshipment node
- Apply tamper resistant electronic seals
- Advance reporting of freight movements to expedite processing through the transportation nodes

5. Physical Facility Security

- **Securing the physical facility**
  - **Through the use of fences/physical barriers/guards/controlled access**
  - **Enhanced lighting, video, sensors**
- **Facility Layout (E.g. warehouse, factory)**
- **Includes screening passengers, cargo and physical inspections**

Major Supply Chain/Logistics Security Initiatives

1. **ISO 28000:2007- Specification for security management systems for the supply chain**
2. **Secure Trade Partnership (STP)**
3. **Transported Asset Protection Association (TAPA) Standards A, B and C**
4. **Customs-Trade Partnership Against Terrorism (C-TPAT)**
5. **24 hour Advance Manifest Rule**
6. **Container Security initiative (CSI)**

1. ISO 28000:2007

- Specifies requirements for a security management system critical to security assurance of the supply chain
- Applicable to both small and multinational companies, in **any stage of the production or supply chain** that wishes to:
  - establish, implement, maintain and improve a security management system;
  - assure conformance with stated security management policy;
  - demonstrate such conformance to others;
  - seek certification/registration of its security management system by an Accredited third party Certification Body; or
  - make a self-determination and self-declaration of conformance with ISO 28000:2007.

1. ISO 28000:2007 (continued)

ISO 28000:2007 is **NOT** about managing your security department.

It is all about managing your security in the supply chain !

2. Secure Trade Partnership (STP)

- Launched by Singapore Customs in 2007
- The Secure Trade Partnership (STP) Guidelines spells out the requirements which companies in the supply chain should adopt to enhance the security of their operations and supply chains
- Under the STP Guidelines, companies are required to:

  (a) have security management systems;

  (b) conduct risk assessments of their business operations; and

  (c) implement the security measures under the STP Guidelines to secure their supply chains.
- Companies meeting such requirements will be certified as **STP companies** by Singapore Customs, and can look forward to greater ease to bring goods into/out from Singapore

3. Transported Asset Protection Association

- TAPA: an organization made up of security professionals representing high technology companies, insurance and related service providers.

- Its purpose is to address the emerging security threats that are common to the technology industry

- Currently there are 3 TAPA organizations:
  - TAPA EMEA (Europe, Middle East, Africa)
  - TAPA America
  - TAPA Asia (formed in 2000)

3. TAPA (continued)

TAPA develop and utilize common tools (Freight Security Requirements, contract language, assessment protocol) to:

✓Increase security awareness and communicate best known methods (BKM's) to industry and supplier base

✓Communicate value and attractiveness of high-tech cargo to criminal element, particularly to violent criminals

✓Establish industry forum to evaluate effectiveness, pursue continuous improvement, and set future goals

3. TAPA (continued)

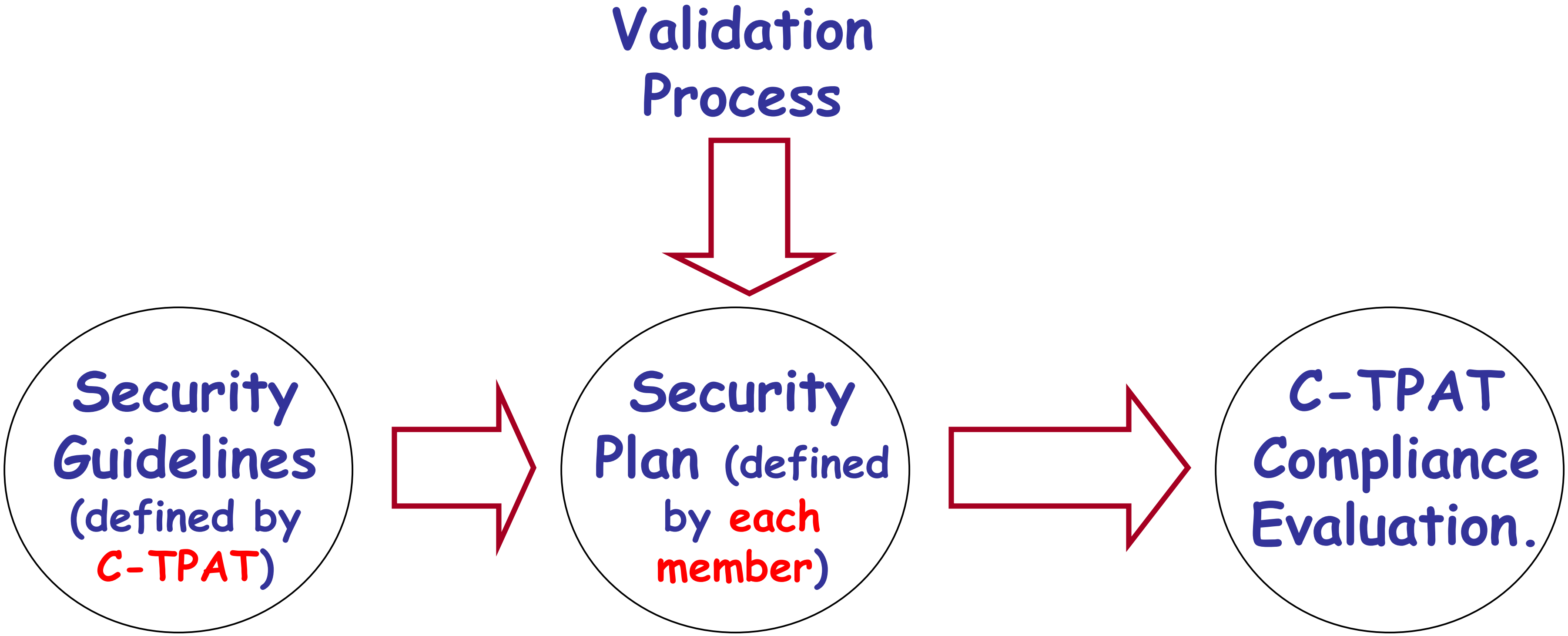
FSR Certification:

- Established to ensure the safe and secure in-transit storage and warehousing of any TAPA member’s (buyer’s) assets throughout the world.
- Specifies the minimum acceptable standards for security
- Example of security requirement:
  - Perimeter fencing
  - CCTV system and its coverage
  - Lighting
  - Alarm detection
  - Documentation of security procedure
  - Lockable cargo doors for trucks
  - Etc

4. Customs-Trade Partnership Against Terrorism (C-TPAT)

- In November 2001, US Customs initiated C-TPAT to improve container security as they move through the global supply chain
- Customs officials work in partnership with private industry to review supply chain security plans and recommending improvements
- In return, C-TPAT members' cargo are **less likely to be screened for weapons of mass destruction (WMDs)**
- Participants include importers, Carriers, Brokers, Warehouse operators, manufacturers (including foreign manufacturers)

C-TPAT Validation Process



Validation Process

Security Guidelines (defined by C-TPAT)

Security Plan (defined by each member)

C-TPAT Compliance Evaluation.

C-TPAT guideline coverage:

-Personnel Security, Physical Security, Access Control, Education & Training Awareness, Manifest procedures, Conveyance Security

5. 24-Hour Advance Manifest Rule

Ocean Cargo

- Carriers must submit a cargo declaration to US Customs and Border Protection (CBP) 24 hours before cargo is laden aboard the vessel at a foreign port

Air Cargo

- At “wheels up” for flights less than four hours
- Four hours prior to arrival for flights over four hours in length.
- No-Load Order or Inspections for
  - Invalid cargo descriptions
  - No address, incomplete address
  - Fields left blank
  - Inconsistent documents

6. Container Security Initiative (CSI)

- Government to government initiative
- This initiative started in 2002
- Deploy CBP staff in foreign ports
- Check containers that are bound to US
- US “borders” now at foreign ports
- Targeting, screening and inspecting suspect cargo prior to lading
- Non-intrusive inspections
- Screen against WMD at foreign ports

CSI Framework

US Port

How can we maximize the likelihood of a high-detection hit-rate.

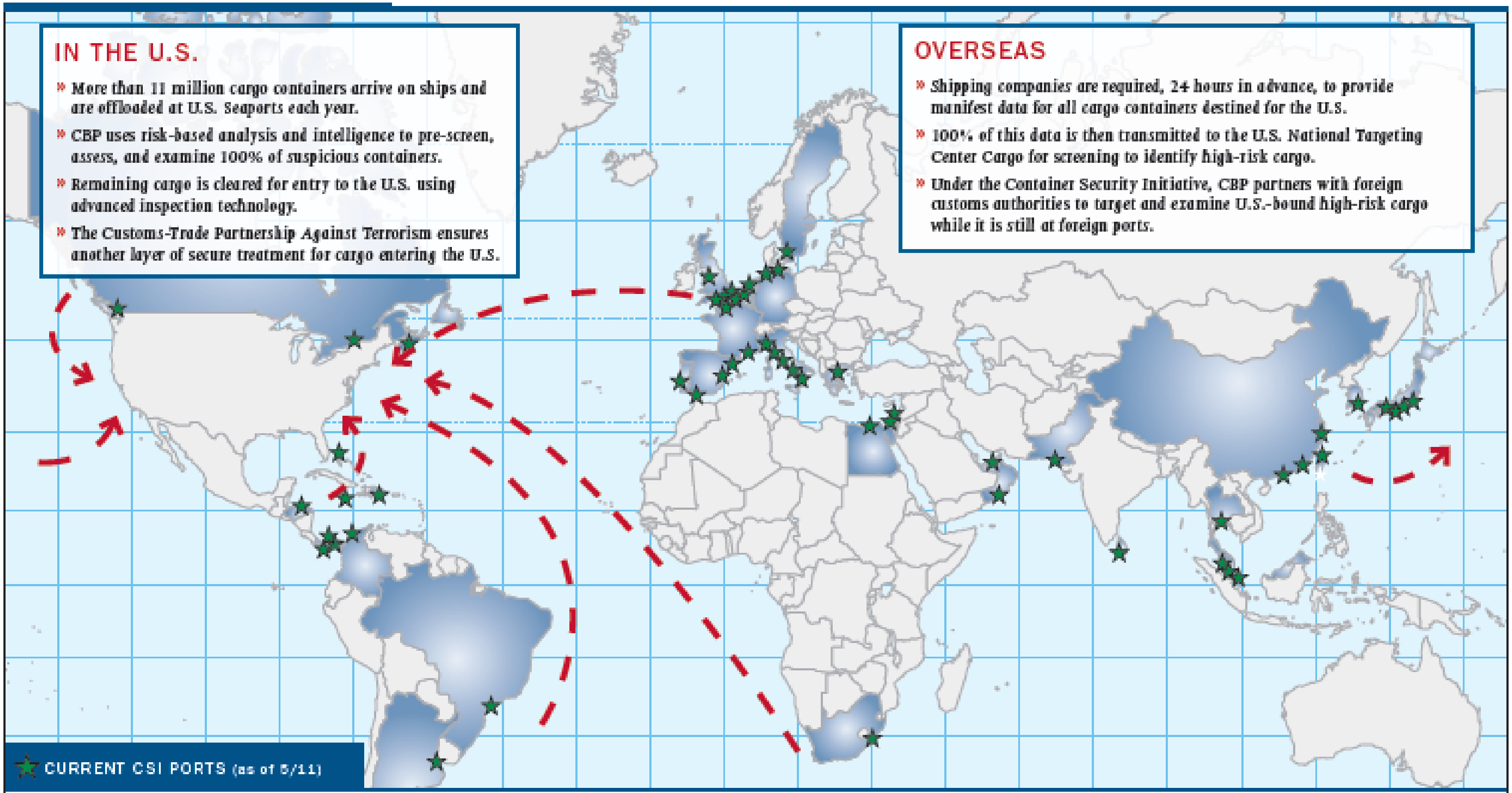
Foreign Port

What do we need here to ensure only legitimate goods are loaded

Transport

How can we be sure nothing "slipped in" ?

CSI Ports



IN THE U.S.

- More than 11 million cargo containers arrive on ships and are offloaded at U.S. Seaports each year.
- CBP uses risk-based analysis and intelligence to pre-screen, assess, and examine 100% of suspicious containers.
- Remaining cargo is cleared for entry to the U.S. using advanced inspection technology.
- The Customs-Trade Partnership Against Terrorism ensures another layer of secure treatment for cargo entering the U.S.

OVERSEAS

- Shipping companies are required, 24 hours in advance, to provide manifest data for all cargo containers destined for the U.S.
- 100% of this data is then transmitted to the U.S. National Targeting Center Cargo for screening to identify high-risk cargo.
- Under the Container Security Initiative, CBP partners with foreign customs authorities to target and examine U.S.-bound high-risk cargo while it is still at foreign ports.

★ CURRENT CSI PORTS (as of 5/11)

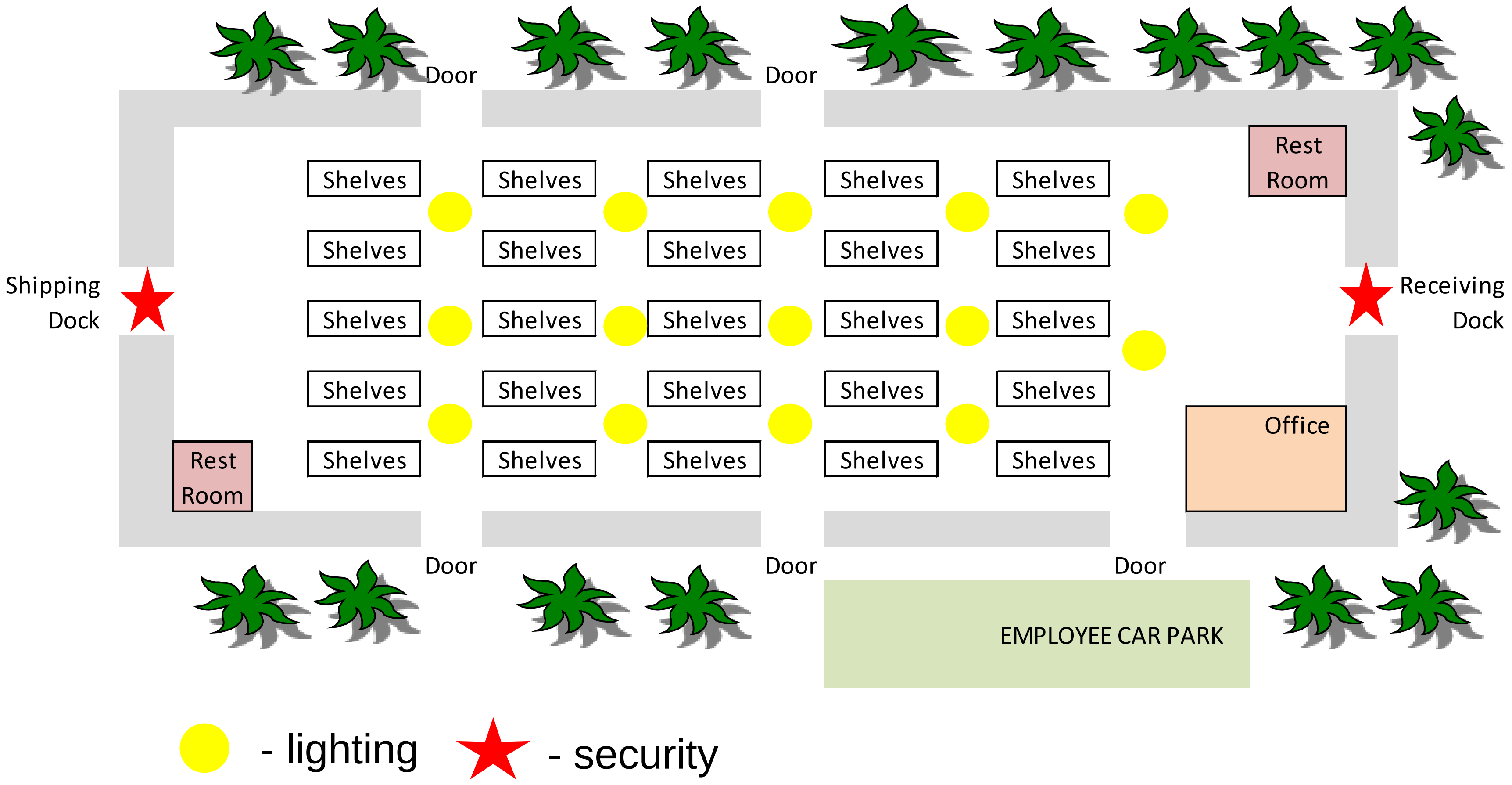
- Halifax, Montréal, and Vancouver, Canada
- Rotterdam, The Netherlands
- Le Havre, France
- Marseille, France
- Bremerhaven, Germany
- Hamburg, Germany
- Antwerp, Belgium
- Zeebrugge, Belgium
- Singapore
- Yokohama, Japan
- Tokyo, Japan
- Hong Kong
- Gothenburg, Sweden
- Felixstowe, United Kingdom
- Liverpool, Thamesport, Tilbury, and Southampton, United Kingdom
- Genoa, Italy
- La Spezia, Italy
- Livorno, Italy
- Naples, Italy
- Gioia Tauro, Italy
- Pusan, Korea
- Durban, South Africa
- Port Klang, Malaysia
- Tanjung Pelepas, Malaysia
- Piraeus, Greece
- Algeciras, Spain
- Nagoya and Kobe, Japan
- Laem Chabang, Thailand
- Dubai, United Arab Emirates
- Shanghai, China
- Shenzhen, China
- Kaohsiung
- Santos, Brazil
- Colombo, Sri Lanka
- Buenos Aires, Argentina
- Lisbon, Portugal
- Port Salalah, Oman
- Port of Cortes, Honduras
- Chi-Lung
- Valencia, Spain
- Caucedo, Dominican Republic
- Barcelona, Spain
- Kingston, Jamaica
- Freeport, Bahamas
- Qasim, Pakistan
- Balboa, Panama
- Cartagena, Colombia
- Ashdod, Israel
- Haifa, Israel
- Colón and Manzanillo, Panama
- Port Alexandria, Egypt

Today's Problem

- **Improve existing warehouse layout for supply chain security**
- **Use seals on the packages so that tampering will be obvious**
- **Check the background of staff involved in transportation, and information like contents revealed to only a few key staff**
- **Provide driver/transportation staff with hand-phone to alert company/civil defense in case of emergency**
- **GPS tracking of transportation trucks**
- **Plan for TAPA certification and C-TPAT validation**
- **Adhere to 24-Hour Advance Manifest Rule**
- **Regular audits of supplier qualification criteria – To comply to certain security standards**

Original Warehouse Layout

Security Issues with existing layout



Problem Identified

1. **The closeness of this parking area, plus the fact that it is right by a door, makes it easier for employees to take things from the warehouse and put them in their cars. The further people park from the warehouse, the better. If possible, have a fence separating the warehouse from the parking lot.**

2. **The receiving dock and the shipping dock are at the opposite side of the building, while it is good for material flow, both side are exposed to security breach. In addition, cross docking will be impossible.**

3. **Existing warehouse has far too many doors. There should only be one that is open, and there should be a guard or other employee in charge of watching this door. If fire regulations require more than one door, use bars that set off an alarm if the doors are opened.**

con’t….

4. **This is a bad spot for the restroom. To reach it, the truckers have to walk into the warehouse. This puts your goods at risk of being stolen. Just because people are dropping off or picking up shipments doesn't mean they are free to wander around. It's best to keep unauthorized people out of the warehouse.**

5. **These bushes are good hiding spots for things stolen out of the warehouse, especially because they are right by the door. So either get rid of the bushes, or lock the doors.**

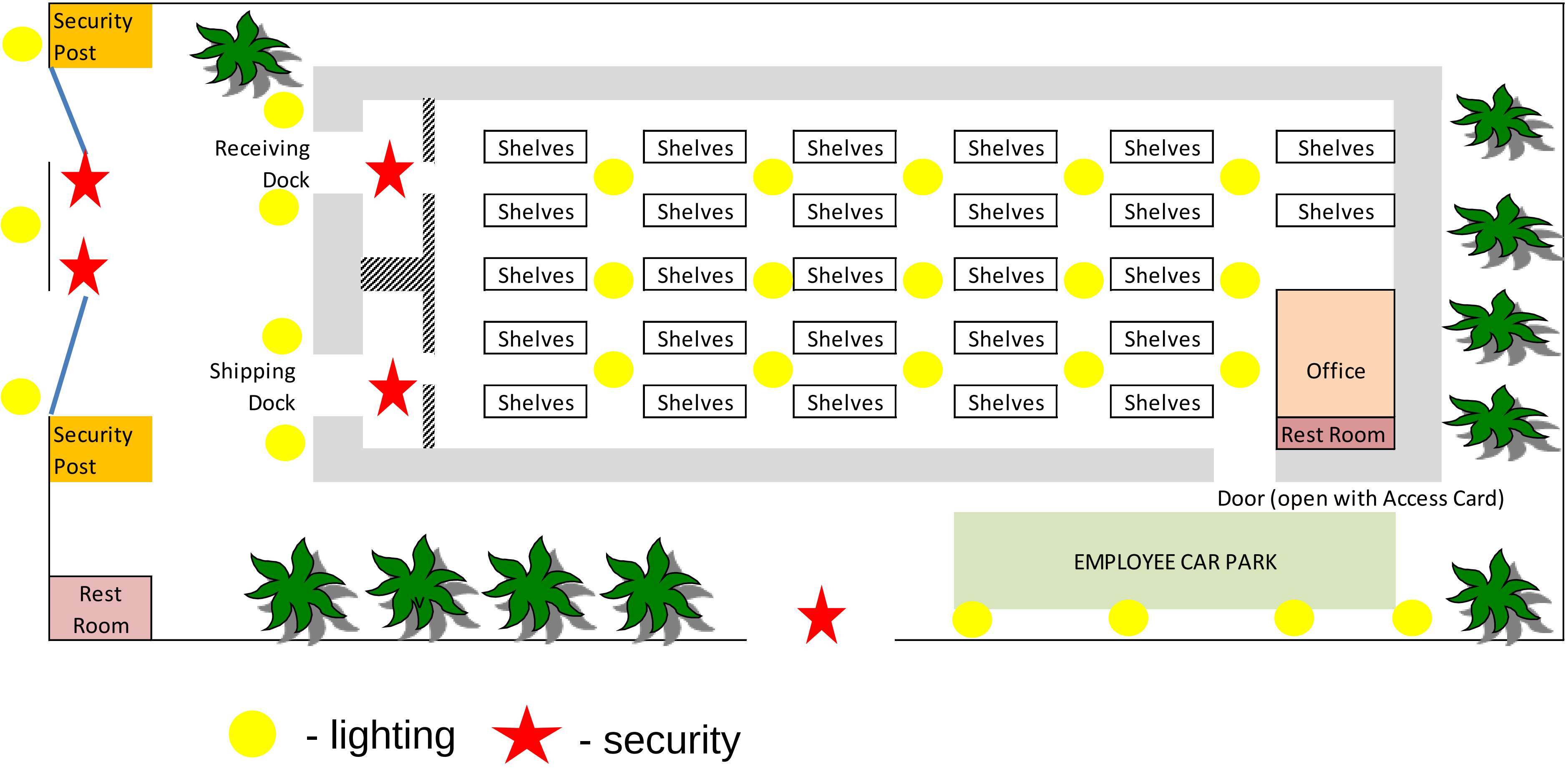
6. **CCTV only covers shipping and receiving docks. It should cover the whole warehouse, especially the doors.**

7. **Lighting should be extended to the receiving and shipping docs.**

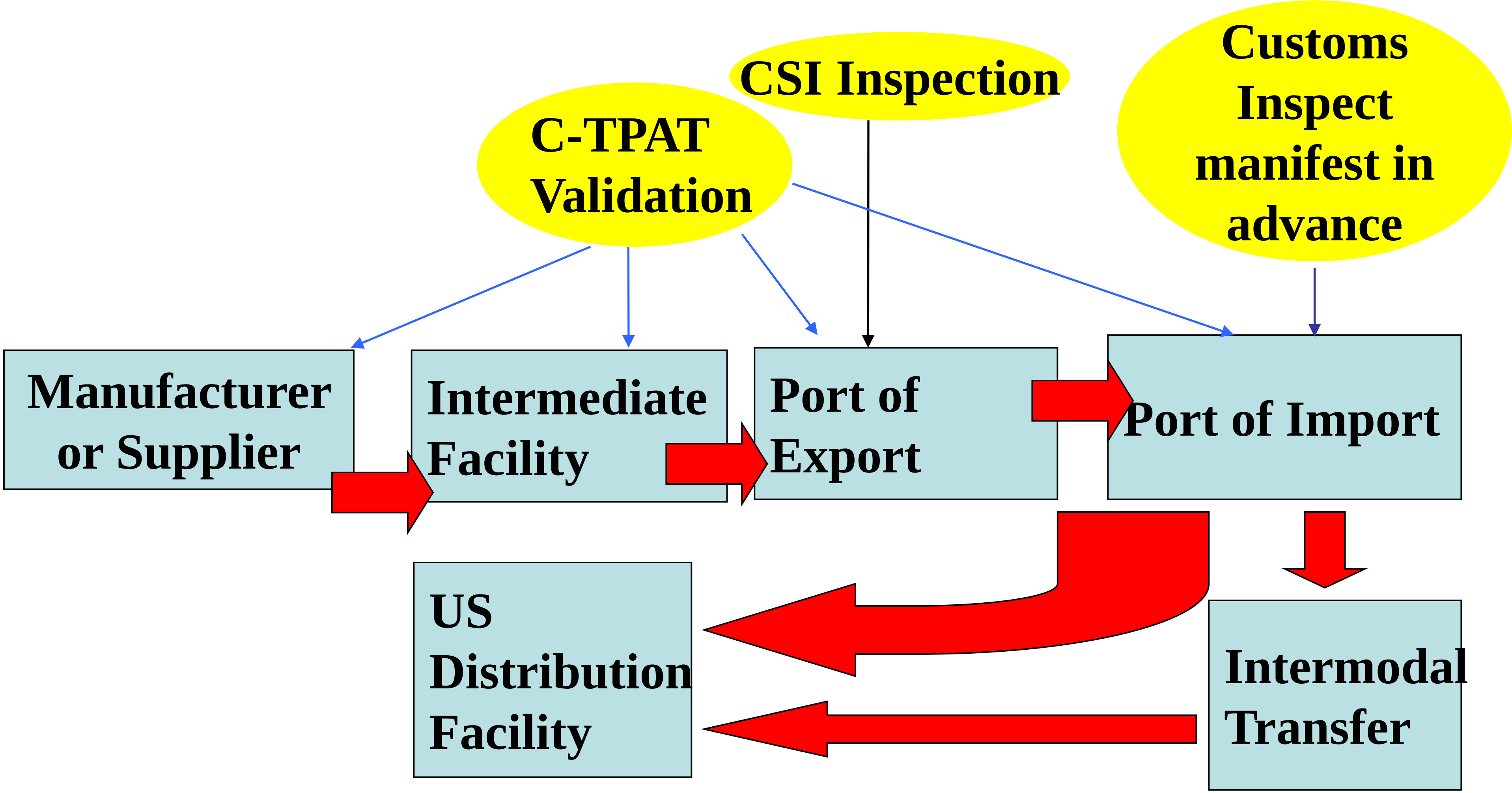
8. **The whole perimeter of the warehouse should be fenced in.**

Suggested Warehouse Layout

Resolves physical facility security



Supply Chain Security (to US)

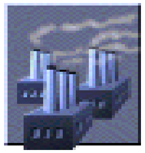


Note: TAPA & ISO 28000:2007 applies to entire supply chain

Supply Chain Visibility

- Enhance C-TPAT validation and CSI process
- Product visibility enables tracking and tracking for security breach investigation
  - When did it happen
  - Who was in custody of the goods
- Meets multiple security concerns
  - Theft
  - Smuggling
  - Bombs and Weapons of Mass Destruction (WMD)

Security Enhanced by Supply Chain Visibility



1. Manufacturer/Consolidator

- Associate manifest with container and seal ID
- Verify user and electronically secure container
- Automatically record departure time and place
- Transmit data to TSS

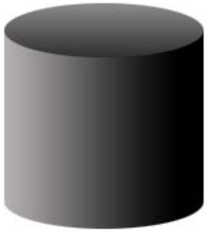
2. Port of Loading - Arrival

- Automatically record container arrival
- Automatically verify security status at entry gate

3. Port of Loading - Vessel load

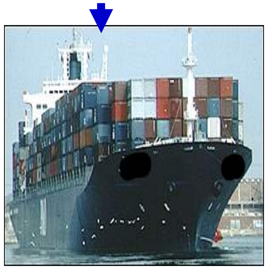
- Verify clear for loading status
- Automatically verify security status at quay cranes

Transportation Security System Platform



4. Port of Unloading - Arrival

- Transmit documentation and updates to Customs
- Provide alerts if container deviates from plan
- Provide reports and other analytics for supply chain and security inefficiencies
- Maintain audit trail of accountability
- Provide web access to users

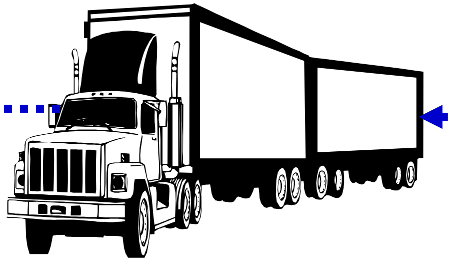


5. Port of Discharge - Vessel Unload

- Verify clear for unloading status
- Automatically verify security status at quay cranes

6. Port of Discharge - Departure

- Automatically record departure
- Automatically verify security status at exit gate



Learning Outcome

- Explain Key aspects of Supply Chain/ Logistics Security
- Describe Major Supply Chain Security Initiatives
- Identify potential security breaches and make recommendations to overcome it
- Enhance the Supply Chain/Logistics Security with Product Visibility